GESTÃO DE SEGURANÇA DA INFORMAÇÃO

ATAQUE À SEGURANÇA

Olá!

Nesta aula você irá Compreender o que são ataques à segurança da Informação.

1. O planejamento de um ataque;

2. Os principais tipos de ataques.

Com o avanço das tecnologias e a valorização da informação nas organizações, o profissional da área de TI necessita atualmente além de ter conhecimento e entendimento profundo das características de funcionamento de sistemas de arquivos, programas de computador e padrões de comunicação em redes de computadores, noção sobre psicologia dos atacantes, seus perfis de comportamento e motivações que os levam a realizar um ataque.

Deverá também ter familiaridade com as ferramentas, técnicas, estratégias e metodologias de ataques conhecidos para que possa desta forma contribuir com a definição correta de quais contramedidas deverão ser adotadas pela organização.

Para que um ataque ocorra, normalmente o atacante irá seguir os seguintes passos:

- **1. Levantamento das informações**

  A fase de reconhecimento é unia fase preparatória onde o atacante procura coletar o maior número possível de informações sobre o "alvo em avaliação" antes do lançamento do ataque.

  Existem duas formas de realizar o reconhecimento: ativo e passivo. O reconhecimento passivo envolve a aquisição de informação sem interação direta com o "alvo". O reconhecimento ativo envolve interação direta com o alvo através de algum meio, como por exemplo, contato telefônico por meio do help desk ou departamento técnico.

- **2. Exploração das informações**

  Fase onde o atacante explora a rede baseado nas informações obtidas na fase de reconhecimento. Esta fase apresenta um alto risco para os negócios de uma empresas, pois além de ser considerado uma fase de pré-ataque envolve a utilização de diferentes técnicas e softwares, como por exemplo, a utilização de port scan, scanner de vulnerabilidade e network mapping.

- **3. Obtenção de acesso**

Esta fase consiste na penetração do sistema propriamente dita. Nesta fase são exploradas as vulnerabilidades encontradas no sistema. Isto pode ocorrer através da internet, da rede local, fraude ou roubo. Os fatores que irão influenciar nos métodos utilizados pelo atacante serão: a arquitetura e configuração do "alvo" escolhido, o grau de conhecimento do atacante e o nível de acesso obtido.

Nesta fase o atacante poderá obter acesso a nível de: sistema operacional, aplicação e rede.

- **4. Manutenção de acesso**

Nesta fase o atacante tenta manter seu próprio domínio sobre o sistema. Poderá também protêge-lo de outros atacantes através da utilização de "acessos exclusivos" obtidos através de rootkits, backdoors ou trojans. Poderá ainda fazer upload, download e manipulação dos dados, aplicações e configurações da máquina atacada. Nesta fase o sistema atacado poderá ficar comprometido.

- **5. Camuflagem das evidências**

Esta fase consiste na atividade realizada pelo atacante de tentar camuflar seus atos não autorizados com o objetivo de prolongar sua permanência na máquina hospedeira, na utilização indevida dos recursos computacionais. Podemos citar como técnicas utilizadas nesta fase a esteganografia (do grego "escrita escondida- é o estudo e uso das técnicas para ocultar a existência de uma mensagem dentro de outra. Em outras palavras, esteganografia é o ramo particular da criptologia que consiste em fazer com que uma forma escrita seja camuflada em outra a fim de mascarar o seu verdadeiro sentido. É importante frisar a diferença entre criptografia e esteganografia. Enquanto a primeira oculta o significado da mensagem, a segunda oculta a existência da mensagem. Fonte: wikipédia), o tunelamento e a alteração dos arquivos de log.

Principais tipos de ataque:

Existem diferentes caminhos que um atacante pode seguir para obter acesso ao sistema. Normalmente o atacante irá explorar uma vulnerabilidade ou fraqueza do sistema. Estes ataques podem ser classificados como:

Ataque para obtenção de informações

Neste tipo de ataque é possível 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 aos sistemas operacionais

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

e hotfixes não é tarefa tão trivial devido a essa complexidade: dos sistemas , da rede de computadores ou ainda pela falta de conhecimento e perfil do profissional de TI. Consequentemente os atacantes procuram e exploram as vulnerabilidades existentes nos sistemas Operacionais para obter acesso para o sistema de rede da organização.

