Discente: Igor Lima Rocha

Disciplina: Introdução a ciência da computação

Docente: Edgar Alexander

**Segurança e privacidade**

**• Adware:** Adware é o nome dado aos programas projetados para exibir anúncios em seu computador, redirecionar suas solicitações de pesquisa para websites de publicidade e coletar dados de marketing sobre você - por exemplo, os tipos de sites que você visita - para que anúncios personalizados possam ser exibidos.

O adware - que coleta dados com o seu consentimento - não deve ser confundido com programas de spyware do Trojan que coletam informações, sem a sua permissão. Se o Adware não o notificar de que está coletando informações, ele será considerado malicioso - por exemplo, malware que usa o comportamento do Trojan-Spy.

**• Application-Layer Attack:** Os ataques DDoS na camada do aplicativo são projetados para atacar o aplicativo em si, concentrando-se em vulnerabilidades ou problemas específicos, resultando no fato de o aplicativo não conseguir entregar conteúdo ao usuário. Os ataques da camada de aplicativo são projetados para atacar aplicativos específicos, o mais comum são os servidores da Web, mas podem incluir qualquer aplicativo, como serviços de voz SIP e BGP.

**• Backdoor:** Um backdoor é um método, muitas vezes secreto, de ignorar autenticação ou criptografia normal em um sistema de computador , produto ou dispositivo incorporado (por exemplo, um roteador doméstico) ou sua incorporação, por exemplo, como parte de um sistema criptográfico , um algoritmo , um chipset ou um "computador homunculus" - um pequeno computador dentro de um computador (como o encontrado na tecnologia AMT da Intel).Os backdoors são usados ​​para proteger o acesso remoto a um computador ou obter acesso a texto simples em sistemas criptográficos. O backdoor pode ser usado para obter acesso a senhas, excluir dados em discos rígidos ou transferir informações dentro da nuvem.

Um backdoor pode assumir a forma de uma parte oculta de um programa, um programa separado (por exemplo, Back Orifice pode subverter o sistema através de um rootkit), código no firmware do hardware, ou partes de um sistema operacional como o Windows. Cavalos de Tróia podem ser usados ​​para criar vulnerabilidades em um dispositivo. Um cavalo de Tróia pode parecer um programa totalmente legítimo, mas, quando executado, aciona uma atividade que pode instalar um backdoor. Embora alguns sejam secretamente instalados, outros backdoors são deliberados e amplamente conhecidos. Esses tipos de backdoors têm usos "legítimos", como fornecer ao fabricante uma maneira de restaurar senhas de usuário.

**• Black Hat:** O black hat refere-se a um hacker que invade um sistema de computador ou uma rede com intenção maliciosa. Um hacker black hat pode explorar vulnerabilidades de segurança para ganho monetário; roubar ou destruir dados privados; ou alterar, interromper ou encerrar sites e redes. O hacker black hat também pode vender essas explorações a outras organizações criminosas.

**• Bloatware:** Bloatware é um software que possui recursos desnecessários que usam grandes quantidades de memória e RAM. O software passa a ser conhecido como bloatware quando se torna tão difícil de manejar que sua funcionalidade é abafada por seus recursos inúteis. Isso também é conhecido como software inchado.

O bloatware também é uma gíria para inúmeros programas pré-instalados em novos PCs. Muitos desses programas são "lite" ou versões limitadas de avaliação projetadas para atrair novos usuários a comprar ou assinar as versões completas.

**• Bluebugging:** O Bluebugging é uma forma de ataque por Bluetooth geralmente causada por falta de conhecimento. Foi desenvolvido após o início do bluejacking e bluesnarfing.

**• Botnet:** Uma botnet é um número de dispositivos conectados à Internet, cada um deles executando um ou mais bots. As botnets podem ser usadas para executar ataques distribuídos de negação de serviço (ataque DDoS), roubar dados, enviar spam e permitir que o invasor acesse o dispositivo e sua conexão.

**• Crapware:** Software que tem pouco valor ou que não funciona corretamente. Também chamado de "lameware", o termo geralmente se refere a vários aplicativos de teste que são pré-instalados em um novo computador (consulte o bloatware).

**• Compromised-Key Attack:** Um Compromised-Key Attack é o uso de uma chave que um invasor roubou para obter acesso a uma transmissão segura. A chave permite que o invasor descriptografe os dados que estão sendo enviados. O remetente e o destinatário geralmente não estão cientes do ataque.

**• Data Modification:** Modificação de dados ocorre quando um valor salvo (ou armazenado) em um computador é alterado para um valor diferente.

**• Denial of Service (DoS):** É um ataque cibernético no qual o autor tenta tornar uma máquina ou recurso de rede indisponível para os usuários pretendidos interrompendo temporariamente ou indefinidamente os serviços de um host conectado à Internet. Normalmente, a negação de serviço é realizada ao inundar a máquina ou o recurso segmentado com solicitações supérfluas, na tentativa de sobrecarregar os sistemas e impedir que algumas ou todas as solicitações legítimas sejam atendidas.

**• Distributed Denial of Service:** Um DDoS é um ataque no qual vários sistemas de computador comprometidos atacam um alvo, como um servidor, site ou outro recurso de rede, e causam uma negação de serviço para os usuários do recurso de destino. A enxurrada de mensagens recebidas, solicitações de conexão ou pacotes malformados para o sistema de destino obriga a desacelerar ou até travar e desligar, negando, assim, o serviço a usuários ou sistemas legítimos.

**• DNS poisoning:** O DNS poisoning, também conhecido como spoofing de DNS, é um tipo de ataque que explora vulnerabilidades no sistema de nomes de domínio (DNS) para desviar o tráfego da Internet de servidores legítimos e falsos.

**• Hacker:** Um hacker de computador é qualquer especialista em computação habilidoso que usa seu conhecimento técnico para superar um problema. Embora "hacker" possa se referir a qualquer programador de computador habilidoso, o termo se tornou associado na cultura popular a um " hacker de segurança ", alguém que, com seu conhecimento técnico, usa bugs ou explorações para invadir sistemas de computador.

**• Crackers:** Um cracker é alguém que invade o sistema de computador de outra pessoa, geralmente em uma rede; ignora senhas ou licenças em programas de computador; ou de outras formas violar intencionalmente a segurança do computador. Um cracker pode estar fazendo isso com fins lucrativos, maliciosamente, por algum propósito ou causa altruísta, ou porque o desafio está lá. Alguma invasão foi feita ostensivamente para apontar fraquezas no sistema de segurança de um site.

**• ICMP Attack:** ICMP significa Internet Control Message Protocol e é o protocolo mais usado na tecnologia de rede. Um protocolo sem conexão, o ICMP não usa nenhum número de porta e funciona na camada de rede. O ICMP é comumente usado para fins de diagnóstico, relatório de erros ou consulta de qualquer servidor, e agora os invasores estão usando o ICMP para enviar cargas úteis, o que discutiremos aqui. O comando ping popular usará o ICMP. Existem muitos problemas de segurança de mensagens ICMP que realmente precisamos analisar.

Uma inundação de ping é uma negação de serviço ataque em que o invasor tenta sobrecarregar um dispositivo alvo de ICMP pacotes de eco-pedido, fazendo com que o alvo para se tornar inacessível ao tráfego normal. Quando o ataque tráfego vem de vários dispositivos, o ataque se torna um DDoS ou de negação de serviço distribuída ataque .

**• ICMP Tunneling:** Um túnel ICMP estabelece uma conexão secreta entre dois computadores remotos (um cliente e um proxy), usando solicitações de eco ICMP e pacotes de resposta. Um exemplo dessa técnica é o tunelamento do tráfego TCP completo através de solicitações e respostas de ping.

**• IP Spoofing:** O IP Spoofing é uma técnica usada para obter acesso não autorizado a máquinas, em que um invasor personifica de forma ilícita outra máquina, manipulando pacotes IP. O IP Spoofing envolve a modificação do cabeçalho do pacote com um endereço IP de origem falsificado (falsificado), uma soma de verificação e o valor do pedido.

**• Keylogging:** Um keylogger (abreviação de keystroke logger) é um software que rastreia ou registra as chaves atingidas em seu teclado, normalmente de maneira oculta, para que você não saiba que suas ações estão sendo monitoradas. Isso geralmente é feito com a intenção mal-intencionada de coletar informações de sua conta, números de cartão de crédito, nomes de usuário, senhas e outros dados privados.

**• Lammer:** Uma pessoa que sabe muito pouco sobre computadores/computação. Também se refere a uma pessoa que finge ser um hacker, mas não é.

