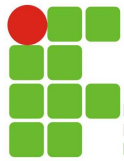
Segurança de Redes

Curso Superior de Tecnologia em Redes de Computadores
Prof. Macêdo Firmino

Introdução à Segurança da Informação



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

Introdução

O que é Informação?

É tudo que tem valor para a organização e para as pessoas.

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

Introdução

Onde está a informação?

Papel, arquivos, banco de dados e na memória das pessoas.

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

Introdução

Por que proporcionar segurança para a informação?

Para garantir que os valores da instituição e/ou pessoas naõ sejam descobertas, manipuladas ou perdidas.

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

Segurança da informação

Trata-se de técnicas de proteção oferecida a um sistema de informação automatizado para atingir os objetivos apropriados de preservação da integridade, disponibilidade e confidencialidade de ativos de sistemas de informação (incluindo *hardware*, *software*, *firmware*, informações/dados e telecomunicações).

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

Confidencialidade

Assegurar que informações privadas e confidenciais não estejam disponíveis nem sejam reveladas para indivíduos não autorizados.

Integridade

Prevenir-se contra a modificação ou destruição imprópria de informação.

Disponibilidade

Assegurar acesso e uso rápido e confiável da informação, ou seja, garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.

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

Autenticidade

Verificar que os usuários são quem dizem ser (garantia da identidade dos participantes da comunicação) e, além disso, que cada entrada no sistema vem de uma fonte confiável.

Responsabilização ou não repúdio

Garantir que as ações de uma entidade sejam atribuídas exclusivamente a ela, ou seja, um agente não consiga negar uma ação que criou ou modificou uma informação.

Auditoria

Permitir o rastreamento do histórico dos fatos de um evento assim como a identificação dos envolvidos.

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

Segurança de Redes

Um conjunto de conceitos, normas, práticas, procedimentos, posturas a serem seguidos pelos profissionais que atuem nesta área da Tecnologia da Informação para garantir a segurança da informação .

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

Ameaça

Uma chance de violação da segurança que existe quando há uma circunstância, capacidade, ação ou evento que poderia quebrar a segurança e causar danos. ou seja, uma ameaça é um possível perigo a explorar uma vulnerabilidade.

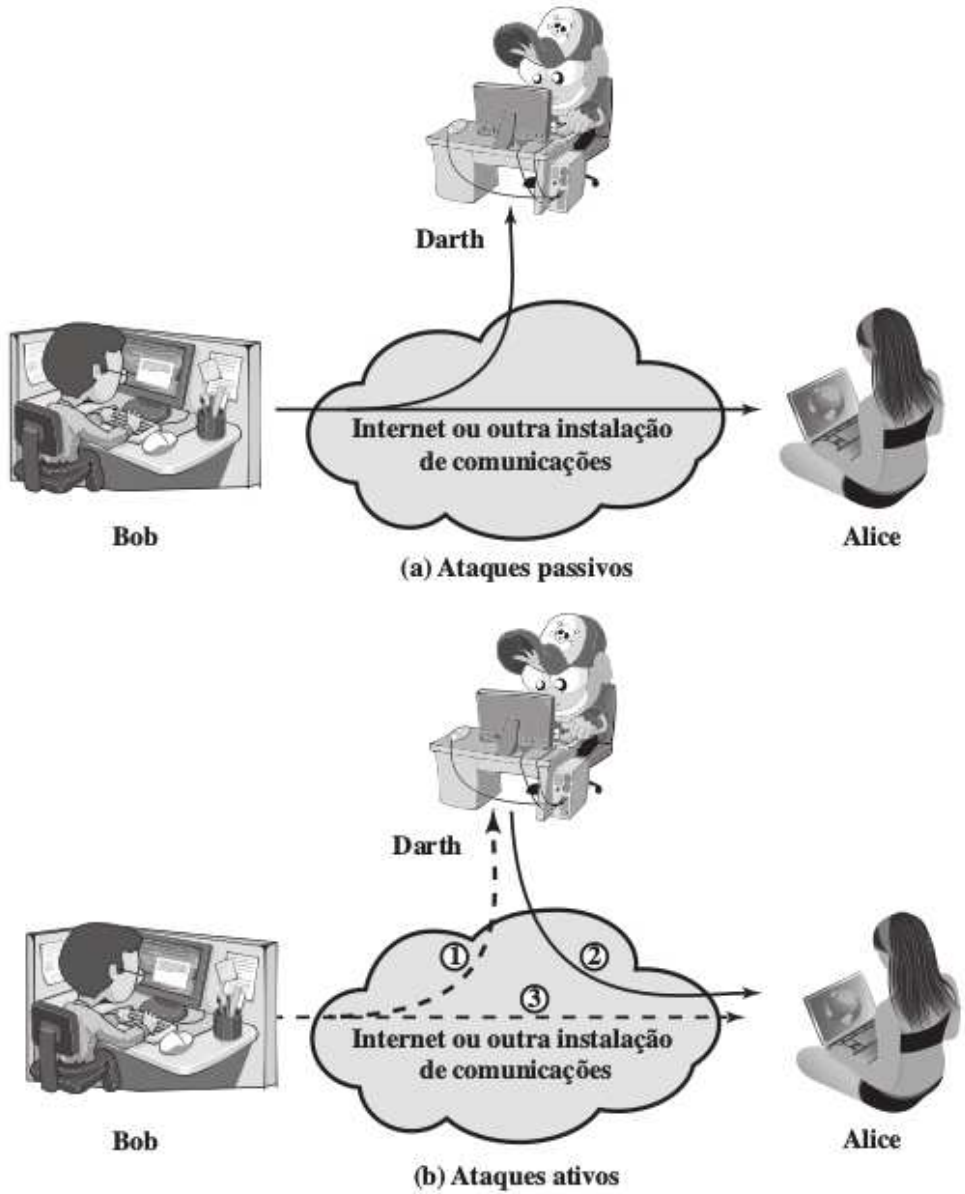
Vulnerabilidade

É uma fraqueza de um ou mais elementos de um sistema que podem ser explorados por um atacante afetando o funcionamento, operação, disponibilidade ou integridade dos dados de uma rede ou sistema.

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

Ataque

É qualquer ação que comprometa a segurança da informação pertencida a uma organização. Ela 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

Principais Ataques

- Códigos maliciosos (*Malware*):
  - Vírus;
  - *Worms*;
  - Bot e *botnet*;
  - *Trojans*);
  - *Spywares*;
  - *Backdoor*.
- Varredura em redes (*Scan*);
- Falsificação de e-mail (E-mail *spoofing*);
- Interceptação de tráfego (*Sniffing*);
- Força bruta (*Brute force*);
- Desfiguração de página (*Defacement*);
- Negação de serviço (DoS e DDoS).

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

Malware

Códigos maliciosos são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Algumas das formas como eles podem infectar ou comprometer um computador são:

- pela exploração de vulnerabilidades existentes nos programas;
- pela auto-execução de mídias removíveis infectadas, como pen-drives;
- pelo acesso a páginas Web maliciosas;
- pela ação direta de atacantes que, invadem o computador e incluem arquivos contendo códigos maliciosos;
- pela execução de arquivos previamente infectados.

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

Malware

Um *malware* pode provocar:

- Perda de desempenho do micro, exclusão de arquivos e alteração de dados;
- Acesso a informações confidenciais por pessoas não autorizadas;
- Perda de desempenho da rede (intranet e internet);
- Desconfiguração do Sistema Operacional.

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

Malware

Os principais motivos que levam um atacante a desenvolver e a propagar códigos maliciosos são a obtenção de vantagens financeiras, a coleta de informações confidenciais, o desejo de autopromoção e o vandalismo. Além disto, os códigos maliciosos são muitas vezes usados como intermediários e possibilitam a prática de golpes, a realização de ataques e a disseminação de *spam*.

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

Vírus

É um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos. Para que possa se tornar ativo, o vírus depende da execução do programa ou arquivo hospedeiro.

Apesar de existirem vírus para outros Sistemas Operacionais (Linux, MacOS e Android), essa quantidade é infinitamente menor, quando comparamos com a quantidade de vírus do sistema Windows.

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

Vírus

Brain foi considerado o primeiro vírus (1986), era da classe dos Vírus de *Boot*, ou seja, danificava o setor de inicialização do disco rígido o disco rígido, e sua propagação era através de um disquete, quando o *boot* ocorria, ele se transferia para o endereço da memória da Bios que o automaticamente o executava.

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

Vírus

Jerusalem, também conhecido como Sexta-feira 13, em 1987, afetou muitos países, universidades, instituições e empresas de todo o mundo, infectando milhares de computadores. Na sexta-feira 13, o vírus apagava todos os arquivos executáveis no disco rígido infectado.

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

Vírus

Conficker bloqueia o acesso a *websites* destinados à venda de produtos de sistemas de segurança. Em janeiro de 2009, o número estimado de computadores infectados variou entre 9 e 15 milhões. A rede de computadores da Marinha da França foi infectada pelo Conficker, forçando a permanência de aeronaves em várias bases aéreas militares. O Ministério da Defesa do Reino Unido disse que alguns de seus maiores sistemas e computadores foram infectados pelo vírus, além de computadores em vários navios de guerra e submarinos da Marinha Real. Computadores de hospitais, governos (legislativo, executivo, judiciário) e milhares empresas foram infectados.

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

Vírus

Chernobyl é um dos vírus mais nocivos que já existiu. Ele corrompia a BIOS e o MBR (*Master Boot Record*) dos sistemas infectados. Dessa forma, os computadores não inicializavam. Estima-se que 60 milhões de computadores foram infectado pelo vírus, resultando em cerca de US $ 1 bilhão de dólares em prejuízos.

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

Vírus

Ransomware é um tipo de vírus que sequestra os dados do computador e exige um resgate para liberá-las. Os hackers mantém os dados do computador invadido criptografados, de forma que o dono não consiga acessá-los, a menos que eles liberem. Ele é considerado um dos tipos mais prejudiciais de *malwares*, uma vez que pode levar a perdas de enormes quantias de dinheiro (em caso de empresas, por exemplo) ou destruição de dados pessoais importantes.

Em 2017, um ransomware chamado de WannaCry infectou mais de 10.000 organizações e 200.000 pessoas em mais de 150 países.

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

Worm

Worm é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o *worm* não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores.

Worms são notadamente responsáveis por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo que costumam propagar e, como consequência, podem afetar o desempenho de redes e a utilização de computadores.

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

Worm

O processo de propagação e infecção dos *worms* ocorre da seguinte maneira:

- Identificação dos computadores alvos, o que pode ser feito por exemplo, efetuando varredura na rede;
- Envio das cópias: por exemplo, como parte da exploração de vulnerabilidades existentes em programas instalados no computador alvo ou anexadas a e-mails.
- Ativação das cópias: o *worm* necessita ser executado para que a infecção ocorra, o que pode acontecer por exemplo, a inserção de uma mídia removível.

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

Worm

Morris, em 1988, infectou mais de 6.000 computadores nos EUA rodando Unix, incluindo alguns da NASA. Robert Morris, estudante da Universidade Cornell (EUA), diz que o criou para saber o tamanho da internet. (Ele foi condenado na Justiça a pagar US$ 10.000.). O worm causou até US$ 100 milhões em danos.

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

Worm

Code Red e *Code Red* II, exploravam a vulnerabilidade encontrada em máquinas que possuíam Windows 2000 e o Windows NT. Ele usava como brecha um problema de sobrecarga do *buffer*, quando um PC equipado com estes sistemas operacionais recebiam mais informações do que tinham capacidade para processar. Com isso, ele começava a sobrescrever a memória adjacente. O *Code Red* ficou famoso por ter afetado PCs da Casa Branca com um ataque de negação de serviço distribuída (DDoS). O dano que ele causou foi estimado em US$ 2 bilhões.

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

Worm

O MyDoom foi o worm que se espalhou mais rápido por e-mail na época em que surgiu. Estima-se que ele reduziu a velocidade global da internet em 10: Ele aproveitou buracos no Outlook (gerenciador de e-mails) e invade o catálogo de endereços do usuário, usando os que encontra para se auto-enviar a todos os endereços da lista. Os computadores foram programados para lançar ataques aos sites da Microsoft e de uma empresas de segurança em informática no dia 1º de fevereiro.

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

Bot e Botnet

Bot é um programa malicioso que dispõe de mecanismos de comunicação com o invasor e permite que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do *worm*, ou seja, é capaz de se propagar automaticamente. A comunicação entre o invasor e o computador infectado pode ocorrer via canais de IRC, servidores *Web* e redes do tipo P2P, entre outros meios. Ao se comunicar, o invasor pode enviar instruções para que ações maliciosas sejam executadas, como desferir ataques, furtar dados do computador infectado e enviar *spam*.

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

Bot e Botnet

Um computador infectado por um *bot* costuma ser chamado de zumbi (*zombie computer*), pois pode ser controlado remotamente, sem o conhecimento do seu dono.

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

Bot e Botnet

Botnet é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos *bots*. Quanto mais zumbis participarem da botnet mais potente ela será. Algumas das ações maliciosas que costumam ser executadas por intermédio de *botnets* são: ataques de negação de serviço, propagação de códigos maliciosos (inclusive do próprio *bot*), coleta de informações de um grande número de computadores, envio de *spam* e camuflagem da identidade do atacante.

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

Bot e Botnet

Funcionamento

- Um atacante propaga um tipo específico de bot na esperança de infectar e conseguir a maior quantidade possível de zumbis;
- Os zumbis ficam então à disposição do atacante, agora seu controlador, à espera dos comandos a serem executados;
- Quando o controlador deseja que uma ação seja realizada, ele envia aos zumbis os comandos a serem executados, usando, por exemplo, redes do tipo P2P ou servidores centralizados;
- Os zumbis executam então os comandos recebidos, durante o período predeterminado pelo controlador;
- Quando a ação se encerra, os zumbis voltam a ficar à espera dos próximos comandos a serem executados.

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

Bot e Botnet

Um exemplo de bot é chamada Geinimi. Ele foi desenvolvido para a plataforma móvel Android. O Geinimi é instalado em *smartphones* junto com *games* adulterados, que podem ser encontrados em sites. O *malware* se comunica com um servidor central, que pode, remotamente, enviar comandos para um celular, como baixar ou desinstalar um *software*. Entre os dados enviados estão a localização do dispositivo e detalhes do *hardware*, como o número do cartão SIM e uma lista com todos os aplicativos instalados.

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

Spyware

É um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Pode ser usado tanto de forma legítima quanto maliciosa, dependendo de como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas.

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

Spyware

keylogger: captura e armazena as teclas digitadas pelo usuário no teclado do computador. Sua ativação, em muitos casos, é condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de *Internet Banking*.

Screenlogger: capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado.

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

Spyware

Adware: projetado especificamente para apresentar propagandas. Pode ser usado para fins maliciosos, quando as propagandas apresentadas são direcionadas, de acordo com a navegação do usuário e sem que este saiba que tal monitoramento está sendo feito.

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

Backdoor

Backdoor é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim. Pode ser incluído pela ação de outros códigos maliciosos, que tenham previamente infectado o computador, ou por atacantes, que exploram vulnerabilidades existentes nos programas instalados no computador para invadi-lo.

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

Cavalo de troia (*Trojan*)

É um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário. Exemplos de *trojans* são programas que você recebe ou obtém de sites na Internet e que parecem ser apenas cartões virtuais animados, álbuns de fotos, jogos e protetores de tela, entre outros. Estes programas, geralmente, consistem de um único arquivo e necessitam ser explicitamente executados para que sejam instalados no computador.

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

Varredura em Rede (*Scan*)

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 e programas instalados. Com base nas informações coletadas é possível associar possíveis vulnerabilidades aos serviços disponibilizados e aos programas instalados nos computadores ativos detectados.

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

Falsificação de e-mail (*E-mail spoofing*)

É uma técnica que consiste em alterar campos do cabeçalho de um e-mail, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.

Ataques deste tipo são bastante usados para propagação de códigos maliciosos e envio de spam. Atacantes utilizam-se de endereços de e-mail coletados de computadores infectados para enviar mensagens e tentar fazer com que os seus destinatários acreditem que elas partiram de pessoas conhecidas.

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

Interceptação de tráfego (*Sniffing*)

É uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de *sniffers*. 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

Força bruta (*Brute force*)

Consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios deste usuário.

Mesmo que o atacante não consiga descobrir a sua senha, você pode ter problemas ao acessar a sua conta caso ela tenha sofrido um ataque de força bruta, pois muitos sistemas bloqueiam as contas quando várias tentativas de acesso sem sucesso são realizadas.

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

Força bruta (*Brute force*)

As tentativas de adivinhação costumam ser baseadas em:

- dicionários de diferentes idiomas e que podem ser facilmente obtidos na Internet;
- listas de palavras comumente usadas, como personagens de filmes e nomes de times de futebol;
- substituições óbvias de caracteres, como trocar "a" por "@" e "o" por "0";
- sequências numéricas e de teclado, como "123456", "qwert" e "1qaz2wsx";
- informações pessoais, de conhecimento prévio do atacante ou coletadas na Internet em redes sociais e blogs, como nome, sobrenome, datas e números de documentos.

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

Desfiguração de página (*Defacement*)

É uma técnica que consiste em alterar o conteúdo da página Web de um site. As principais formas que um atacante, pode utilizar para desfigurar uma página Web são:

- explorar erros da aplicação Web;
- explorar vulnerabilidades do servidor de aplicação Web;
- explorar vulnerabilidades da linguagem de programação ou dos pacotes utilizados no desenvolvimento da aplicação Web;
- invadir o servidor onde a aplicação Web está hospedada e alterar diretamente os arquivos que compõem o site;
- furtar senhas de acesso à interface Web usada para administração remota.

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

Negação de serviço (DoS e DDoS)

Negação de serviço, ou DoS (*Denial of Service*), é uma técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Quando utilizada de forma coordenada e distribuída, ou seja, quando um conjunto de computadores é utilizado no ataque, recebe o nome de negação de serviço distribuído, ou DDoS (*Distributed Denial of Service*).

O objetivo destes ataques não é invadir e nem coletar informações, mas sim exaurir recursos e causar indisponibilidades ao alvo. Quando isto ocorre, todas as pessoas que dependem dos recursos afetados são prejudicadas, pois ficam impossibilitadas de acessar ou realizar as operações desejadas.

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

Ataque Físico

Este tipo de ataque é obtido quando um hacker consegue ter acesso físico ao seu ambiente de rede e obtêm alguma informação valiosa ou danificar equipamentos.

Para se proteger deste tipo de ataque você deve impedir, restringir ou controlar o acesso a determinados ambientes de sua rede. Uma forma de garantir isso é através do uso de crachás de identificação, documentos de identidade, câmeras de vídeo, etc.

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

Engenharia Social

O atacante começa com o levantamento de informações sobre as pessoas que ele deseja retirar alguma informação, como por exemplo, o nome e a função da pessoa. Ele muitas vezes usa jornais, revistas ou o próprio site da empresa para obter estas informações.

Após adquirir estas informações, o hacker pode fazer uma ligação para alguém da empresa, apresentar-se como colega de outra pessoa e no meio da conversa solicitar alguma informação valiosa que poderá ser útil em um possível ataque.

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

Dumpsterdiving ou trashing

OS atacantes procuram informações nos lixos das empresas 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 alvo.

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

Hacker, cracker e outros personagens

Quem são as pessoas que fazem os ataques?

- Um *hacker* é apenas uma pessoa que detém muitos conhecimentos sobre a área de compu- tação. Em geral, são pessoas interessadas em Sistemas Operacionais, *softwares*, segurança, internet e programação. Um *hacker* tem interesse em descobrir coisas novas (inclusive vulnerabilidades em programas), mas não possui nenhuma motivação destrutiva.
- Cracker: é um *hacker* com propósitos maldosos de invadir e violar a integridade de sistemas.
- *Script kiddies* ou *Lammer*: com pouco conhecimento de informática, usam *exploits* criados pelo *cracker* e executam ataques na internet.

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

Atividade

01. Para verificar as portas que estão abertas na máquina:
    - Windows: netstat
    - Linux: sudo netstat -t
02. O que são *malwares*? Cite exemplos de *malwares*.
03. Observe no site: `https://www.garykessler.net/library/bad_ports.html` algumas portas usadas por *malwares*.
04. Acesse o site `https://cybermap.kaspersky.com/stats` e observe em tempo real as estatísticas de ataques. Observe as estatísticas no Brasil na ultima semana. Qual foi o malware mais disseminado no Brasil nesse período?

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