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. Apesar de muitas organizações utilizarem metodologias baseadas na engenharia de software, as aplicações muitas vezes são desenvolvidas com um grande número de funcionalidades e Recursos, seja para cumprir prazos ou por falta de profissionais qualificados, não são realizados testes antes da liberaração dos produtos.

Além disso, normalmente as caracteristicas de segurança da aplicação são oferecidas posteriormente ou muitas das vezes como um componente “add-on”. A não existência de controles de erros nas aplicações podem levar a ataques por exemplo, de buffer overflow.

Ataques de códigos pré-fabricados (shrink wrap code)

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 scripts, é que não passaram por um processo de refinamento e customização quanto as reais necessidades de cada administrador e quando utilizado em sua versão padrão podem então conduzir a um ataque do tipo shrink wrap code, ou seja o atacante utiliza possível falhas de segurança nestes scripts para realizar o ataque.

Ataques de configuração mal feita (misconfiguration)

Muitos sistemas que deveriam estar fortemente seguros, podem apresentam vulnerabilidades caso não tenham sido configurados adequadamente. Com a complexidade dos sistemas atuais os administradores podem não ter os conhecimentos e recursos necessários para corrigir ou perceber um problema de segurança. Normalmente para agilizar e simplificar o trabalho, os administradores criam configurações simples. Para aumentar a probabilidade de configurar um sistema adequadamente os administradores devem remover qualquer serviço ou software que não sejam requeridos pelo sistema operacional, evitando que algum serviço ou software não necessário possa ser explorado.

Principais tipos de ataque:

Packet Sniffing

Consiste na captura de informações valiosas diretamente pelo fluxo de pacotes transmitido na rede. Este tipo de ataque também é conhecido como espionagem passiva e sua utilização diminuiu muito com a utilização de switches no lugar dos hubs.

Fique ligado

Evite a utilização de serviços que possuem senhas abertas, tais como telnet, FTP e POP, pois podem ser facilmente capturadas pela rede dessa forma. Além da utilização de serviços que possuem suas mensagens criptografadas (iremos estudar criptografia nas próximas aulas!)

Port Scanning

Ocorre na camada de transporte do modelo OSI. É realizado um mapeamento das portas do protocolos TCP e UDP abertas em um determinado host, e partir daí, o atacante poderá deduzir quais os serviços estão ativos em cada porta.

Saiba mais

A utilização de firewalls (É o nome dado ao dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto de controle da rede. Sua função consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra. Fonte: wikipedia) contribui muito para evitar esse tipo de ataque. Pois além de limitar as portas que poderão ser acessadas, podemos definir os estados das conexões tcp que serão aceitos. Podemos, por exemplo, definir que para a porta 21, somente o endereço IP xpto.xpto. xpto.xpto poderá acessar.

Como funciona o Port Scanning ?

Um dos métodos de se implementar um port scanning é a partir do protocolo TCP e através da primitiva connect() onde a system call connect() é utilizada para abrir uma conexão nas portas do alvo. Se a porta estiver aberta, a system call retornará com sucesso.

Scanning de vulnerabilidades

Após mapear os sistemas que podem ser atacados e os serviços que são executados, o atacante irá mapear as vulnerabilidades específicas para cada serviço através da utilização de um software de scanning de vulnerabilidades.

Estes softwares possuem diversos padrões e testes para detectar vulnerabilidades. Seu principal alvo são aplicativos desatualizados, por exemplo:

A versão de algum software utilizado na sua organização na qual foram achadas falhas críticas de segurança mas que a equipe técnica, por não saber dessas falhas não atualizou a versão do mesmo.

Saiba mais

Mantenha-se sempre atualizado através das listas de segurança a respeito dos aplicativos de rede utilizados pela empresa e deixe-os sempre atualizados.

Fique ligado

"Este tipo de scanner é muito útil para o invasor, já que, através dele, poderá escolher qual o exploit a ser utilizado para a invasão. Basicamente, a idéia do scanner de vulnerabilidade é, através de uma lista, checar se o sistema está ou não executando um serviço com problemas. Estes scanners são facilmente desatualizados, pois existe uma quantidade enorme de descobertas hoje publicadas em sites de segurança.

Ip Spoofing

Nesta técnica o endereço IP real do atacante é alterado, evitando assim que ele seja encontrado. Sistemas que possuem a segurança baseada em lista de endereço IP são o principal alvo desse tipo de ataque, onde o atacante se passa por um usuário legítimo.