**• Logic Bomb:** Uma bomba lógica é um pedaço de código intencionalmente inserido em um sistema de software que ativará uma função maliciosa quando condições especificadas forem atendidas. Por exemplo, um programador pode ocultar uma parte do código que inicia a exclusão de arquivos (como um acionador de banco de dados salarial), caso eles sejam rescindidos da empresa.

**• Malware:** Malware ou software mal-intencionado é qualquer programa ou arquivo que seja prejudicial a um usuário de computador. Os tipos de malware podem incluir vírus de computador, worms, cavalos de Tróia e spyware. Esses programas mal-intencionados podem executar uma variedade de funções diferentes, como roubar, criptografar ou excluir dados confidenciais, alterar ou seqüestrar as principais funções de computação e monitorar a atividade do computador dos usuários sem a permissão deles.

**• Man-in-the-Middle-Atack:** Em criptografia e segurança de computadores, um ataque man-in-the-middle (MITM) é um ataque em que o invasor retransmite secretamente e possivelmente altera as comunicações entre duas partes que acreditam estar se comunicando diretamente entre si. Um exemplo de um ataque MITM é a escuta ativa, em que o invasor faz conexões independentes com as vítimas e transmite mensagens entre elas para fazê-las acreditar que estão falando diretamente umas com as outras por meio de uma conexão privada, quando, na verdade, toda a conversa é controlada pelo invasor. O atacante deve ser capaz de interceptar todas as mensagens relevantes que passam entre as duas vítimas e injetar novas. Isso é simples em muitas circunstâncias; por exemplo, um invasor dentro do alcance de recepção de um ponto de acesso sem fio não criptografado (Wi-Fi) pode se inserir como um intermediário.

**• Password-based Attacks:** Um ataque no qual tentativas repetitivas são feitas para duplicar uma sequência válida de logon ou senha.

**• Ping of Death:** Um ping de morte é um tipo de ataque em um sistema de computador que envolve o envio de um ping malformado ou mal-intencionado para um computador. Um pacote de ping formado corretamente tem tipicamente 56 bytes de tamanho ou 64 bytes quando o cabeçalho do Protocolo da Internet é considerado.

**• Phishing:** Phishing é a tentativa fraudulenta de obter informações confidenciais, como nomes de usuário, senhas e detalhes de cartão de crédito, disfarçando-se de uma entidade confiável em uma comunicação eletrônica. Geralmente realizado por e-mail spoofing ou mensagens instantâneas, ele geralmente direciona os usuários a inserir informações pessoais em um site falso que corresponde à aparência do site legítimo.

**• Phreaker:** Phreaking é um termo de gíria criado para descrever a atividade de uma cultura de pessoas que estudam, experimentam ou exploram sistemas de telecomunicações, como equipamentos e sistemas conectados a redes telefônicas públicas.

**• Pod Slurping:** Pod slurping é o ato de usar um dispositivo portátil de armazenamento de dados, como um player de áudio digital iPod, para baixar ilicitamente grandes quantidades de dados confidenciais, conectando-os diretamente a um computador onde os dados são mantidos e que podem estar dentro de um firewall.

**• Port Scanning:** Um Port Scanning é um aplicativo projetado para investigar um servidor ou host quanto a portas abertas. Esse aplicativo pode ser usado por administradores para verificar as políticas de segurança de suas redes e por invasores para identificar serviços de rede em execução em um host e explorar vulnerabilidades.

**• Ransomware:** Ransomware é um tipo de software malicioso, ou malware, projetado para negar acesso a um sistema de computador ou dados até que um resgate seja pago. O ransomware normalmente se espalha através de e-mails de phishing ou visitando inadvertidamente um site infectado. O ransomware pode ser devastador para um indivíduo ou uma organização.

**• Repudiation Attacks:** Repúdio é o ato de recusar a autoria de algo que aconteceu. Um ataque de repúdio ocorre quando um aplicativo ou sistema não adota controles para rastrear e registrar adequadamente as ações dos usuários, permitindo assim a manipulação mal-intencionada ou forjando a identificação de novas ações.

**• Rootkit:** Um rootkit é uma coleção de software de computador, normalmente mal-intencionada, projetada para permitir o acesso a um computador ou a uma área de seu software que não é permitida e, com frequência, mascara sua existência ou a existência de outro software. O termo rootkit é uma concatenação de "root" e a palavra "kit".

**• Scareware:** Scareware é um tipo de malware projetado para enganar as vítimas para que comprem e baixem softwares inúteis e potencialmente perigosos. O Scareware , que gera pop-ups que se assemelham a mensagens do sistema do Windows, geralmente diz ser um software antivírus ou antispyware, um aplicativo de firewall ou um limpador de registro.

**• Session hijacking:** Na ciência da computação, o sequestro de sessão, às vezes também conhecido como seqüestro de cookie, é a exploração de uma sessão de computador válida - às vezes também chamada de chave de sessão - para obter acesso não autorizado a informações ou serviços em um sistema de computador.

**• Scanners:** Um scanner é um dispositivo que captura imagens de impressões fotográficas, cartazes, páginas de revistas e fontes semelhantes para edição e exibição de computadores. Os scanners vêm em tipos de mão, de alimentação e de mesa e para digitalizar somente em preto e branco ou em cores.

**• Script Kiddy:** Na programação e na cultura hacker, um script kiddie, skiddie, ou skid é um indivíduo não qualificado que usa scripts ou programas desenvolvidos por outros para atacar sistemas e redes de computadores e desfigurar sites, como um web shell. É geralmente assumido que a maioria das crianças de script são jovens que não têm a capacidade de escrever programas sofisticados ou façanhas por conta própria e que seu objetivo é tentar impressionar seus amigos ou ganhar crédito em comunidades entusiastas de computadores. No entanto, o termo não se relaciona com a idade real do participante. O termo é considerado depreciativo.

**• Server Spoofing:** Um Server Spoofing ocorre quando uma parte mal-intencionada se faz passar por outro dispositivo ou usuário em uma rede para lançar ataques contra hosts da rede , roubar dados, espalhar malware ou ignorar controles de acesso. Existem vários tipos diferentes de ataques de falsificação que as partes mal-intencionadas podem usar para realizar isso.

**• Sidejacking:** O sidejacking é o processo de roubar o acesso de alguém a um site, muitas vezes feito em redes públicas sem fio. Para obter acesso a um site, o mau ator usa um sniffer de pacotes para obter um cookie não criptografado que concede acesso a um site, como o webmail.

**• Shovelware:** O Shovelware é um jargão de informática para pacotes de software mais conhecido pela quantidade do que está incluído do que pela qualidade ou utilidade. A metáfora implica que os criadores mostraram pouco cuidado com a qualidade do software original, como se a nova compilação ou versão tivesse sido criada pela adição indiscriminada de títulos "pela pá" da mesma maneira que alguém colocaria material a granel em uma pilha. O termo "shovelware" é cunhado por analogia semântica com frases como shareware e freeware, que descrevem métodos de distribuição de software. Surgiu pela primeira vez no início dos anos 90, quando grandes quantidades de programas de demonstração shareware foram copiados em CD-ROMs e anunciados em revistas ou vendidos em mercados de pulgas de computador.

**• SMiShing:** O SMiShing é um ataque de segurança em que o usuário é induzido a baixar um cavalo de tróia, vírus ou outro malware em seu telefone celular ou outro dispositivo móvel. SMiShing é a abreviação de "SMS phishing".

**• Smurf:** O ataque Smurf é um ataque distribuído de negação de serviço no qual um grande número de pacotes ICMP (Internet Control Message Protocol) com o IP de origem falsificado da vítima é transmitido para uma rede de computadores usando um endereço de broadcast IP. A maioria dos dispositivos em uma rede responderá, por padrão, enviando uma resposta para o endereço IP de origem. Se o número de máquinas na rede que recebe e responde a esses pacotes for muito grande, o computador da vítima será inundado com tráfego. Isso pode retardar o computador da vítima ao ponto em que se torna impossível trabalhar.

**• Sniffer Attack:** O Sniffing attack ou sniffer attack, no contexto da segurança da rede, corresponde ao roubo ou interceptação de dados, capturando o tráfego da rede usando um sniffer (um aplicativo destinado a capturar pacotes de rede).

**• Snooping:** O Snooping, em um contexto de segurança, é um acesso não autorizado aos dados de outra pessoa ou empresa. A prática é semelhante à escuta clandestina, mas não se limita necessariamente ao acesso aos dados durante sua transmissão. A espionagem pode incluir a observação casual de um e-mail que aparece na tela do computador de outra pessoa ou observa o que alguém está digitando. A espionagem mais sofisticada usa programas de software para monitorar remotamente a atividade em um computador ou dispositivo de rede.

