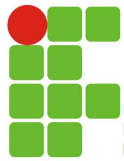
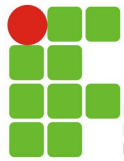
Segurança de Redes

Tecnologia em Redes de Computadores
Prof. Macêdo Firmino

Aula 02
Principais Ataques de Segurança de Redes



"Problemas são estímulos que a Vida nos apresenta para nos autoconhecer." (Hammed)



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

O que Aprenderemos?

- Entender os conceitos de ataques, ameças e vulnerabilidades;
- Compreender os principais tipos de ataques à segurança de redes, suas características e métodos de execução.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Segurança da Informação

Com o crescimento da interconectividade e da dependência de sistemas digitais, as redes se tornaram alvos frequentes de ataques cibernéticos. Esses ataques podem ser realizados por indivíduos ou grupos com diferentes objetivos: roubo de informações, interrupção de serviços, danos à reputação de uma organização, motivações políticas ou sociais, ganhos financeiros (fraudes ou extorsão), funcionários ou ex-funcionários que exploram acesso autorizado para causar danos e por diversão ou aprendizado.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Segurança da Informação

Na área da segurança da informação, ataques, ameaças e vulnerabilidades estão intimamente relacionados e são conceitos-chave para entender a natureza dos problemas de segurança e como lidar com eles.

- Vulnerabilidades: é qualquer falha, fraqueza ou brecha em um sistema, rede, aplicação ou processo que pode ser explorada por um atacante para causar danos, obter acesso não autorizado ou comprometer a segurança da informação. Exemplos incluem falta de atualizações de software, senhas fracas, sistemas mal configurados e erros de programação.

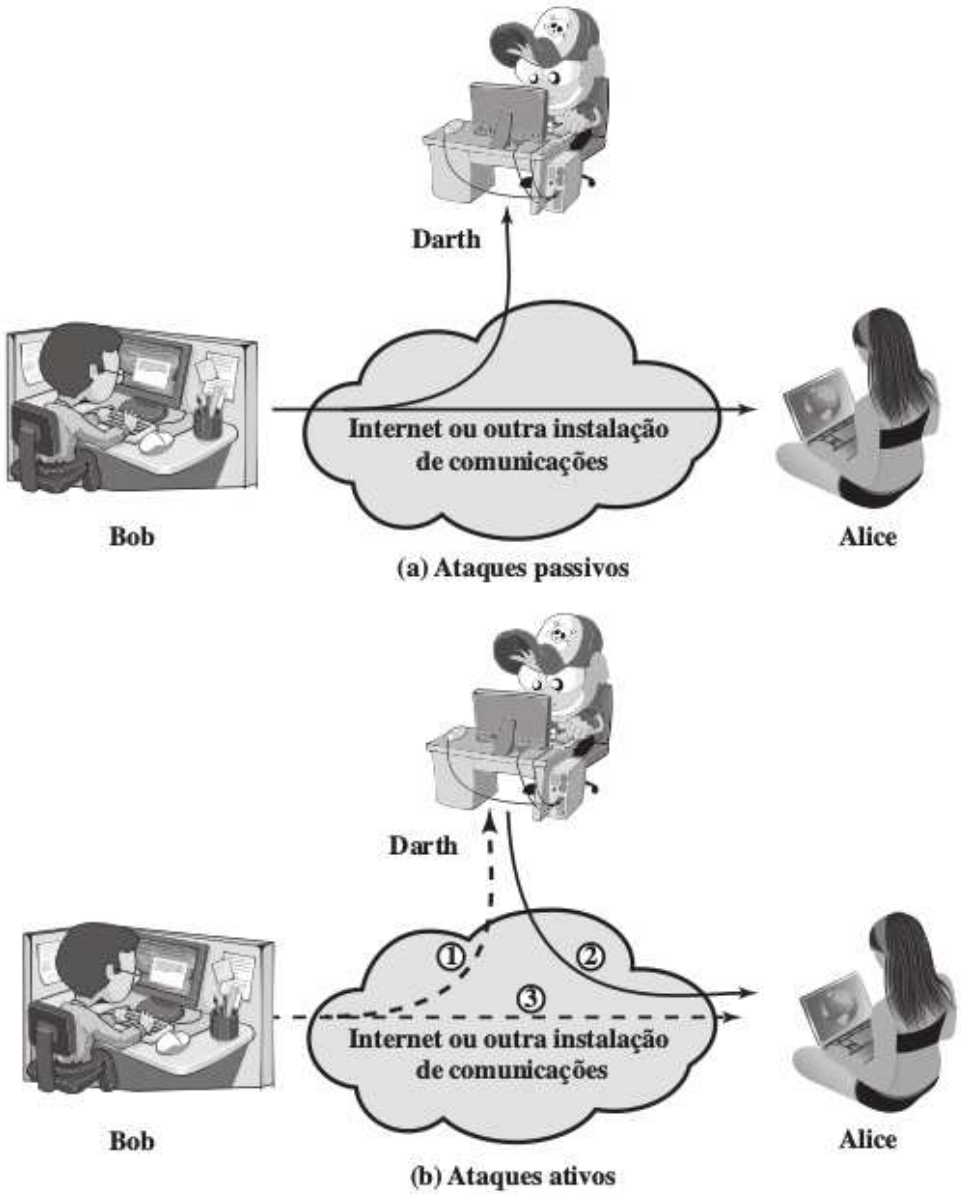
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Segurança da Informação