Você sabia?

A melhor forma de tentar se proteger desse tipo de ataque é com a aplicação de filtros, de acordo com as interfaces de rede onde os IPs são validados e as interfaces de rede por onde trafegam também.

SYN Flooding

Este tipo de ataque explora a metodologia de estabelecimento de conexões do protocoloTCP, baseado no three-way-handshake. Desta forma um grande número de requisições de conexão (pacotes SYN) é enviando, de tal maneira que o servidor não seja capaz de responder a todas elas.

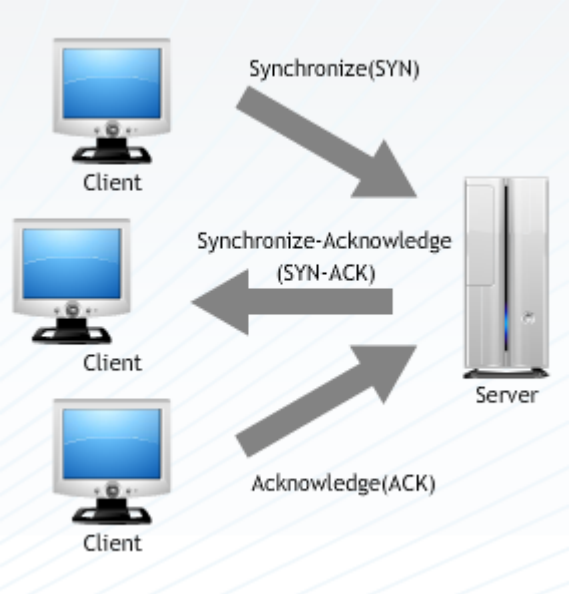
A pilha de memória sofre então um overflow e as requisições de conexões de usuários legítimos são, desta forma, desprezadas, prejudicando a disponibilidade do sistema.

Para relembrar:

Three-way-handshake

O protocolo TCP é um protocolo confiável, pertencente a pilha de protocolos TCP/IP. Para que ocorra troca de dados entre dois computadores é necessário que as duas máquinas estabeleçam uma conexão. Essa conexão é virtual e é conhecida como uma sessão e ocorre através de um processo chamado handshake de três vias, pois ocorre em três etapas. Esse processo sincroniza os números de seqüência e fornece outras informações necessárias para estabelecer a sessão:

1. O cliente manda uma requisição (SYN).
2. O servidor responde com SYN-ACK (quer dizer que aceitou o protocolo e estabeleceu a conexão).
3. O cliente envia as informações em forma de "pacotes".



Fragmentação de pacotes IP

Os pacotes do protocolo TCP/IP possuem um campo MTU (maximum transfer unit) que especifica a quantidade máxima de dados que podem passar em um pacote por um meio físico da rede. Este tipo de ataque utiliza-se dessa característica devido ao modo como a fragmentação e o reagrupamento são implementados. Os sistemas

não tentam processar o pacote até que todos os fragmentos sejam recebidos e reagrupados, isso cria a possibilidade de ocorrer um overflow na pilha do protocolo TCP quando há o reagrupamento dos pacotes.

Fique ligado

Esse tipo de ataque não pode ser evitado por meio da implementação de filtro de pacotes, apenas com a aplicação de correções no kernel do sistema operacional. Os atuais sistemas operacionais já lidam com esse problema.

Fraggle

Consiste em enviar um excessivo número de pacotes PING para o domínio de broadcast da rede, tendo como endereço IP de origem, a vítima desejada. Dessa forma todos os hosts do domínio de broadcast irão responder pra o endereço IP da vítima, que foi mascarado pelo atacante, ficando desabilitada de suas funções normais.

Smurf

O ataque smurf é idêntico ao ataque Fraggle, alterando apenas o fato que utiliza-se de pacotes do protocolo UDP.

Saiba mais

Para evitar esse tipo de ataque o roteador não deve permitir esse tipo de comunicação para endereços broadcast por meio de suas interfaces de rede.

SQL Injection

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.

Buffer Overflow

Conseqüência direta de péssimos hábitos de programação. Consiste em enviar para um programa que espera por uma entrada de dados qualquer, informações inconsistentes ou que não estão de acordo com o padrão de entrada de dados.