**• Social Engineering:** A engenharia social é um vetor de ataque que depende muito da interação humana e geralmente envolve a manipulação de pessoas para que infrinjam procedimentos normais de segurança e melhores práticas, a fim de obter acesso a sistemas, redes ou locais físicos, ou para ganhos financeiros.

**• Spam:** O spam é um lixo eletrônico ou postagens de grupos de notícias indesejados. Algumas pessoas definem spam ainda mais geralmente como qualquer email não solicitado. No entanto, se um irmão perdido encontrar seu endereço de e-mail e enviar uma mensagem, isso dificilmente poderia ser chamado de spam, mesmo que não seja solicitado. O spam real é geralmente publicidade por e-mail para algum produto enviado para uma lista de discussão ou grupo de notícias.

**• Spoof:** A palavra “spoof" significa enganar, enganar ou enganar. Portanto, no mundo da TI, spoofing refere-se a enganar ou enganar sistemas de computador ou outros usuários de computador. Isso geralmente é feito escondendo-se a identidade ou falsificando a identidade de outro usuário na Internet.

**• Spyware:** Spyware é um software indesejado que se infiltra em seu dispositivo de computação, roubando seus dados de uso da Internet e informações confidenciais. O spyware é classificado como um tipo de malware - um software malicioso projetado para acessar ou danificar seu computador, geralmente sem o seu conhecimento. O spyware reúne suas informações pessoais e as retransmite para anunciantes, empresas de dados ou usuários externos.

**• TCP Syn / TCP ACk Attack:** O TCP SYN flood (também conhecido como SYN flood) é um tipo de ataque DDoS ( Distributed Denial of Service ) que explora parte do handshake de três vias TCP normal para consumir recursos no servidor de destino e torná-lo irresponsivo.

Essencialmente, com o DDoS de inundação SYN, o ofensor envia solicitações de conexão TCP mais rápido do que a máquina de destino pode processá-las, causando saturação da rede.

**• TCP Sequence Number Attack:** Um ataque de previsão de sequência TCP é uma tentativa de prever o número de sequência usado para identificar os pacotes em uma conexão TCP, que pode ser usada para falsificar pacotes. Ao monitorar o tráfego antes de um ataque ser montado, o host mal-intencionado pode descobrir o número de sequência correto.

**• TCP Hijacking:** O TCP Hijacking ocorre quando um usuário autorizado obtém acesso a uma conexão de rede genuína de outro usuário. Isso é feito para ignorar a autenticação de senha, que normalmente é o início de uma sessão.

**• Teardrop:** Um Teardrop Attack é uma negação de serviço (DoS) ataque que envolve o envio de pacotes fragmentados para uma máquina de destino. Como a máquina que recebe esses pacotes não pode montá-los devido a um bug na remontagem de fragmentação TCP / IP, os pacotes se sobrepõem, causando um crash no dispositivo de rede de destino.

**• Trojan:** Na computação, um cavalo de Tróia (Trojan) é qualquer malware que engane os usuários de sua verdadeira intenção. O termo é derivado da história grega antiga do enganoso Cavalo de Tróia que levou à queda da cidade de Tróia.

**• Vírus:** Um vírus de computador é um tipo de malware que, quando executado, se replica modificando outros programas de computador e inserindo seu próprio código. Quando essa replicação é bem-sucedida, as áreas afetadas são consideradas "infectadas" por um vírus de computador.

**• White Hat:** O termo "White Hat" na gíria da Internet refere-se a um hacker de computador ético, ou a um especialista em segurança de computadores, especializado em testes de penetração e em outras metodologias de teste que garantam a segurança dos sistemas de informação de uma organização. Hacking ético é um termo destinado a implicar uma categoria mais ampla do que apenas testes de penetração. Contrastado com o chapéu preto, um hacker mal-intencionado, o nome vem de filmes ocidentais, onde cowboys heróicos e antagônicos tradicionalmente vestem um chapéu branco e um preto, respectivamente. Enquanto um hacker de chapéu branco hackeia sob boas intenções com permissão, e um hacker de chapéu preto tem intenção maliciosa, há um terceiro tipo conhecido como umhacker de chapéu cinza que hackeia com boas intenções sem permissão.

**• Worm:** Um worm de computador é um programa de computador de malware autônomo que se replica para se espalhar para outros computadores. Muitas vezes, ele usa uma rede de computadores para se espalhar, contando com falhas de segurança no computador de destino para acessá-lo.