Tipos de Ataques e Ameaças

Prof.: Thiago H. Bom Conselho
UNATEC- Rede de Computadores

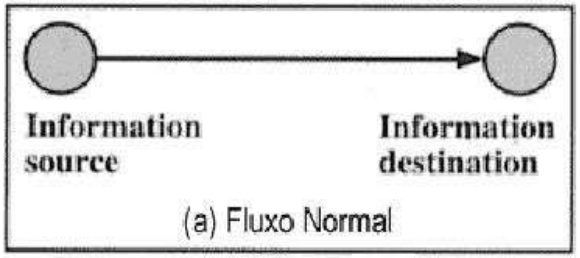
Objetivo do Apresentação

- **Analise e síntese dos principais tipo de ataques e ameaças defrontadas em um sistema de segurança de rede de computadores**

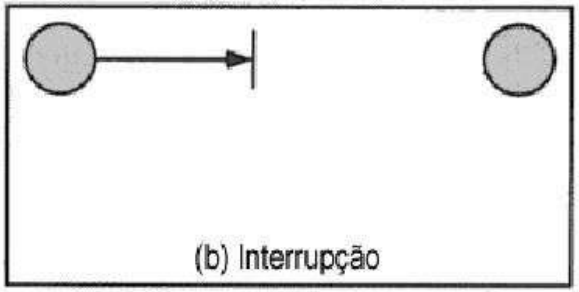
Foco em Vulnerabilidades Principais Origens

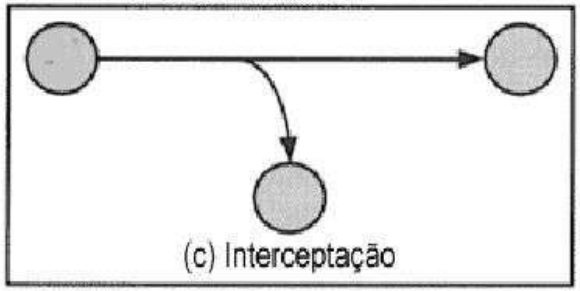
- Deficiência de projeto: hardware ou software.
  - Má proteção física dos equipamentos e mídias.
  - Bugs em software.
- Deficiência de implementação: instalação / configuração incorreta, por inexperiência, falta de treinamento ou negligência.
  - Portas e acessos desbloqueados.
  - Regras de filtros mal implementadas ou mal planejadas.
- Deficiência de gerenciamento: procedimentos inadequados, verificações e monitoramento insuficientes.
  - Interceptação de sinal, grampo, monitoramento
  - Roubo, perda, danificação, desgaste de discos

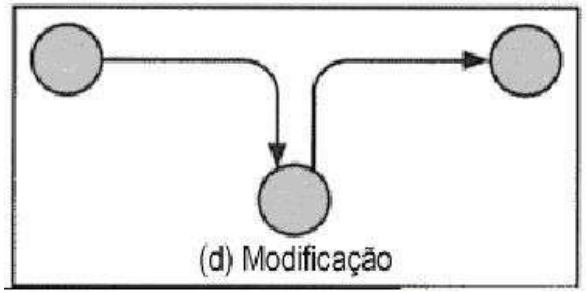
Tipos de Ataques de Segurança

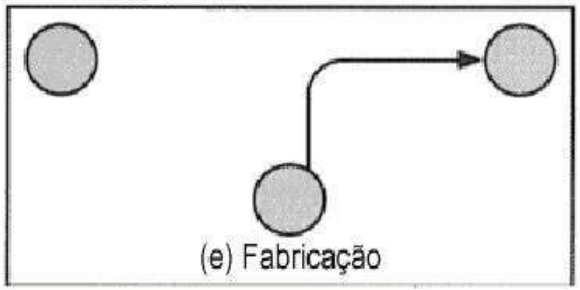


(a) Fluxo Normal


(b) Interrupção


(c) Interceptação


(d) Modificação


(e) Fabricação

Vírus

- Pequenos programas parasitas que infiltram-se em programas funcionais modificando-os, afim de, incluir-se causando alguma forma de dano ao sistema.
- Os danos mais comuns são a lentidão, exclusão total ou parcial de arquivos e inutilização de S.O.
- Ativado juntamente com o software hospedeiro.
- Propaga-se através de arquivos infectados

Worms e Spywares

- Worms constitui-se por um programa autônomo, auto-replicante, semelhante ao funcionamento do vírus, com ressalva a ausência da necessidade de um hospedeiro.
- Em “worms” de redes a replicação acontece através dos meios físico de transmissão.
- Spyware consiste em um software oculto e autônomo, cuja a função é recolher informações sobre/do usuário e transmiti-las sem o conhecimento ou consentimento do mesmo.

Trojan Horses

- Programas que apresentam-se como software legitimo ao usuário, porem funcionando de forma maligna, comumente abrindo as portas TCP.
- Diferenciam-se dos vírus e worms por não criarem réplicas.
- Não existe uma preocupação primordial de auto-preservação após o payload, já que não visam a auto-replicação.

Backdoors

- Forma não documentada de ganhar acesso a um sistema, criada por quem o projetou.
- Pode ser também, ou programa alterado, ou incluído no sistema para permitir acesso privilegiado a alguém

Buffer Overflow

- Sobrecarga intencional da área de memória disponível a variáveis, ou seja técnica de armazenar mais dados que a memória suporta.
- A falha ocorre quando a sobrecarga de uma variável “estoura” a área reservada as demais variáveis.
- Normalmente, esta técnica é utilizada para obter controle do programa atacado e/ou obter privilégios de administrador sobre a maquina atacada.

Exploits

- Pequenos códigos de programas desenvolvidos especialmente para explorar falhas introduzidas em aplicativos por erros involuntários de programação.
- Esses exploits, que podem ser preparados para atacar um sistema local ou remotamente, variam muito quanto à sua forma e poder de ataque. Pelo fato de serem peças de código especialmente preparadas para explorar falhas muito específicas, geralmente há um diferente exploit para cada tipo de aplicativo, para cada tipo de falha ou para cada tipo de sistema operacional.
- Os exploits podem existir como programas executáveis ou, quando usados remotamente, podem estar ocultos, por exemplo, dentro de uma mensagem de correio eletrônico ou dentro de determinado comando de um protocolo de rede.

Password Cracks

- São ataques de “força bruta”, que utilizam programas abastecidos com enormes dicionários de combinações de senhas, testando uma a uma afim de obter a senha correta.
- Devido aos seu dicionário de senhas são programas extremamente lentos.

DoS – Denial of Service

- De acordo com a definição do CERT (**C**omputer **E**mergency **R**esponse **T**eam), os ataques de Negação de Serviços, consistem em tentativas de impedir usuários legítimos de utilizarem um determinado serviço de um computador.
- Tal técnicas consiste em: sobrecarga de uma rede a tal ponto em que os verdadeiros usuários dela não consigam usá-la; derrubar uma conexão entre dois ou mais computadores; fazer tantas requisições a um site até que este não consiga mais ser acessado; negar acesso a um sistema ou a determinados usuários.

Spoofing

- Técnica baseada no mascaramento do numero IP, normalmente utilizando números pertencentes a faixa de IPs inválidos, afim de não ser detectado a origem do ataque.
- Ou seja, técnica de se passar por um outro host afim de obter acesso a um sistema.

Grampo e Phreaking

- Técnicas e procedimentos indevidos sob a utilização do sistema telefônico.
- Atualmente em decadência devido a proteção das operadoras e aos serviços digitais.

Smurf

- Técnica primaria de DoS, que utiliza-se inicialmente de um spoofing, adulteração de IP, seguido de envio rápido e seqüencial de sinais de Ping para endereço de broadcast.
- Tal técnica tem como resultado o flood (inundação) da maquina alvo.
- Para o bom funcionamento da técnica utiliza-se servidores em backbones de altíssima velocidade e banda.

Sniffing

- Técnica de “farejo”, analise, dos dados da rede.
- Utiliza-se de técnicas de captura e analise de dados de uma determinada maquina ou trafego de um rede, sem a autorização ou percepção do usuário.
- Inicialmente desenvolvidas para o gerenciamento de redes.

Key Loggers e Mouse Loggers

- Softwares locais, autônomos e ocultos, cuja função é capturam os dados e informações geradas pelo teclado ou mouse.
- Afim de driblar os teclados virtuais os mouse loggers atuais armazenam parcelas de imagens ao redor do clique ocorrido.
- KeyBanks e KeyCredits

DNS Poisoning ou DNS Spoof

- Ataque ao servidor DNS com o objetivo de redirecionar o numero IP referente a URL a um servidor clandestino com intenções malignas.
- Há de se observar que esta técnica possui alta complexidade devido as proteções aplicadas aos servidores DNS em WAN.

DLL Injection e SQL Injection

- Estas técnicas consistem em utilizar comandos ou recursos SQL ou DLL afim de obter dados confidenciais.
- DLL injection, baseia-se na ocupação de um mesmo espaço de memória de um programa com o objetivo de ter acesso aos dados do mesmo.
- SQL Injection, baseia-se na manipulação de instruções SQL em scripts php ou asp, utilizado largamente em aplicações web.

Scanners

- Ferramentas de varredura de maquinas ou redes, com o objetivo de obter informações sobre os alvos.
- IP Scanners: Varrem uma faixa de IP, afim de obter os IPs distribuídos em uma rede ou maquina. Há versões mais atuais que possibilitam a obtenção do endereço MAC das mesmas.

Scanners (Cont)

- Port Scanners: Varrem portas abertas, comumente TCP, que facilitem o processo de invasão ou ataque
- Portas mais comuns
  - 20 FTP dados
  - 21 FTP controle
  - 23 Telnet
  - 25 SMTP
  - 80 HTTP
  - 110 POP3:

Engenharia Social

- Não se trata de um ataque real a uma rede ou um sistema, mas sim consiste em técnicas de persuasão e/ou deludiar pessoas afim de obter informações sigilosas, tais como senhas, configurações, nomes, rotinas.
- Kevin Mitnick – Arte de Enganar / A Arte de Invadir

Ameaças Internet

- Spam e Fishing
- Mail Bomb
- Teclado Virtual Falso
- Scamming (Site de Banco Falso)
- Clonagem de URLs
- Web Site Defacement

Conclusão

- Vamos pensar um pouco?!?

Bibliografia e Complementos

- Redes de Computadores, Tanenbaum A.
- Segurança na Internet – DR. Miguel Franklin
- Tipos de Ataques a Redes de Computadores – Dailson Fernandes.