Ataque físico

Muitas vezes as organizações investem em equipamentos do tipo firewalls e anti-vírus e pensam que estão protegidos e esquecem que os ataque não ocorrem somente pela rede de computadores. As salas aonde ficam os servidores e os equipamentos de rede devem ter um controle rígido de acesso, assim como os arquivos com dados sigilosos ou sensíveis. Um ataque físico também pode ocorrer em instâncias menores como roubo da fita magnética de backup, através da conexão de dispositivos USB, ou ainda por acesso as informações sigilosas.

Fique ligado

Funcionários insatisfeitos e que possuem acesso às informações podem copiar dados sigilosos e distribuí-los à concorrência ou realizar outros propósitos maléficos.

Dumpster diving ou trashing

Consiste na verificação do lixo em busca de informações que possam facilitar o ataque. É uma técnica eficiente e muito utilizada e que pode ser considerada legal visto que não existem leis a respeito dos lixos. Neste caso é interessante que as informações críticas da organização (planilhas de custos, senhas e outros dados importantes) sejam triturados ou destruídos de alguma forma.

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.

Isso ocorre pois a maioria da empresas não possui métodos que protejam seus funcionários das armadilhas de engenharia social.

Para atingir seu objetivo o atacante pode se passar por outra pessoa, assumir outra personalidade, fingir que é um profissional de determinada área, etc.

Os ataques de engenharia social são muito freqüentes, não só na Internet, mas no dia-a-dia das pessoas.

Saiba mais

Pesquise na internet sobre dois personagens que merecem destaques relevantes no contexto da engenharia social: Frank Abagnale W. Jr e Kevin Mitnick.

Phishing Scam

Phishing, também conhecido como phishing scam ou phishing/scam, é um método de ataque que se dá através do envio de mensagem não solicitada 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.

Saiba mais

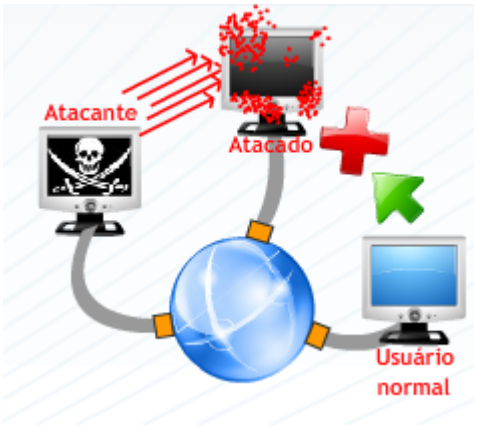
Novas formas de phishing estão sempre surgindo, portanto é muito importante que os profissionais de TI e segurança se mantenham informados sobre os tipos de phishing que vêm sendo utilizados pelos fraudadores, através dos veículos de comunicação.

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. Estes tipos de ataques podem ser realizados de duas formas:

- Forçando o sistema alvo a reinicializar ou consumir todos os seus recursos (como memória ou processamento) de forma a não poder mais fornecer seu serviço.
- Obstruindo a mídia de comunicação entre os clientes e o sistema alvo de forma a não comunicarem-se adequadamente.

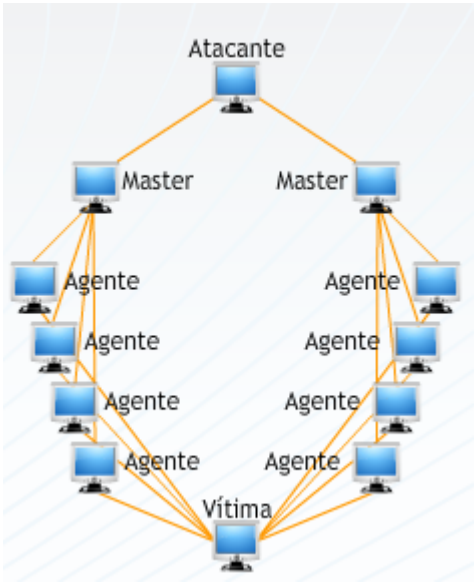


Ataques coordenados (DDoS)

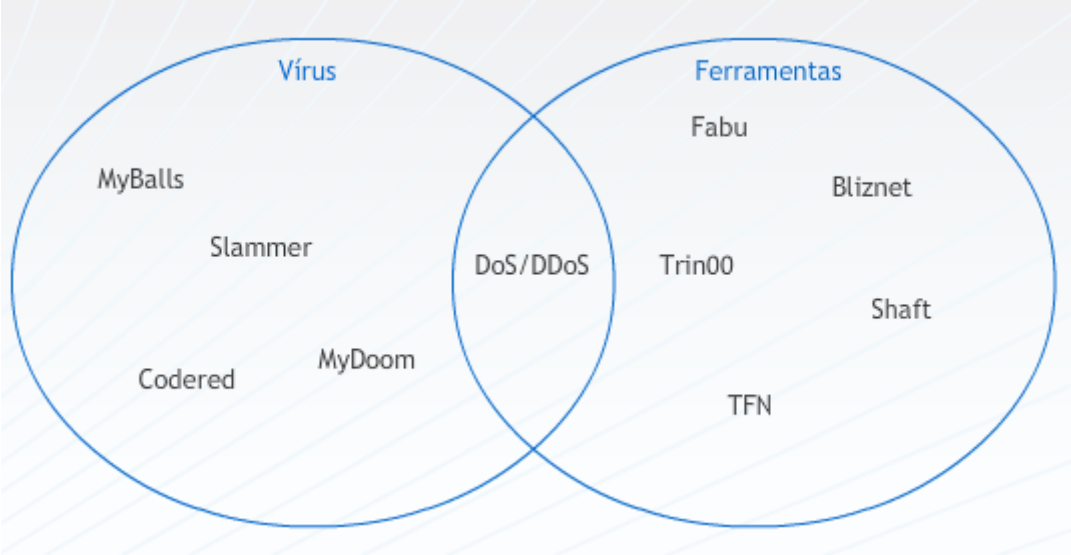
Semelhante ao ataque DoS, porém ocorre de forma distribuída. Neste tipo de ataque distribuído de negação de serviço, também conhecido como DDoS (é um acrônimo em inglês para Distributed Denial of Service. Fonte: wikipedia), um computador mestre (denominado "Master") pode ter sob seu comando até milhares de computadores ("Zombies" - zumbis) que terão a tarefa de ataque de negação de serviço.

Como o ataque funciona?

- Consiste em fazer com que os Zumbis se preparem para acessar um determinado recurso em um determinado servidor em uma mesma hora de uma mesma data.
- Passada essa fase, na determinada hora, todos os zumbis (ligados e conectados à rede) acessarão ao mesmo recurso do mesmo servidor.
- Como servidores web possuem um número limitado de usuários que pode atender simultaneamente, o grande e repentino número de requisições de acesso faz com que o servidor não seja capaz de atender a mais nenhum pedido. Dependendo do recurso atacado, o servidor pode chegar a reiniciar ou até mesmo ficar travado.



Existem uma série de vírus e ferramentas que foram criadas para a distribuição de rotinas de ataque de negação de serviço:



Seqüestros de conexões

As conexões do protocolo TCP são definidas por quatro informações essenciais:

- endereço IP de origem;
- porta TCP de origem;
- endereço IP do destino;
- porta TCP do destino.

Todo byte enviado por um host é identificado com um número de seqüência que é conhecido pelo receptor. O número de seqüência do primeiro byte é definido durante a abertura da conexão e é diferente para cada uma delas.

Neste tipo de ataque um terceiro host, do atacante, cria os pacotes com números de seqüencias válidos, colocando-se entre os dois hosts e enviando os pacotes válidos para ambos.

Saiba mais

Foram realizadas implementações no protocolo TCP/IP que praticamente inviabilizou esse tipo de ataque, que se tornou famoso por ter sido utilizado pelo Mitnick em conjunto com outras técnicas.

Source Routing

Mecanismo legítimo que foi especificado para o protocolo IP, mas que pode ser explorado de forma ilícita. Neste tipo de ataque define-se uma rota reversa para o tráfego de resposta, em vez de utilizar algum protocolo de roteamento padrão.

Saiba mais

A melhor forma de evitar esse tipo de ataque é bloqueando a utilização da opção source routing, visto que normalmente não é utilizada.

O que vem na próxima aula

Na próxima aula, aprenderemos o seguinte tema: Gestão de Riscos em Segurança da Informação

- O estabelecimento do contexto e as etapas da gestão do risco;
- Análise e avaliação do risco;
- Tratamento, aceitação e comunicação do risco;
- Monitoramento e revisão dos riscos.

CONCLUSÃO

Nesta aula, você:

- Compreendeu o que são ataques à segurança da Informação e sua importância.
- Estudou as etapas de planejamento de um ataque.
- Conheceu os principais tipos de ataques.