- Ameaças: são potenciais eventos ou ações que podem causar danos a um sistema ou organização. As ameaças podem incluir hackers mal-intencionados, *malware*, funcionários mal-intencionados ou negligentes, entre outros.
- Ataques: são ações concretas realizadas por um agente mal-intencionado para explorar as vulnerabilidades e causar danos a um sistema ou organização. Os ataques podem ser direcionados a diferentes partes de um sistema de informação, como a infraestrutura de rede, os servidores, os dados ou os usuários finais.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Um ataque pode ser de forma passiva (interceptação, monitoramento e análise de pacotes) ou ativa (adulteração, fraude, reprodução e bloqueio).



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Ameaças de Segurança de Redes

Os principais ameaças de segurança são:

- Exploração de Vulnerabilidades:
  - Códigos maliciosos (*Malwares*);
- Atacar servidores, serviços e infraestrutura de redes:
  - Negação de serviço (DoS e DDoS);
  - Desfiguração de página (*Defacement*);
  - Força bruta (*Brute force*);
- Obter informações:
  - Varredura em redes (*Scan*);
  - Interceptação de tráfego (*Sniffing*);
  - Dumpsterdiving ou trashing.
- Se passar por alguém ou falsificar informações de rede:
  - Engenharia Social.
  - IP, DNS e e-mail *spoofing*.

Malwares

Malware refere-se a qualquer *software* projetado para causar danos a computadores, redes ou usuários. Esses programas são criados com intenções maliciosas, que podem incluir roubo de informações, danificação de sistemas, espionagem, interrupção de operações normais ou até mesmo o controle remoto do dispositivo infectado.

Eles podem ser adquiridos por meio de *downloads* de sites maliciosos, anexos de e-mails infectados, dispositivos USB contaminados, ou exploração de vulnerabilidades em sistemas não atualizados.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Malwares

Alguns dos tipos mais comuns incluem:

Vírus é um programa que se anexa a outro *software* executável e pode se replicar e se espalhar quando o *software* hospedeiro é executado. Ele pode causar danos aos dados, modificar ou destruir arquivos. Os vírus são bem específicos, ou seja, um determinado vírus só ataca apenas algumas versões de determinados programas onde ele explora determinada vulnerabilidade.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Malwares

Worms são programas autônomos que se espalham de um computador para outro, geralmente através de redes. Ao contrário dos vírus, os worms não precisam se anexar a programas existentes para se propagar.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Malwares

Trojans (cavalo de tróia) são programas que parecem inofensivos ou úteis (por exemplo, jogos), mas, na realidade, têm funções maliciosas. Eles geralmente são disfarçados como *software* legítimo para enganar os usuários. Por definição, o cavalo de tróia distingue-se de um vírus ou de um worm por não infectar outros arquivos, nem propagar cópias de si mesmo automaticamente.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Malwares

