FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

4SEG – SEGURANÇA DE REDES
AULA 2
Principais Tipos de Ameaças e Ataques

Profa. Maria Cláudia Roenick Guimarães
E-mail: maria.roenick@faeterj-rio.edu.br

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Vulnerabilidades

- O que são vulnerabilidades?
  - Pontos fracos em que os ativos estão suscetíveis a ataques - fatores negativos internos.
  - Permitem o aparecimento de ameaças potenciais à continuidade dos negócios das organizações.
  - Fragilidade presente ou associada à ativos, que manipula ou processam informações, que, ao ser explorada por ameaças, permitem a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios de segurança da informação (CID).

- Uma ameaça é um possível perigo que pode explorar uma vulnerabilidade.

- Vulnerabilidades Físicas:
  - Instalações prediais fora dos padrões de engenharia;
  - Salas de servidores mal planejadas;
  - Falta de extintores, detectores de fumaça e de outros recursos para detecção e combate a incêndio.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Vulnerabilidades

- Vulnerabilidades Naturais:
  - Possibilidade de desastres naturais (incêndios, enchentes, terremotos, tempestades, falta de energia);
  - Problemas nos equipamentos de apoio (acúmulo de poeira, aumento de umidade e de temperatura).

- Vulnerabilidades de Hardware:
  - Falha nos recursos tecnológicos (desgaste, obsolescência, mau uso);
  - Erros durante a instalação;
  - A ausência de atualizações de acordo com as orientações dos fabricantes dos programas utilizados;
  - A conservação inadequada dos equipamentos.

- Vulnerabilidades de Software:
  - Erros de instalação ou de configuração possibilitando acessos indevidos, vazamento de informações, perda de dados ou indisponibilidade de recursos quando necessários.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Vulnerabilidades

- Vulnerabilidades de Comunicação:
  - Acessos não autorizados ou perda de comunicação;
  - A ausência de sistemas de criptografia nas comunicações;
  - A má escolha dos sistemas de comunicação para envio de mensagens de alta prioridade da empresa.

- Vulnerabilidades Humanas:
  - Falta de treinamento;
  - Compartilhamento de informações confidenciais;
  - Falta de execução de rotinas de segurança;
  - Erros ou omissões;
  - Terrorismo ou vandalismo (ameaça de bomba, sabotagem, distúrbios civis, greves, roubo, furto, assalto, destruição de propriedades ou de dados, invasões, guerras etc.).

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Vulnerabilidades

- Vulnerabilidades por si só não provocam incidentes, pois são elementos passivos, necessitando para tanto de um agente causador ou uma condição favorável que são as ameaças.

- A análise das vulnerabilidades tem por objetivo verificar a existência de falhas de segurança no ambiente de TI das empresa;
- É uma ferramenta importante para a implementação de controles de segurança eficientes sobre os ativos de informação das empresas;
- É realizada através de um levantamento detalhado do ambiente computacional da empresa, verificando se o ambiente atual fornece condições de segurança compatíveis com a importância estratégica dos serviços que fornece ou desempenha;
- Esta análise compreende todos os ativos da informação da empresa.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Vulnerabilidades

- Importância dos testes:
  - Conhecer as fragilidades de redes de computadores;
  - Conhecer os alertas de segurança antes de um ataque de rede;
  - Conhecer como recuperar uma rede após um ataque.
  - As portas dos protocolos da pilha TCP/IP que encontram-se desprotegidas (abertas);
  - Os sistemas operacionais utilizados;
  - Patches e service packs (se for o caso) aplicados;
  - Aplicativos instalados;
  - Bugs específicos dos sistemas operacionais/ aplicativos;
  - Fraqueza nas implementações de segurança dos sistemas operacionais/aplicativos;
  - Falhas nos softwares dos equipamentos de comunicações.
  - Fraquezas nas implementações de segurança dos equipamentos de comunicação;
  - Fraqueza de segurança/falhas nos scripts que executam nos servidores web;
  - Falhas nas implementações de segurança nos compartilhamentos de rede entre os sistemas e pastas de arquivos;

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Vulnerabilidades

- Importância dos testes (Cont.):
  - Identificar e corrigir vulnerabilidades de rede;
  - Proteger a rede de ser atacada por invasores;
  - Obter informações que auxiliam a prevenir os problemas de segurança;
  - Obter informações sobre vírus.

- Vulnerabilidade: Condição que, quando explorada por um atacante, pode resultar em uma violação de segurança.

- Risco: É o potencial de que uma dada ameaça venha a explorar vulnerabilidades em um determinado ativo, comprometendo sua segurança.

Fonte: Cartilha de Segurança do CERT. br / CGI.br

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Ameaças

- O que são ameaças?
  - Representam perigo para os ativos;
  - Oferecem riscos potenciais ao ambiente de TI e á continuidade dos negócios;
  - Podem afetar aspectos básicos da segurança.
  - Potencial para violação da segurança quando há uma circunstância, capacidade, ação ou evento que pode quebrar a segurança e causar danos.
  - Ou seja, uma ameaça é um possível perigo que pode explorar uma vulnerabilidade.
- Ameaças Naturais:
  - Ameaças decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades eletromagnéticas, maremotos, aquecimento, poluição etc.
- Ameaças Involuntárias: Danos involuntários - quase sempre internos - são uma das maiores ameaças ao ambiente. Podem ser ocasionados por falha no treinamento, acidentes, erros ou omissões.
- Ameaças Intencionais: Ameaças propositais causadas por agentes humanos como hackers, invasores, espiões, ladrões, criadores e disseminadores de vírus de computadores, incendiários.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Ameaças

- Códigos Maliciosos:
  - Programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Também chamados de malware ou praga;
  - Infectam também dispositivos móveis tablets, celulares, smartphones etc.
  - Uma vez instalados, passam a ter acesso aos dados armazenados no computador e podem executar ações em nome dos usuários de acordo com as permissões de cada um.
  - O dispositivo pode ser infectado ou comprometido:

Pela exploração de vulnerabilidades nos programas instalados;	Pela execução de arquivos previamente infectados, obtidos:
Pela autoexecução de mídias removíveis infectadas;	Anexos em mensagens eletrônicas;
Pelo acesso a páginas Web maliciosas, via navegadores vulneráveis;	Via mídias removíveis;
Pela ação direta de atacantes;	Em páginas Web.
	Diretamente de outros computadores.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Ameaças

- Códigos Maliciosos:
  - Porque são desenvolvidos e propagados:
  - Obtenção de vantagens financeiras;
  - Coleta de informações confidenciais;
  - Desejo de autopromoção;
  - Vandalismo.

- São usados como intermediários, pois possibilitam:
  - Prática de golpes
  - Realização de ataques
  - Disseminação de spam

- Descrição dos tipos: https://cartilha.cert.br/malware/

Ameaças

- Resumo sobre ameaças:

Códigos Maliciosos							
Como é obtido?	**Vírus**	**Worm**	**Bot**	**Trojan**	**Spyware**	**Backdoor**	**Rootkit**
Recebido automaticamente pela rede		X	X				
Redebido por e-mail	X	X	X	X	X		
Baixado de sites na Internet	X	X	X	X	X		
Compartilhamento de arquivos	X	X	X	X	X		
Uso de mídias removíveis infectadas	X	X	X	X	X		
Redes sociais	X	X	X	X	X		
Mensagens instantâneas	X	X	X	X	X		
Inserido por um invasor		X	X	X	X	X	X
Ação de outro código malicioso		X	X	X	X	X	X

Fonte: Cartilha de Segurança do CERT. br / CGI.br

Ameaças

- Resumo sobre ameaças:

Códigos Maliciosos							
Como ocorre a instalação?	**Vírus**	**Worm**	**Bot**	**Trojan**	**Spyware**	**Backdoor**	**Rootkit**
Execução de um arquivo infectado	X						
Execução explícita do código malicioso		X	X	X	X		
Via execução de outro código malicioso						X	X
Exploração de vulnerabilidades		X	X			X	X

Códigos Maliciosos							
Como se propaga?	**Vírus**	**Worm**	**Bot**	**Trojan**	**Spyware**	**Backdoor**	**Rootkit**
Insere cópia de próprio em arquivos	X						
Envia código de si próprio pela rede		X	X				
Envia cópia de si próprio por e-mail		X	X				
Não se propaga				X	X	X	X

Fonte: Cartilha de Segurança do CERT. br / CGI.br

Ameaças

- Resumo sobre ameaças:

Códigos Maliciosos							
Ações maliciosas mais comuns:	**Vírus**	**Worm**	**Bot**	**Trojan**	**Spyware**	**Backdoor**	**Rootkit**
Altera e/ou remove arquivos	X			X			X
Consome grande quantidade de recursos		X	X				
Furta informações sensíveis			X	X	X		
Instala outros códigos maliciosos		X	X	X			X
Possibilita o retorno do invasor						X	X
Envia spam e phishing			X				
Desfere ataques na Internet		X	X				
Procura se manter escondido	X				X	X	X

Fonte: Cartilha de Segurança do CERT. br / CGI.br

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Ataques

- Nomenclatura dos atacantes:
  - Hacker: Uma pessoa intensivamente interessada em pesquisar sistemas operacionais; constantemente buscam por novos conhecimentos, os compartilham e nunca causam destruição;
  - Cracker: Pessoa que invade ou viola sistemas com má intenção;
  - Phreaker: É o Cracker especializado em telefonia;
  - Script Kiddies: São as pessoas que utilizam receitas de bolos para crackear.

- Definições:
  - Ataque: Qualquer tentativa, bem ou mal sucedida, de acesso ou uso não autorizado de um serviço, computador ou rede;
  - Exploit: Programa ou parte de um programa malicioso projetado para explorar uma vulnerabilidade existente em um programa de computador;
  - Código Malicioso: Termo genérico usado para se referir a programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel;
  - Tipos específicos: Vírus, worm, bot, spyware, backdoor, cavalo de tróia e rootkit.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Ataques

- Tipos de Ataques:
  - Passivo: possuem a natureza de bisbilhotar ou monitora transmissões;
  - Ativo: envolvem alguma modificação do fluxo de dados ou a criação de um fluxo falso.
- Os ataques passivos são mais difíceis de serem identificados;

- Chamamos de invasão ou comprometimento ao ataque bem sucedido que resulte no acesso, manipulação ou destruição de informações em um computador;

- Os ataques podem ser classificados em:
  - Ataques para obtenção de informações;
  - Ataques ao sistema operacional;
  - Ataques à aplicação;
  - Ataques de códigos pré-fabricados;
  - Ataques de configuração mal feita.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Ataques

- Ataques para obtenção de informações:
  - Permite obter informações sobre um endereço específico, sobre o sistema operacional, a arquitetura do sistema e os serviços que estão sendo executados em cada computador.

- Ataques ao sistema operacional:
  - Os sistemas operacionais atuais apresentam uma natureza muito complexa devido a implementação de vários serviços, portas abertas por padrão, além de diversos programas instalados;
  - Muitas vezes a aplicação de patches não é tarefa tão trivial devido a essa complexidade dos sistemas ou da própria rede de computadores ou ainda pela falta de conhecimento e perfil do profissional de TI.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Ataques

- Ataques à aplicação:
  - Na maioria das vezes para conseguir entregar os produtos no prazo acordado, os desenvolvedores de software tem um tempo de desenvolvimento do produto muito curto;
  - As aplicações muitas vezes são desenvolvidas com um grande número de funcionalidades e recursos e seja para cumprir prazos ou por falta de profissionais qualificados, não realizam testes antes de liberar seus produtos.

- Ataques de códigos pré-fabricados:
  - Por que reinventar a roda se existem uma série de exemplos de códigos já prontos para serem executados? Quando um administrador de sistemas instala um sistema operacional ou uma aplicação, normalmente já existem uma série de scripts prontos, que acompanham a instalação e que tornam o trabalho dos administradores mais fácil e mais ágil;
  - Normalmente o problema na utilização destes script, é que não passaram por um processo de refinamento e customização quanto as reais necessidades de cada administrador.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Ataques

- Ataques de configuração mal feita:
  - Muitos sistemas que deveriam estar fortemente seguros apresentam vulnerabilidades, pois não foram configurados corretamente. Os administradores podem não ter os conhecimentos e recursos necessários para corrigir ou perceber um problema de segurança;
  - Para aumentar a probabilidade de configurar um sistema corretamente os administradores devem remover qualquer serviço ou software que não sejam requeridos pelo sistema operacional.

- As escolhas de ataque mais comuns são:
  - Desfiguração de página (defacement): Consiste em alterar o conteúdo da página web de um site;
  - Escuta de tráfego: Consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos;

Ataques

- As escolhas de ataque mais comuns são (Cont.):
  - Força bruta: Consiste em adivinhar, por tentativa e erro, um nome de usuário e senha de um serviço ou sistema;
  - Varredura em redes (scan): Consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados;
  - Engenharia social:
    - Método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.
    - É um dos meios mais utilizados de obtenção de informações sigilosas e importantes;
    - Para atingir seu objetivo o atacante pode se passar por outra pessoa, assumir outra personalidade, fingir que é um profissional de determinada área, etc.

Ataques

- As escolhas de ataque mais comuns são (Cont.):
  - Phishing scan:
    - É um método de ataque que se dá através do envio de mensagem não solicitada (spam) com o intuito de induzir o acesso a páginas fraudulentas, projetadas para furtar dados pessoais e financeiros da vítima ou ainda o preenchimento de formulários e envio de dados pessoais e financeiros.
    - Normalmente as mensagens enviadas se passam por comunicação de uma instituição conhecida, como um banco, empresa ou site popular.
  - SQL injection:
    - É um tipo de ameaça que se aproveita de falhas em sistemas que interagem com bases de dados através da utilização de SQL;
    - A injeção de SQL ocorre quando o atacante consegue inserir uma série de instruções SQL dentro de uma consulta (query) através da manipulação das entrada de dados de uma aplicação.

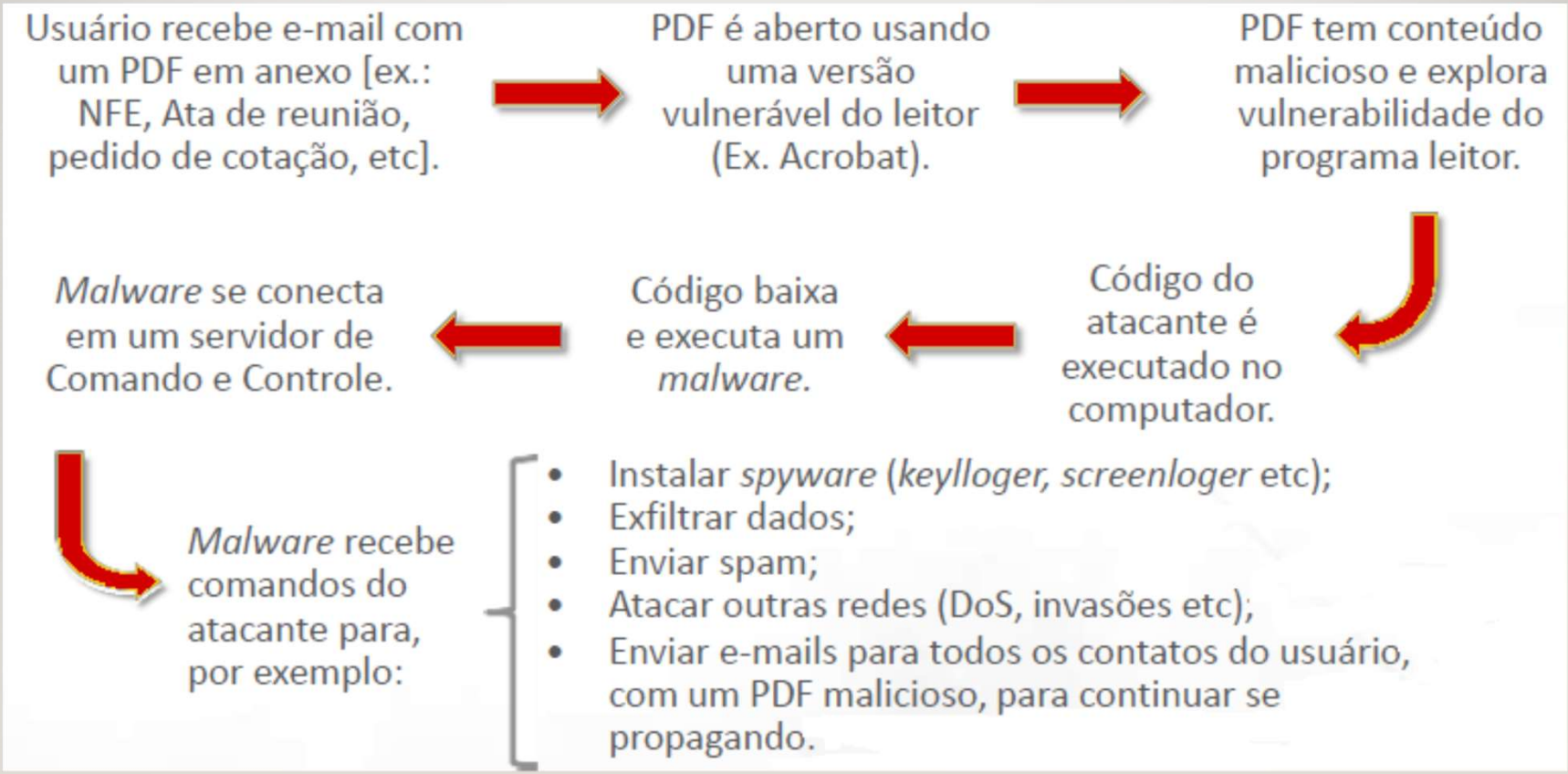
Ataques

- As escolhas de ataque mais comuns são (Cont.):
  - Ataque de negação de serviço (DoS):
    - Um ataque de negação de serviço (também conhecido como DoS é uma tentativa em tornar os recursos de um sistema indisponíveis para seus utilizadores;
    - Normalmente tem como objetivo atingir máquinas servidoras da WEB de forma a tornar as páginas hospedadas nestes servidores indisponíveis;
    - Neste tipo de ataque não ocorre uma invasão no sistema mas a sua invalidação por sobrecarga.
  - Ataques coordenados (DDoS):
    - Semelhante ao ataque DoS, porém ocorre de forma distribuída;
    - Neste tipo de ataque, um computador mestre (denominado "Master") pode ter sob seu comando até milhares de computadores ("Zombies" - zumbis) que terão a tarefa de ataque de negação de serviço.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Ataques

- Exemplo de cenário de ataque contra usuários de Internet:



FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Ataques

- Exemplo de cenário de ataque contra servidores na Internet: