Ameaças e Ataques

Segurança e Auditoria em Sistemas

Profa. Natássya Barlate Floro da Silva

Universidade Tecnológica Federal do Paraná — Câmpus Cornélio Procópio

09 de Março de 2020

Roteiro

Introdução

- Ameaça: uma chance de violação da segurança que poderia quebrar a segurança e causar danos. Pode ser uma ação ou evento.
- Vulnerabilidade: condição que pode causar uma violação de segurança, ou seja, fraqueza inerente de um elemento do sistema.
- Ataque: ato inteligente e deliberado de violar a política de segurança de um sistema.
- Contramedida: técnicas e métodos usados para se defender de ataques ou para evitar e compensar vulnerabilidades.

Introdução

- Atacantes exploram vulnerabilidades para obter acesso a informações confidenciais ou comprometerem recursos dos sistemas.
- Muitas ameaças estão vinculadas ao uso de programas que exploram vulnerabilidades dos sistemas: *Malicious software* ou **Malwares**.

Tipos de Ataques

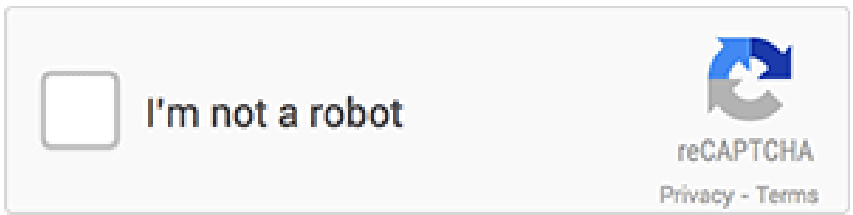
- Força Bruta, Dicionário e *Rainbow Tables*;
- *Phishing*;
- *Packet Sniffing*;
- *Scanning*;
- *Spoofing*;
- Engenharia Social;
- DoS e DDoS.

Ataque Força Bruta

- Consiste na tentativa de cada chave/senha possível até que se obtenha a mensagem decifrada ou o acesso ao sistema.
- Na detecção de mensagens é necessário automatizar o reconhecimento da mensagem decifrada.
- Contramedida: adicionar tempo de atraso ou limite de tentativas após falhas de acesso e uso de CAPTCHAS (**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part).

Ataque de Dicionário

- Consiste na tentativa de se obter uma senha a partir de uma lista predefinida, como a lista de palavras de um dicionário.
- A lista pode ser construída a partir de dados do usuário, como nomes, datas, telefones e outros.
- Contramedida: adicionar tempo de atraso ou limite de tentativas após falhas de acesso e uso de CAPTCHAS (**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part).



Ataque de *Rainbow Table*

- Senhas não podem ser enviadas pela rede como texto plano. A maioria dos sistemas, enviam o *hash* da senha para autenticação no servidor.
- *Rainbow Table*: é uma tabela pré-computada que possui os valores de *hash* de possíveis senhas.
- No ataque *Rainbow Table*, os valores dos *hashs* capturados são comparados com os valores das tabelas para se descobrir a senha original.
- Maior uso de armazenamento e menor uso de processamento.
- Contramedida: funções *hash* com *sal* (*salt*). O *salt* é um valor aleatório que é processado juntamente com a senha e permite que senhas iguais gerem valores de *hash* diferentes.

Phishing

- Envio de mensagens não solicitadas que procura induzir o acesso a páginas fraudulentas projetadas para furtar dados confidenciais do usuário. Geralmente tenta se passar por uma instituição conhecida.
- Principais situações:
  - Mensagens que contém links para acesso de programas maliciosos;
  - Páginas falsas de comércio eletrônico ou de Internet Banking;
  - E-mails contendo formulários para o fornecimento de informações;
  - Comprometimento do serviço de resolução de nomes (DNS).

Phishing

- Contramedidas:
  - Educação dos usuários;
  - Uso de filtros de e-mails (identificação de SPAM);
  - Uso de HTTPS;
  - Identificação de sites maliciosos.
- Catálogo de Fraudes da RNP:
  `https://catalogodefraudes.rnp.br/`

Packet Sniffing

- Também conhecido como *eavesdropping*.
- Consiste no monitoramento e captura dos pacotes do tráfego de uma rede.
- Muitas vezes é usada de forma legítima por administradores de rede para solucionar problemas da rede.
- Usado por atacantes para obter informações confidenciais, como dados de contas e senhas.

Packet Sniffing

- **Sniffer**: dispositivo ou programa utilizado para capturar e armazenar dados trafegando em uma rede.
- Exemplos:
  - Tcpdump;
  - Wireshark;
  - PRTG Network Monitor.
- *Passive Sniffing*: geralmente os dados capturados são os que estão disponíveis na placa de rede.
- *Active Sniffing*: quando a rede é manipulada para que o atacante tenha acesso a outros pacotes da rede.

Packet Sniffing

- Contramedidas:
  - Criptografia para garantir confidencialidade;
  - Restringir acesso físico;
  - Uso de *switches*.

Scanning

- Procedimentos para identificar *hosts*, portas, serviços, sistemas operacionais, arquiteturas, aplicações e possíveis vulnerabilidades dos elementos que compõem uma rede.
- Tipos:
  - *Port Scanning*: detecção de portas e serviços.
  - *Network Scanning*: detecção de endereços IP, detalhes do SO, roteadores e topologias.
  - *Vulnerabilities Scanning*: busca por vulnerabilidades e fraquezas do sistema.

Scanning

- *Nmap* (*Network Mapper*): principal ferramenta usada para coletar informações da rede.
- Exemplos de uso:
  - Busca por portas TCP abertas: nmap -v -p- <TargetIP>.
  - Busca por portas TCP abertas e SOs em uma subrede: sudo nmap -sS <TargetIP>/<Mask>.
  - Busca por portas TCP abertas utilizando-se de outra máquina para o *scanning*: sudo nmap -Pn -sI <ZombieIP> <TargetIP>.

Scanning

- Contramedidas:
  - *Firewall*: restringir mensagens ICMP e configurar para identificar *port scan*.

Spoofing

- Ataque em que um usuário malicioso se mascara como um usuário legítimo do sistema.
- Tipos:
  - *E-mail Spoofing*: atacante se passa por outro ao alterar o campo "From" do SMTP. Usado para SPAM.
  - *IP Spoofing*.
  - *ARP Spoofing*.
  - *DNS Spoofing*.

IP Spoofing

- Atacante altera o endereço de origem dos pacotes IP.
- Usado para serviços que utilizam uma autenticação baseada em endereços IP:
  - Após um usuário autorizado se autenticar, o servidor considera seu endereço IP como confiável.
  - Atacante utiliza o endereço IP do usuário autorizado para conseguir acesso ao serviço.
  - Porém, não é suficiente em conexões TCP em andamento devido à dificuldade de sincronização do número de sequência.

IP Spoofing

- Também pode ser usado para iniciar ataques DDoS:
  - Atacante envia pacotes para múltiplos nós com o IP de origem do alvo.
  - O alvo acaba sendo sobrecarregado com as respostas dos nós.

ARP Spoofing

- Protocolo ARP provê a tradução de endereços MAC para endereços IP.
- Atacante altera o endereço de origem MAC dos quadros, atualizando a tabela ARP com o IP do atacante.
- Atacante passa a receber os quadros destinados ao usuário original.

DNS Spoofing

- Também conhecido por envenenamento de DNS.
- Alteração dos endereços IPs que estão mapeados para sites legítimos de servidores DNS ou da cache local de DNS.
- Geralmente redirecionam para sites que disseminam *malwares*.

Spoofing

- Contramedidas:
  - Uso de protocolos que realizam a autenticação no recebimento de pacotes, como TSL e SSH.
  - *Firewall*: podem detectar pacotes com IPs da rede interna vindo da rede externa.

Engenharia Social

- Uso da persuasão, explorando a ingenuidade ou confiança de um usuário para se obter informações confidenciais ou acesso não autorizado a sistemas.
- Exemplos:
  - Atacantes que se passam por outras pessoas de maior autoridade.
  - Mensagens que alegam que o dispositivo do usuário foi infectado com um *malware*.
  - Uso de relacionamentos pessoais com funcionários para se obter informações do sistema computacional de uma empresa.
  - Atacantes internos: funcionários descontentes que roubam informações confidenciais.

Engenharia Social

- Contramedidas:
  - Educação dos usuários.
  - Criação de políticas de segurança.
  - Implantação de controle de acesso.
  - Monitoramento constante.

DoS e *DDoS*

- Ataques de Negação de Serviço, do inglês *Denial of Service* (DoS), são direcionados a serviços, dispositivos ou redes com o intuito de reduzir ou impedir o seu acesso aos usuários legítimos.
- Ataques Distribuídos de Negação de Serviço, do inglês *Distributed Denial of Service* (DDoS), são ataques DoS que partem de múltiplos nós chamados zumbis e que são geralmente máquinas comprometidas.

DoS e *DDoS*

- Exemplos:
  - Inundação da rede com mensagens de requisição ICMP.
  - SYN *flooding*: envio de múltiplos pacotes SYN do estabelecimento de conexão do TCP comprometendo também o processamento de servidores.
  - Fragmentação de pacotes de IP: envio de vários pacotes fragmentados, explorando o custo de processamento para o seu reagrupamento.

DoS e *DDoS*

- Contramedidas:
  - *Firewall*.
  - IDS - Sistema de Detecção de Intrusão.
  - Uso de redundância para balanceamento de carga.

Malwares

- Programas maliciosos que auxiliam atacantes a obter controle de sistemas computacionais ou causar danos aos recursos do sistema.
- Podem modificar ou danificar funcionalidades do sistema, além de obter informações confidenciais.

Tipos de *Malwares*

- Vírus;
- *Worms*;
- *Bots* e *Botnets*;
- *Backdoors*;
- Cavalos de tróia;
- *Keyloggers* e *Screenloggers*;
- *Adwares* e *Spywares*;
- *Ransomwares*.
- *Rootkits*;
- *Exploits*;

Vírus

- Programa capaz de se replicar e infectar outros dispositivos, transmitindo cópias de si mesmo.
- Depende da execução do programa ou arquivo hospedeiro para iniciar suas ações: alterar dados e infectar outros dispositivos.
- Existem atualmente vírus capazes de realizar mutações, reescrevendo seu próprio código e alterando seu comportamento, sendo mais difíceis de serem detectados. Podem ser *polymorphic* (mantém suas funções básicas maliciosas) ou *metamorphic* (tradução e reescrita).

Worms

- Programas capazes de se replicarem de forma independente e infectar outros dispositivos, transmitindo cópias de si mesmos, por meio da exploração de vulnerabilidades do sistema.
- Inicia em um *host* e é capaz de buscar outros nós a partir de uma rede. Não depende de uma ação humana para ser ativado.
- Continua sua retransmissão indefinidamente ou até que uma condição predeterminada seja atingida.
- Assim como o vírus, além de se propagar, pode executar ações maliciosas e prejudicar recursos do sistema infectado.

Bots e *Botnets*

- ***Bots***: programa capaz de se propagar automaticamente, semelhante a um *worm* e que possui mecanismos de comunicação com o invasor.
- Normalmente, se mantém conectado a um servidor de IRC (*Internet Relay Chat*), entra em um canal e aguarda por instruções maliciosas.
- ***Botnets***: redes formadas por nós infectados por *bots*. Podem ser usadas para ataques DDoS.

Backdoors

- Mecanismos que permitem violar checagens de segurança, principalmente para prover acesso não-autorizado.
- A forma mais usual consiste na disponibilização de um novo serviço ou substituição por uma versão alterada, geralmente provendo recursos que permitam o acesso remoto.
- Podem ser falhas inerentes a aplicações ou serem adicionados aos sistemas pelo próprio invasor ou por outros *malwares*, como cavalos de tróia.

Cavalos de Tróia

- Também conhecidos como *Trojans*, são programas que executam ações maliciosas e são incluídos ou disfarçados de arquivos legítimos.
- Normalmente dependem da execução de um arquivo infectado.
- Geralmente incluem também *backdoors*, possibilitando que atacantes tenham acesso à máquina alvo.
- Podem instalar outros *malwares*, realizar furtos de informações confidenciais e prejudicar funcionalidades do sistema.

Keyloggers e *Screenloggers*

- ***Keyloggers***: programas ou dispositivos que registram as teclas acionadas do teclado.
- Existem também no formato de hardware, como um dispositivo colocado entre o cabo do teclado e a interface no computador.
- Por conta deles, instituições financeiras passaram a adotar o uso do teclado virtual.

Keyloggers e *Screenloggers*

- ***Screenloggers***: programas que registram o estado total ou parcial da tela (PrintScreen).
- Ativados por certas condições, como cliques do mouse ou de telas *touchscreens*.
- Usados para a captura de entradas em teclados virtuais.

Adwares e *Spywares*

- ***Adwares*** (*Advertising Softwares*): programas projetados para apresentar propaganda. Geralmente exibem um número excessivo de propaganda sem a permissão do usuário na forma de *pop-up* na Web ou com redirecionamento.
- ***Spywares***: programas que monitora, atividades de um sistema e enviam as informações coletadas a um terceiro.
- Podem ser usados de forma legítima, mas na maioria das vezes são usados de forma dissimulada, não autorizada e maliciosa.

Adwares e *Spywares*

- Funcionalidades:
  - Alteração da página inicial do navegador do usuário;
  - Monitoramento de URLs acessadas;
  - Varredura dos arquivos armazenados;
  - Roubo de informações armazenadas nos *cookies*.
  - Instalação de outros *spywares* ou *adwares*.
  - Instalação de *keyloggers*.

Ransomwares

- Programas que restringem o acesso ao sistema de arquivos de uma máquina, exigindo o pagamento de um resgate para a sua recuperação.
- Tipos:
  - *Scareware*: usa de táticas ameaçadoras, disparando alertas no sistema, alegando a infecção da máquina ou uso ilegal da máquina e induzindo o pagamento para uma falsa solução.
  - *Encrypting ransomware*: atacantes criptografam os arquivos e exigem um pagamento pelos dados decriptografados.

Rootkits

- Conjunto de programas que fornecem mecanismos para o atacante ter acesso ao computador e esconder sua presença.
- Pode ser instalado fisicamente pelo atacante ou de forma remota ao explorar uma vulnerabilidade do sistema.
- São projetados para se manter ocultos, dificultando sua detecção.

Exploits

- Programas que exploram uma vulnerabilidade específica ou um conjunto de vulnerabilidades de um sistema.
- Banco de dados de *exploits*: https://www.exploit-db.com/

- Contramedidas:
  - Não abrir sites ou arquivos suspeitos.
  - Uso de anti-vírus, *anti-adware* e *anti-spyware*.
  - Uso de filtros anti-SPAM.
  - Manter sistemas atualizados.
  - *Firewall*.
  - IDS.

Referências

- STALLINGS, William. Network Security Essentials – Applications and Standards – 4rd Edition, Pearson, 2011.
- Cartilhas CERT: https://cartilha.cert.br/
- Ethical-hacking por GreyCampus: https://www.greycampus.com/opencampus/ethical-hacking/