Ransomware sequestra os dados criptografando no sistema da vítima e exige um resgate em troca da chave para descriptografar os dados. É uma forma de extorsão digital.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Malwares

Spyware é projetado para coletar informações sobre as atividades do usuário sem o seu conhecimento e enviar as informações coletadas para terceiros. Pode monitorar hábitos de navegação, registros de teclas digitadas (keylogger), posição do cursor nos momentos em que o mouse é clicado (screenlogger) e outras informações pessoais.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Malwares

Adware: exibe anúncios publicitários de forma invasiva ou indesejada no dispositivo da vítima. Normalmente se instala junto com programas "gratuitos", sem que o usuário perceba. Eles exibe pop-ups, banners e fazem redirecionamentos automáticos para sites de propaganda.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Malwares

Botnets consistem em um grupo de computadores infectados que dispõe de mecanismos de comunicação com o invasor e permite que ele seja controlado remotamente. São frequentemente usados para realizar ataques coordenados, enviar spam, ou realizar atividades maliciosas em larga escala.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Malwares

Backdoor: permite o acesso de um invasor a um computador comprometido contornando a autenticação. A partir daí, ele pode ser usado para obter acesso a informações privilegiadas, excluir dados em discos rígidos, instalar outros *software* ou transferir informações.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Malwares

Rootkit é um *malware* projetado para se esconder dentro de um sistema e dar acesso privilegiado (geralmente nível de administrador ou "*root*") a um invasor, sem que o usuário perceba. Ele atua de forma invisível e pode desativar antivírus, modificar o sistema operacional e monitorar tudo o que acontece no computador. O cibercriminoso pode ter controle remoto total do computador.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Malwares

Stalkerware é *software* malicioso projetado para monitorar e rastrear as atividades de um usuário em um dispositivo, normalmente celular. Ele pode coletar informações detalhadas sobre as atividades de um usuário, incluindo mensagens de texto, chamadas telefônicas, histórico de navegação, localização GPS, fotos e vídeos.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

