SEGURANÇA DA INFORMAÇÃO



TERCEIRA PARTE

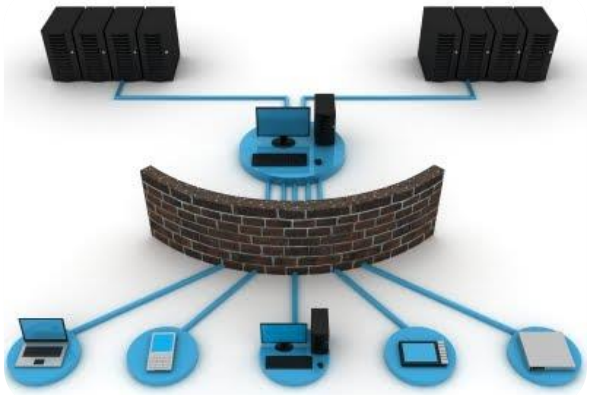
UNIFAI
Ciência da Computação
Prof. José Ricardo P. de Moraes

SEGURANÇA DE REDES

UNIFAI
Ciência da Computação
Prof. José Ricardo P. de Moraes

Segurança de Redes

Ao conectar um **computador** a uma **rede**, é necessário que tome as providencias para se certificar que esta nova máquina conectada possa não vir a ser um **portão** que servirá de entrada de **invasores**, ou seja, de pessoas que estão mal intencionadas, procurando prejudicar alguém ou até mesmo paralisar **a rede inteira**.



Segurança de Redes

Hacker é um indivíduo que se dedica, com intensidade incomum, a conhecer e modificar os aspectos mais internos de dispositivos, programas e redes de computadores. Graças a esses conhecimentos, um *hacker* frequentemente consegue obter soluções e efeitos extraordinários, que extrapolam os limites do funcionamento *normal* dos sistemas como previstos pelos seus criadores.

Segurança de Redes

Cracker é o termo usado para designar o indivíduo que pratica a quebra (ou *cracking*) de um sistema de segurança de forma ilegal ou sem ética. Este termo foi criado em 1985 por *hackers* em defesa contra o uso jornalístico pejorativo do termo '*hacker*'. A criação do termo pelos *hackers* reflete a forte revolta destes contra o roubo e o vandalismo praticados pelos *crackers*.

Black Hat x White Hat

Um *hacker* de *Chapéu Preto* (**Black Hat**) é um individuo que viola a segurança de sistemas de informação para ganho pessoal ou por pura maldade. Ao contrário deste, o *hacker* de *Chapéu Branco* (**White Hat**) *hackeia* protetoramente (com consentimento e de forma organizada), chamando a atenção para *vulnerabilidades* em sistemas de informação que requerem reparo ou maior proteção.

Os termos chapéu preto / chapéu branco se originam na cultura popular americana, em que os chapéus preto e branco denotam cowboys vilões e heroicos, respectivamente.

Ataque

Um **ataque**, ao ser planejado, segue um **plano de estratégia** sobre o alvo desejado, e uma pessoa experiente em planejamento de ataque sempre traça um **roteiro** a ser seguido a fim de **alcançar o objetivo**.

Roteiro de um Ataque

- Localizar o alvo desejado;
- Concentrar o máximo de informações possíveis sobre o alvo, geralmente utilizando alguns serviços da própria rede;
- Disparar o ataque sobre o alvo, a fim de invadir o sistema, explorando a vulnerabilidade do sistema operacional, servidores e serviços oferecidos pela rede.

Roteiro de um Ataque

- Não deixar pistas da invasão, pois geralmente as ações realizadas pelos invasores são registradas no sistema alvo em arquivos de log, possibilitando que o administrador do sistema invadido possa vir a descobrir a invasão;
- O invasor deve conseguir não somente senhas de usuários comuns, pois os privilégios destes usuários são limitados, não dando acesso a recursos mais abrangentes do sistema.

Roteiro de um Ataque

- Criar caminhos alternativos de invasão, logo que o administrador do sistema encontrar uma "porta aberta" que permita a invasão esta será fechada, mas se o invasor gerar outras maneiras de invadir o sistema, certamente terá outra chance de invasão;
- Utilizar a máquina invadida como "portão de entrada" para invasão de outras máquinas da rede e até mesmo do computador central.

CÓDIGOS MALICIOSOS

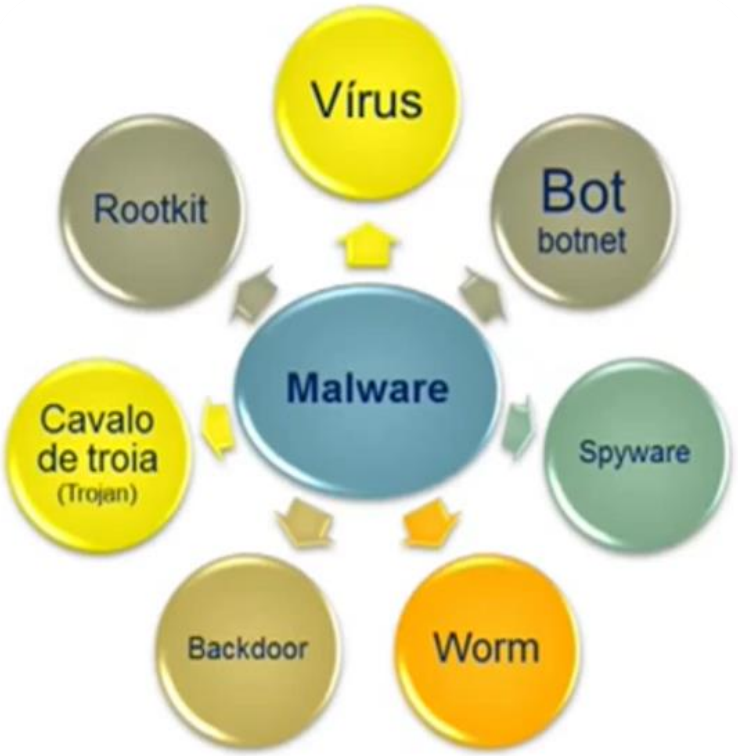
UNIFAI
Ciência da Computação
Prof. José Ricardo P. de Moraes

Códigos Maliciosos

Depois de instalados, os códigos maliciosos passam a ter acesso aos dados armazenados no computador e podem executar ações em nome dos usuários, coletar informações confidenciais, possibilitam a prática de golpes, a realização de ataques e disseminação de *spam*.

Malware

Malware é um termo genérico para qualquer aplicativo que **acessa informações do sistema** ou de documentos alocados no disco rígido, **sem a autorização** do administrador ou usuário. Podendo ainda causar danos irreversíveis ao sistema. Isso inclui *worms*, *trojans*, e vários outros códigos maliciosos.



Vírus

Vírus é um programa (na verdade, parte de um programa) que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos. É um tipo de *Malware* que pode causar ou pode proporcionar danos ao sistema. Necessita de um hospedeiro, ou seja, não atua de forma independente.

Principais Meios de Propagação: Programas, Envio de E-mails, Mídias Removíveis, Vírus de Scripts, Vírus de Macro e Vírus de Smartphone.

Worm

Worm (*Verme*) é um *malware* capaz de se propagar automaticamente pelas **redes**, enviando cópias de si mesmo **de computador para computador**. Ao contrário do *Vírus*, o *Worm* não necessita de hospedeiro para se propagar. Afeta o desempenho das redes, consumindo seus recursos.

Principais Meios de Propagação: Execução Direta de Suas Cópias e Exploração Automática de Vulnerabilidades.

Adware

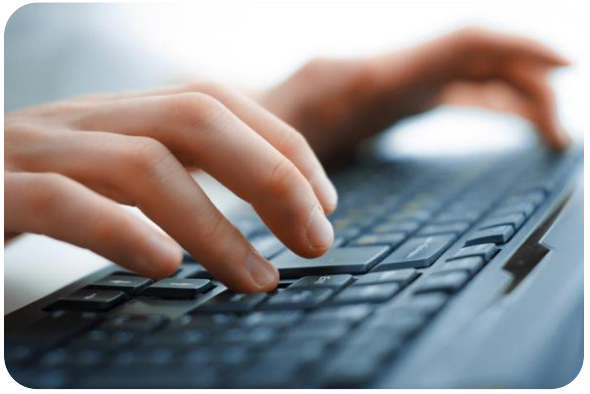
Adware é um tipo de *código malicioso* que **nem sempre** é baixado por acidente para o computador. É um aplicativo que baixa ou exibe, sem exigir autorização, anúncios na tela do computador. Alguns programas carregados de **propagandas** que só as eliminam após a aquisição de uma licença também são considerados *Adwares*.

Spyware

Spyware é um programa automático que recolhe informações sobre o usuário (espiona), sobre os seus costumes na Internet e transmite essas informações a uma entidade externa, sem o conhecimento e consentimento do usuário. Os *Spywares* podem ser desenvolvidos por firmas comerciais, que desejam monitorar o hábito dos usuários para avaliar seus costumes e vender este dados.

Keylogger

Keylogger é um tipo de *Spyware*. Consiste em um aplicativo oculto instalado no computador invadido que gera relatórios completos de tudo o que é digitado na máquina. Assim, podem ser capturados senhas e nomes de acesso de contas de e-mail, serviços online e até mesmo Internet Banking.



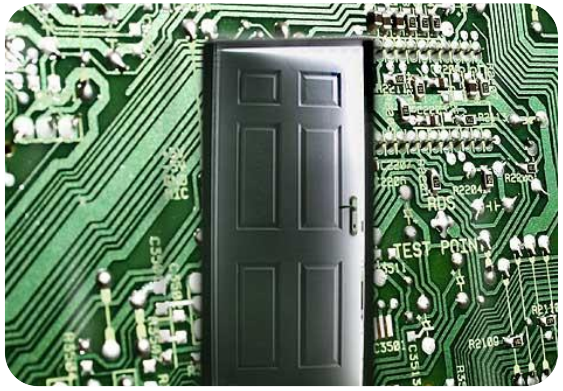
Trojan

Trojan (*Trojan-Horse* - Cavalo de Tróia) é um *malware* que pode entrar em um computador disfarçado como um aplicativo (ou arquivo) comum e legítimo. Ele serve para possibilitar a abertura de uma *porta* (falha) de forma que usuários mal intencionados possam realizar ações não autorizadas.

O *Trojan*, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções sem o conhecimento do usuário.

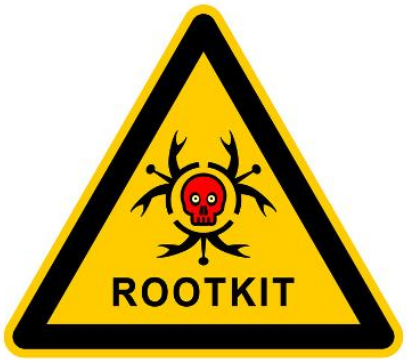
Backdoor

Backdoor (Porta dos Fundos), são *códigos maliciosos* que exploram falhas de segurança de um Sistema Operacional, permitindo que invasores acessem as informações dos computadores sem que sejam detectados. Associados aos *Trojans*, os *Backdoors* abrem portas específicas do sistema para os invasores.



Rootkit

Rootkit é um conjunto de programas ou aplicativos instalados de forma *mal intencionada* em um computador para **esconder ou camuflar** a existência *processos maliciosos* de métodos normais de *detecção* e assegurar acesso ao computador e suas informações a invasores e/ou usuários mal intencionados.



Bot

Bot é um *malware* que dispõe de mecanismos de comunicação com o invasor, permitindo que o computador seja controlado remotamente. O computador, quando infectado por um *Bot*, é chamado de **zumbi**. Permite o *invasor* realizar ações *maliciosas* através do computador *zumbi* sem o conhecimento do usuário.

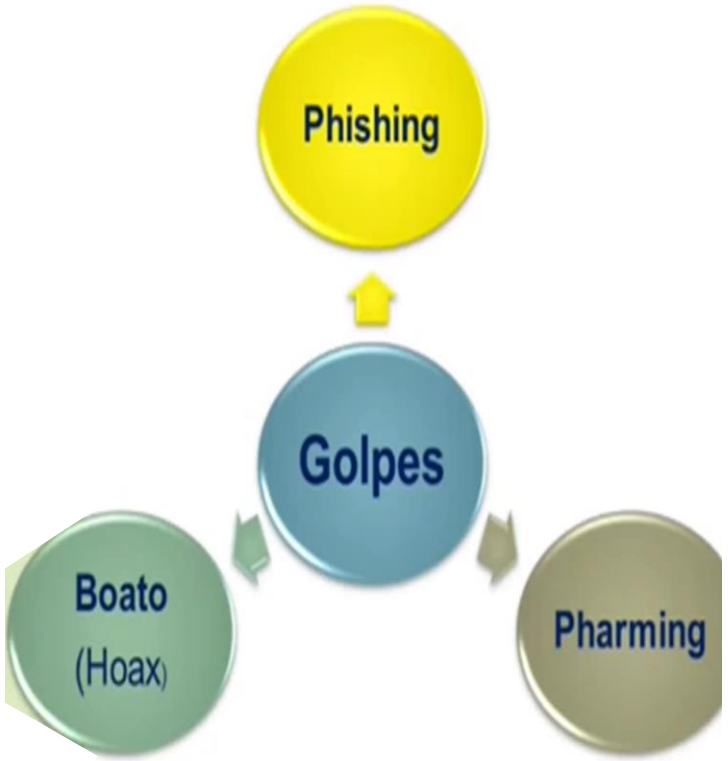
Semelhante ao *Worm*, o *Bot* se propaga automaticamente pela rede, explorando vulnerabilidades.

Botnet

Botnet é uma rede formada por muitos computadores **zumbis** e que permite aumentar a capacidade de ações danosas executadas pelos *Bots*. As *Botnets* podem ser usadas para executar ataques do tipo *DDoS*, roubar dados, enviar *spam* e permitir que o invasor acesse o dispositivo e sua conexão.

Golpes

Golpes ou **Fraudes** na Internet, não são propriamente *programas* ou *aplicativos maliciosos* em si, mas se utilizam de programas e/ou *elementos tecnológicos* para serem aplicados. Infelizmente, *muitos* ainda são *vítimas* de *Golpes* e a cada dia novos golpes surgem na Internet.



Phishing

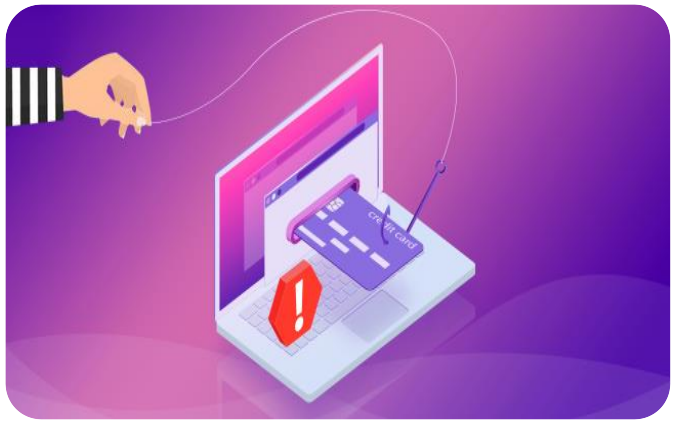
Phishing (*Pescaria*) é um tipo de **Golpe**. São *mensagens* de e-mail criadas com interfaces e nomes que fazem referência a empresas famosas e conhecidas, como bancos e lojas. Nestas mensagens são colocados links disfarçados, que dizem ser prêmios ou informações sobre a empresa em questão, mas na verdade são arquivos maliciosos.

O *Phishing* também pode utilizar um site falso com intensão de capturar as informações de identificação pessoal do usuário.

Pharming

Pharming é outro tipo de Golpe, semelhante ao *Phishing*, porém, consiste no *Envenenamento de DNS* que ataca e corrompe o *Sistema de Nomes de Domínio* em uma rede de computadores, ou o corrompe o próprio navegador do usuário, fazendo com que a *URL* de um site passe a apontar para um servidor diferente do original que esteja sob controle de um golpista.

Os golpistas geralmente copiam fielmente as páginas das instituições, criando a falsa impressão que o usuário está no site desejado.



Hoax

Hoax (*Boato*) é um tipo de **Golpe**, onde o golpista envia uma *mensagem falsa* a um grupo muito grande de pessoas (*spam*) com a intensão de *denegrir* a imagem de uma pessoa ou empresa. Ou ainda, difundir uma Informação Viral Falsa (*Fake News*) onde muitos *acreditam* e com isso, prejudicando *alguém ou alguma instituição*.

Hoax: Mensagem difundida por *Redes Sociais* que possui conteúdo alarmante ou falso e aponta como autora alguma organização importante.

Ataques

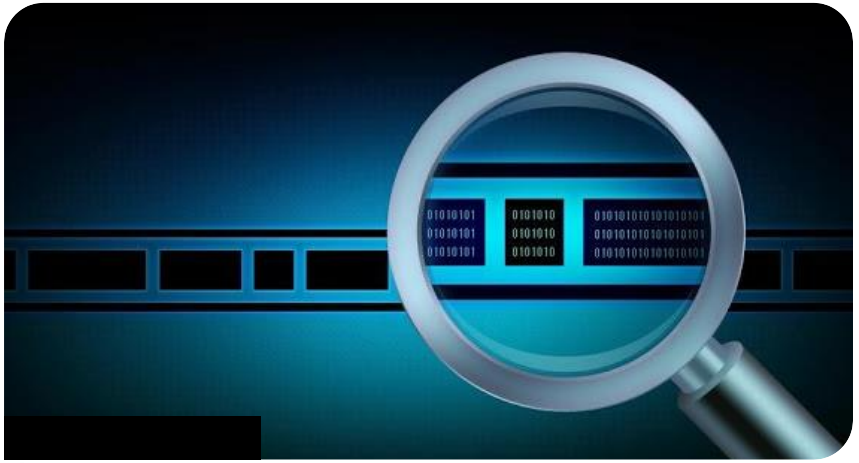
Ataque ou **Ciberataque**, é qualquer tentativa de expor, alterar, desativar, destruir, roubar ou obter acesso não autorizado ou fazer uso não autorizado de um dispositivo. Um *Ataque* é qualquer tipo de manobra ofensiva voltada para sistemas de informação de computadores, infraestruturas, redes de computadores ou dispositivos de computadores pessoais.

Scan

Scan é uma técnica que efetua buscas em redes de computadores, verificando computadores ativos e coletando informações sobre eles. A técnica de *Scan da Rede* é considerada como um tipo *passivo* de ataque, pois apenas coleta informações dos ativos da rede, sem causar nenhum dano.

Sniffing

Sniffing (*Farejador*) é um tipo de ataque que *Intercepta os Pacotes de Informações* que trafegam pela rede. Se os dados não forem *criptografados*, os ofensores podem ter acesso às conversas, senhas e outras *informações* capturadas.



Spoofing

Spoofing é uma técnica utilizada para *Mascarar* o IP do computador. Utilizando endereços falsos, os invasores podem atacar Servidores ou computadores domésticos sem medo de serem rastreados, pois o endereço que é enviado para os destinatários é falso.

Brute Force

Brute Force (*Força Bruta*) é um tipo de ataque que pode, *em teoria*, ser usado contra quaisquer dados criptografados. Pode ser usado quando não é possível tomar vantagem de outras fraquezas em um sistema. Consiste de verificação sistemática de todas as possíveis chaves e senhas até que as corretas sejam encontradas.

Defacement

Defacement (*Desconfigurar*) é um termo usado para categorizar os ataques realizados por *defacers* (*modificadores*) para modificar a página de um site na Internet. Geralmente os ataques tem cunho político, objetivando disseminar uma mensagem do autor do ataque para os frequentadores do site alvo.

DoS

Denial of Service – DoS (*Ataque de Negação de Serviço*) é um tipo de ataque que impede o acesso dos usuários a determinados serviços. Alvos mais frequentes são Servidores Web, pois os atacantes visam deixar sites indisponíveis. As consequências mais comuns neste caso são: consumo excessivo de recursos e falhas na comunicação entre sistema e usuário.

DDoS

Distributed Denial of Service – DDoS (*Ataque Distribuído de Negação de Serviço*), segue o mesmo princípio do *DoS*, mas realizado a partir de vários computadores. São utilizados muitos *computadores zumbis* (*Botnet*) em conjunto com a técnica de *Spoofing* (*Camuflagem*) e computadores (ou até mesmo Servidores e sites) infectados (*Malware*) que servem de *refletores* para *despistar e ampliar* o ataque.

Compromised-Key

Compromised-Key é um tipo de ataque realizado para determinadas *chaves de registro* de um Sistema Operacional (*falhas de segurança*). Quando o invasor consegue ter acesso às chaves vulneráveis, pode gerar relatórios com a decodificação de *Senhas Criptografadas* e invadir contas e serviços cadastrados.

Man-in-the-Middle

Man-in-the-Middle é um tipo de ataque que ocorre quando um *equipamento* intercepta conexões de dois outros. Cliente e Servidor trocam informações com o *Invasor*, que se esconde com as máscaras de ambos. Ou seja, pode ser um interceptador de uma *conversa*, que passa a falar com os dois usuários, enganando à ambos.

Ping of Death

Ping of Death (*Ping da Morte*), é um tipo de ataque em que um *Invasor* realiza constantes *pings* na máquina invadida para causar travamentos na banda e até mesmo para travar o equipamento. É um tipo de ataque de *Negação de Serviço*.

ATAQUES WIRELESS

UNIFAI
Ciência da Computação
Prof. José Ricardo P. de Moraes

Evil Twin

O ataque do tipo **Evil Twin**, também conhecido como **Rouge AP**, é uma junção de outros tipos de ataques como o *Man-in-the-Middle-Attack*, *Phishing*, etc., porém atuando na Rede Wireless. Usuários pensam que se conectaram a um ponto legítimo da rede, mas na realidade, estão se conectando a um servidor malicioso que pode monitorar e obter dados digitados pelo usuário.

BlueSnarfing

Bluesnarfing é o acesso não autorizado a informações de um dispositivo sem fio através de um Bluetooth, muitas vezes, entre os telefones, desktops, laptops e PDAs. Isso permite o acesso a um calendário, lista de contatos, e-mails e mensagens de texto, e em alguns aparelhos os usuários podem copiar fotos e vídeos privados.

BlueJacking

Bluejacking se refere a uma técnica consistente em enviar mensagens não solicitadas entre dispositivos Bluetooth, como por exemplo telefones, desktops, laptops e PDAs. A tecnologia Bluetooth tem um alcance limitado de uns 10 metros normalmente.

I.V. Attack

O **Initialization Vector Attack** ataque consiste em sobrecarregar a rede com vários pacotes com diferentes tipos de informações e/ou requisições para que isso gere milhares de pacotes de resposta e assim possa deduzir a chave de criptografia e facilitar a descoberta da senha da rede.

ATAQUES DE APLICAÇÃO

UNIFAI
Ciência da Computação
Prof. José Ricardo P. de Moraes

Cross-site Scripiting

Neste tipo de ataque o **Cracker** insere scripts maliciosos diretamente no código fonte de sites utilizando o browser (navegador) para enviar o script. Também conhecido como **XSS**.

SQL Injection

O **SQL Injection** é o nome dado a uma falha na codificação de uma aplicação qualquer (seja web ou local) que possibilita, por meio de um input, a manipulação de uma consulta SQL. Essa manipulação é chamada Injeção, então, o termo *Injeção SQL*.

Buffer Overflow

Buffer Overflow (Transbordamento de Dados ou Estouro de Buffer) é uma anomalia onde um programa, ao escrever dados em um buffer, ultrapassa os limites do buffer e sobrescreve a memória adjacente, sobrecarregando a aplicação forçando a parada.

Códigos Maliciosos

Vídeo: 6 dos vírus de computador mais icônicos da história

Duração: 05min e 34seg

Produção: TechMundo

Local: YouTube

Link:

https://www.youtube.com/watch?v=P-m_DM3WnLA