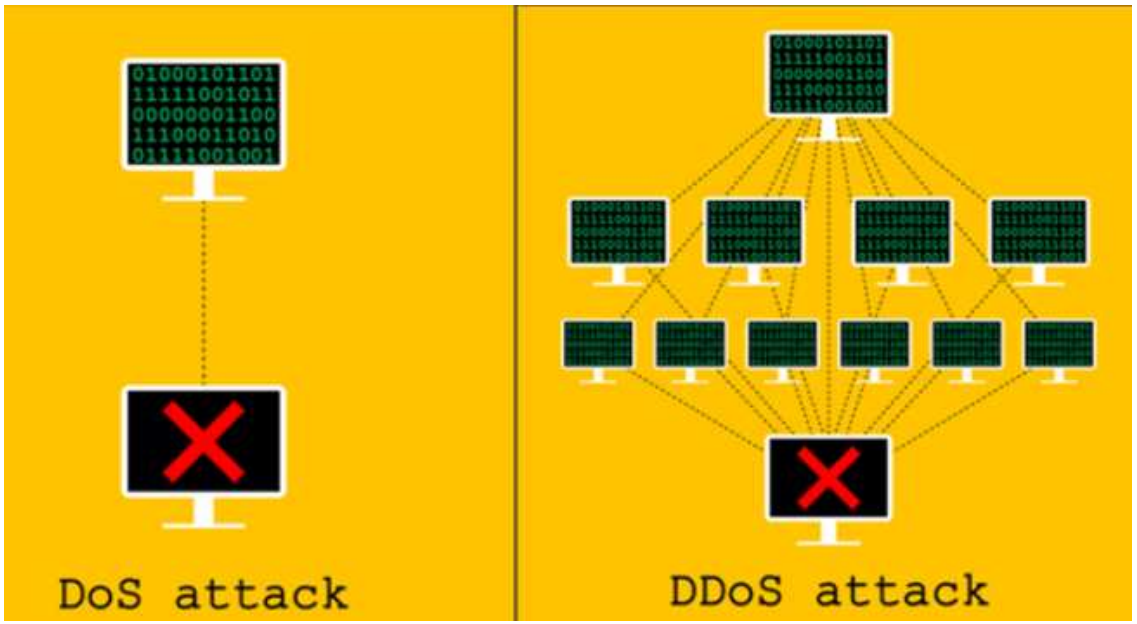
Negação de Serviço

Um ataque de Negação de Serviço (DoS), ou *Denial of Service*, é uma ação maliciosa com o objetivo de tornar um sistema, serviço ou rede indisponível para os usuários legítimos. Isso é feito geralmente sobrecarregando os recursos do sistema, como processamento, memória, largura de banda ou conexões simultâneas. Por exemplo, imagine um site com capacidade para 1.000 acessos por minuto. Um atacante envia 500.000 requisições falsas de uma vez, impedindo que usuários reais consigam entrar.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

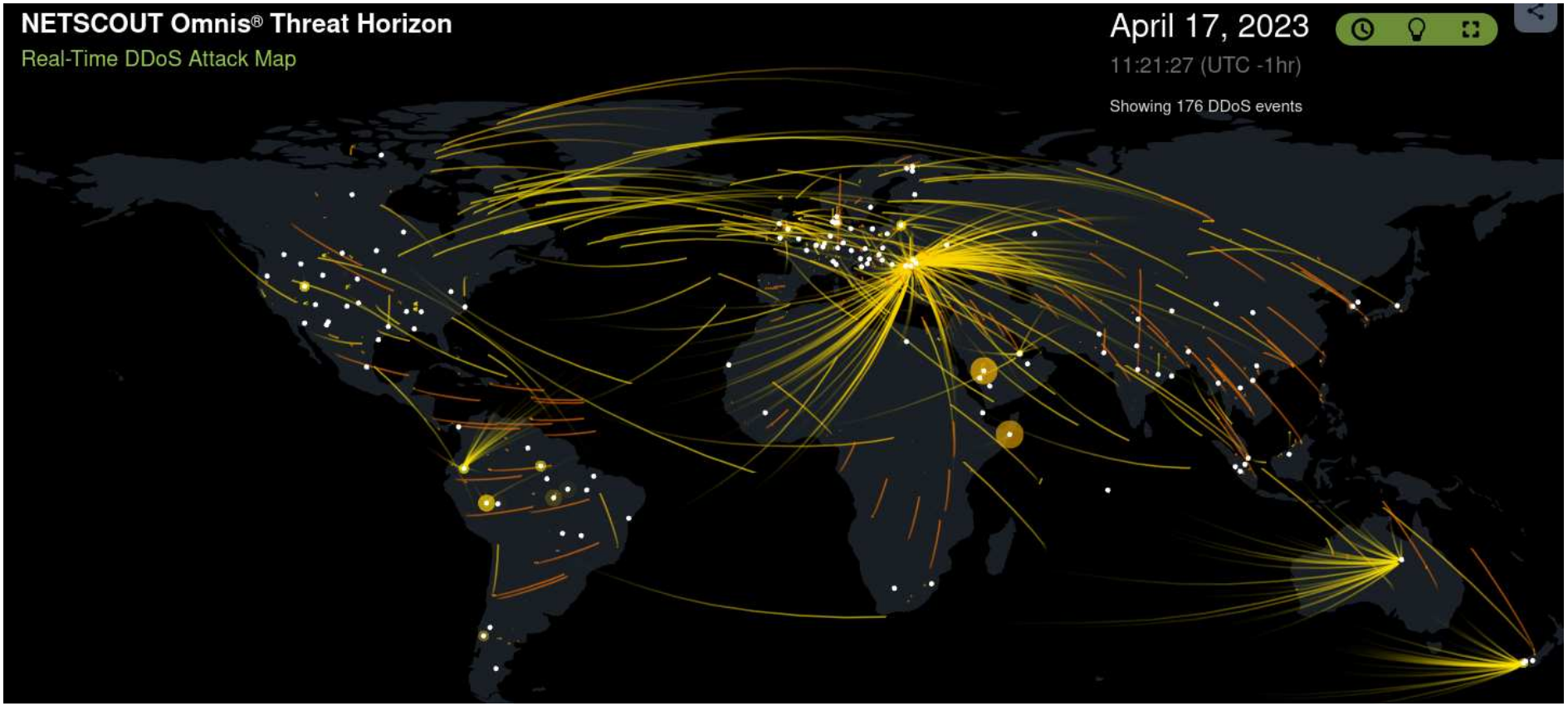
Negação de Serviço

Ataque de Negação de Serviço pode ser distribuído (DDoS) sendo realizado a partir de múltiplos dispositivos coordenados, tornando-o mais difícil de ser parado. Botnets são frequentemente usadas para realizar ataques DDoS.



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Negação de Serviço (DoS e DDoS)



https://horizon.netscout.com/

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Desfiguração de Página (*Defacement*)

Ataque de desfiguração é um tipo de ataque no qual um invasor altera o conteúdo de uma página da web para exibir mensagens, imagens ou informações maliciosas. O atacante altera a aparência visual da página, muitas vezes com o objetivo de transmitir uma mensagem política, social ou simplesmente para causar danos à reputação do site ou da organização.

O ataque geralmente ocorre quando o invasor consegue obter acesso não autorizado ao servidor web que hospeda a página alvo. Isso pode ser feito por meio de vulnerabilidades de segurança no servidor, como falhas de configuração, *software* desatualizado ou senhas fracas.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

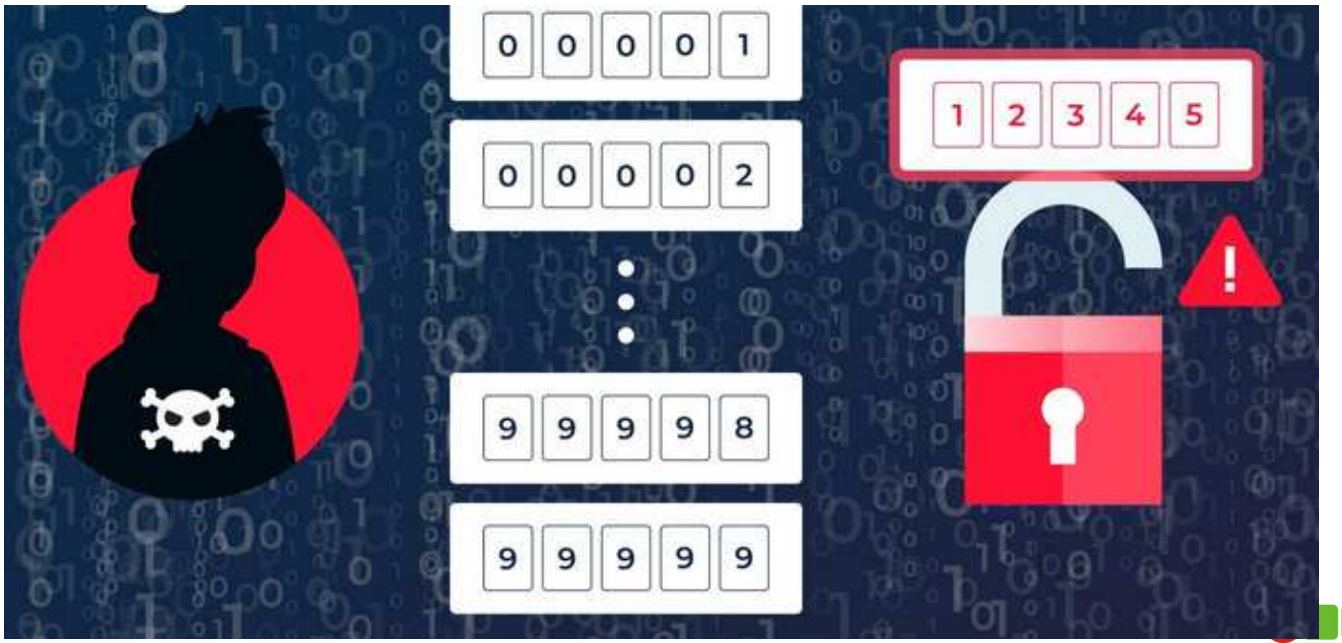
Força Bruta

O ataque de força bruta é uma técnica que visa descobrir uma senha ou chave secreta ao tentar sistematicamente todas as combinações possíveis. Por exemplo, o atacante realiza repetidas tentativas de login ou autenticação, testando diferentes combinações de senhas, até encontrar a correta. Além de tentativas aleatórias, os atacantes podem usar dicionários de senhas, que são listas predefinidas de palavras comuns, sequências numéricas, ou outras combinações conhecidas.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Força Bruta

Esse método é direto e geralmente requer um grande número de tentativas, mas pode ser eficaz, especialmente contra senhas mais fracas ou mal protegidas.



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Varredura em Rede (*Scan*)

A varredura em Rede é uma técnica que consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados, sistemas operacionais e programas instalados. Esse tipo de ataque é frequentemente usado como parte de uma fase de reconhecimento em um ataque mais amplo, permitindo que os invasores identifiquem alvos potenciais e explorem possíveis vulnerabilidades. O principal *software* utilizado neste fase é o Nmap.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Interceptação de tráfego (*Sniffing*)

Interceptação de tráfego é uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de *sniffers*, por exemplo Wireshark. Atacantes podem capturar informações sensíveis, como senhas, números de cartão de crédito e o conteúdo de arquivos confidenciais que estejam trafegando por meio de conexões inseguras, ou seja, sem criptografia.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Trashing

Também chamado de dumpsterdiving, nele os atacantes procuram informações nos lixos das empresas ou das casas das pessoas a serem atacadas, como por exemplo, nomes de usuários e senhas, informações pessoais e confidenciais.Também são buscadas outras informações, como: organogramas, impressões de códigos fonte, inventário de *hardware*, topologia.

Esta técnica é considerada legal, uma vez que estas informações foram recuperadas do lixo por terem sido consideradas sem qualquer valor pela empresa ou pessoa alvo.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Engenharia Social

O ataque de engenharia social é uma técnica psicológica que visa manipular ou ludibriar pessoas para obter informações confidenciais, acesso a sistemas ou induzi-las a realizar ações específicas que beneficiem o atacante. Os ataques exploram a natureza humana e buscam enganar as vítimas por meio de manipulação psicológica. Isso pode incluir o uso de persuasão, intimidação, simpatia ou autoridade falsa.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Engenharia Social

Os atacantes podem: se fazer passar por colegas de trabalho, autoridades, amigos ou prestadores de serviços confiáveis; criar identidades falsas online ou por telefone para ganhar a confiança da vítima; criar perfis falsos em redes sociais, uso de e-mails falsos ou chamadas telefônicas com identidade falsificada; envolver situações de emergência, benefícios inesperados, prêmios falsos, entre outros.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Engenharia Social – Phishing

Os ataques de phishing são uma forma comum de engenharia social, onde os atacantes enviam e-mails ou mensagens de WhatsApp falsas, muitas vezes parecendo legítimas, para induzir as vítimas a clicarem em links maliciosos, fornecerem informações pessoais ou realizar ações prejudiciais.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Spoofing de IP, MAC, DNS e E-mail

Spoofing, em geral, refere-se à prática de falsificar informações em pacotes de dados, cabeçalhos ou outros tipos de comunicação para mascarar a verdadeira identidade do remetente. Os principais são:

- Spoofing de IP: o invasor falsifica o endereço IP de origem em um pacote IP para fazer parecer que o pacote foi enviado de um local diferente.
- Spoofing de MAC: o invasor falsifica o endereço MAC de um dispositivo para se passar por outro dispositivo na rede.
- Spoofing de DNS: o invasor falsifica informações no sistema de nomes de domínio para redirecionar os usuários para sites maliciosos ou falsos.
- Spoofing de E-mail: envolve o envio de e-mails falsificados que parecem ser de uma fonte legítima, como um banco ou uma empresa conhecida.

Dúvidas

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE