Curso de Ciência da Computação
Disciplina: Segurança e Auditoria da Informação - 8º período
Professor: José Maurício S. Pinheiro

AULA 4: Proteção de Sistemas de Informação

1. Senhas e Autenticação

A autenticação é o processo de verificar a identidade declarada por uma entidade do sistema, ou seja, verificar se, quem está tentando utilizar o sistema ou ganhar acesso, é realmente quem declara ser.
A definição dada pela RFC 4949 (*Request for Coments* nº 4949) para o termo password (ou senha) é "um dado secreto, usualmente composto por uma sequência de caracteres, que é usado como informação para autenticar um usuário ou pessoa". Esclarece também que, normalmente é utilizada em conjunto com uma identificação do usuário no processo de autenticação, quando da entrada do usuário na rede ou sistema.
O processo de autenticação pode ser dividido em dois passos, conforme descrito pela mesma RFC:

- **Identificação**: apresentação de uma identificação ao sistema de segurança. Pode ser o login de entrada ou o nome da conta;
- **Verificação**: compara com dados já armazenados previamente se a password e o login estão corretos, gerando então a informação se a autenticação está correta ou não. Em caso positivo, o sistema assume que a pessoa ou a entidade que requer o acesso é quem realmente declara ser, e então, libera as transações permitidas para serem realizadas.

1.1. Política de Senhas

Uma senha serve para autenticar o usuário, ou seja, a senha garante que determinado indivíduo que utiliza um serviço é ele mesmo, permitindo o acesso aos vários serviços disponibilizados em uma rede. A senha, por definição é uma assinatura eletrônica e, portanto, ela é pessoal e deve ser mantida em sigilo.
Pode parecer primário, mas muitas pessoas utilizam senhas fáceis de adivinhar, anotando em agendas, colocando o código em local visível ou simplesmente compartilhando seu conteúdo com outras pessoas. Se um usuário fornece sua senha para uma outra pessoa, esta poderá utilizá-la como se fosse o próprio usuário, tendo acesso a informações restritas.
Com o objetivo de dificultar a dedução de senhas por terceiros, algumas recomendações importantes podem ser seguidas para evitar problemas de segurança:

- Evitar anotar as senhas em papéis soltos ou agendas. As senhas são pessoais e devem ser memorizadas preferencialmente, não escritas.
- Nunca utilizar senhas fáceis de identificar como data de aniversário, placa de carro, etc.
- Uma boa senha deve ter pelo menos oito caracteres, preferencialmente alfanumérica (combinação de letras, números e símbolos), deve ser simples de digitar e fácil de lembrar.

2. Ameaças e ataques

Uma ameaça consiste em uma possível violação de um sistema computacional e pode ser acidental ou intencional. Uma ameaça acidental é aquela que não foi planejada. Pode ser, por exemplo, uma falha no hardware (um defeito no disco rígido) ou uma falha de software (bug do sistema). Já uma ameaça intencional, como o nome diz, está associada à intencionalidade premeditada. Pode ser desde um monitoramento do sistema até ataques sofisticados, como aqueles feitos por hackers ou crackers.
Algumas das principais ameaças aos sistemas de computadores envolvem destruição de informações ou recursos, modificação ou deturpação da informação, roubo, remoção ou perda de informação, revelação de informações confidenciais ou não, chegando até a interrupção de serviços de rede.
Já um ataque ocorre quando uma ameaça intencional é realizada. Os ataques ocorrem por motivos diversos. Variam desde a pura curiosidade pela curiosidade, passando pelo interesse em adquirir conhecimento, pelo teste de capacidade "vamos ver se eu sou capaz", até o extremo, envolvendo ganhos financeiros, extorsão, chantagem de algum tipo, espionagem industrial, venda de informações confidenciais e, o que está muito na moda, ferir a imagem de um governo ou uma determinada empresa ou serviço. Quando isso acontece, a notícia de uma invasão é proporcional à fama de quem sofreu essa invasão e normalmente representa um desastre em termos de repercussão pública.

2.1. Ameaças quanto a sua Intencionalidade

- **Naturais** – fenômenos da natureza (incêndio, terremoto, tempestade, etc.);
- **Involuntárias** – causadas quase sempre pelo desconhecimento (acidentes, erros, falta de energia, etc.);
- **Voluntárias** – causadas propositalmente por agentes humanos (hackers, espiões, ladrões, invasores, etc.).

2.2. Ameaças aos Sistemas Computacionais

- **Vazamento:** ocorre quando um usuário legítimo (autorizado) fornece informação para um ou mais receptores não autorizados. Isto pode ocorrer propositalmente, ou não.
- **Violação** ocorre quando uma informação legítima sofre alteração não autorizada (incluindo programas).

- **Furto de recursos:** ocorre quando alguém não autorizado beneficia-se das facilidades dos sistemas computacionais.
- **Vandalismo:** quando alguém não autorizado, interfere, causando prejuízo às operações dos sistemas, sem ganhos próprios.

3. Vulnerabilidade

Ponto pelo qual alguém pode ser atacado, molestado ou ter suas informações corrompidas. Exemplos de vulnerabilidades:

- Físicas – Instalações prediais fora do padrão, salas de equipamentos mal planejadas; falta de sistemas de proteção ambiental;
- Naturais – Incêndios, enchentes, falta de energia, umidade excessiva;
- Hardware – Falha de recursos, danos em mídias, erros de instalação;
- Software – Erros na instalação e ou na configuração;
- Comunicação – Acessos não autorizados ou perda de comunicação;
- Humanas – Falta de treinamento, erros ou omissão, vandalismo.

As principais ameaças que devem ser tratadas pela da Política de Segurança da Informação são as seguintes:

- Ameaças à integridade: Ameaças ambientais (fogo, água, terremoto, etc.), erros humanos, fraudes, falhas de processamento;
- Ameaças de indisponibilidade: Falhas em sistemas ou nos diversos ambientes computacionais;
- Ameaças de divulgação da informação: Divulgação de informações premeditada ou acidental;
- Ameaças por alterações não autorizadas: Alteração premeditada ou acidental do conteúdo das informações do sistema.

São três os aspectos básicos que um sistema de segurança da informação deve atender para evitar a concretização dessas ameaças:

3.1. Prevenção

- **Proteção de hardware**: normalmente chamado de segurança física, impede acessos físicos não autorizados à infra-estrutura da rede, prevenindo roubos de dados, desligamento de equipamentos e demais danos possíveis quando se está fisicamente no local;
- **Proteção de arquivos e dados**: providenciado por autenticação, controle de acesso e antivírus. No processo de autenticação, é verificada a identidade do usuário. No processo de controle de acesso, só são disponibilizadas as transações realmente pertinentes ao usuário. O antivírus garante a proteção do sistema contra programas maliciosos;
- **Proteção de perímetro**: ferramentas de firewall cuidam desse aspecto, mantendo a rede protegida contra invasões de usuários não autorizados.

3.2. Detecção

- **Alertas**: sistemas de detecção de intrusos (IDS - Intrusion Detection System) alertam os administradores e responsáveis pela segurança da rede sobre qualquer sinal de invasão ou mudança suspeita no comportamento da rede que possa significar um padrão de ataque. Os avisos podem ser via e-mail, via mensagem no terminal do administrador, etc.;
- **Auditoria**: periodicamente deve-se analisar os componentes críticos do sistema a procura de mudanças suspeitas. Esse processo pode ser realizado por ferramentas que procuram, por exemplo, modificações no tamanho dos arquivos de senhas, usuários inativos, etc.

3.3. Recuperação

- **Cópia de segurança dos dados (Backup)**: manter sempre atualizados e testados os arquivos de segurança dos dados em mídia confiável e separado dos servidores;
- **Aplicações de Backup**: ferramentas que proporcionam a recuperação rápida e confiável dos dados mais atualizados em caso de perda dos dados originais do sistema;
- **Backup do Hardware**: a existência de backup de hardware (servidor reserva, UPS reserva, linhas de dados reserva, etc.) podem ser justificados levando-se em conta o custo de uma parada do sistema e determinando-se a importância da informática para a organização.

4. Recomendações Contra Ameaças

É possível proteger os ativos computacionais de uma organização seguindo algumas recomendações básicas contra as ameaças oferecidas pelas diversas pragas virtuais que circulam atualmente pela Internet:

- **Atualização do programa antivírus** – recomenda-se que os programas de antivírus sejam atualizados diariamente, principalmente quando um novo vírus for descoberto. Outra medida importante é efetuar as correções de outros programas utilizados, pois 90% dos vírus se aproveitam de falhas nesses programas para se disseminar;
- **Bloquear arquivos executáveis no gateway -** quando uma pessoa deseja enviar um e-mail com um arquivo executável, ela o faz "zipando" tal arquivo. Somente usuários específicos têm reais motivos para enviar, via e-mail, arquivos com tais extensões;
- **Bloqueio de programas de mensagens instantâneas** - os programas de mensagens instantâneas permitem o compartilhamento de arquivos. Assim, o usuário pode ser infectado ao baixar um arquivo, mesmo possuindo um programa de antivírus e um controle de firewall;

- **Autenticação Segura** - sempre que se utilizar a Internet para transações comerciais, verificar se o site visitado pertence a uma instituição conhecida e se utiliza algum esquema de conexão segura (SSL - *Secure Socket Layer*). Existem duas maneiras para verificar se uma conexão é segura ou não. Primeiro através do endereço do site que deve começar com https://. O s antes do sinal de dois-pontos indica que o endereço em questão é de um site com conexão segura e, portanto, os dados do formulário serão criptografados antes de serem enviados. Outra forma de indicação através de algum sinal. O sinal mais adotado nos browsers é o de um desenho de um cadeado fechado. Se o cadeado estiver aberto, a conexão não é segura.

Outras providências para a segurança dos sistemas dizem respeito especificamente aos serviços de correio eletrônico. Dentre elas destacam-se:

- **Visualização de e-mail** - desligar o recurso de visualização do programa de correio eletrônico. Essa função exibe o conteúdo de uma mensagem eletrônica antes de o usuário optar por abri-la de fato. Há vários vírus que são ativados através da pré-visualização da mensagem infectada;
- **Arquivos anexos** - não abrir arquivos anexados diretamente do programa de e-mail. Deve-se salvar primeiramente no disco rígido e, em seguida, passar o antivírus;
- **E-mails de origem desconhecida** - jamais abrir e-mails com arquivos provenientes de desconhecidos. Além dos possíveis estragos causados pelas pragas virtuais, existe o perigo de mensagens maliciosas redirecionarem automaticamente para uma página da *web*, havendo o risco de um hacker roubar informações pessoais do computador;
- **E-mails inesperados de conhecidos** - suspeitar de qualquer arquivo inesperado anexado em um e-mail de algum conhecido. Ele pode ter sido enviado sem o conhecimento da pessoa, que logicamente está com a máquina infectada;
- **Verificar e-mails suspeitos** - no caso de receber uma mensagem de um conhecido, mas que tenha um título ou arquivo anexado estranho, melhor contatar o remetente e perguntar se ele realmente enviou aquele e-mail;
- **Usar criptografia** - se a informação que se deseja enviar por e-mail for confidencial a solução é a utilização de programas de criptografia utilizando chaves e que só podem ser abertas por quem possuir a chave para isso. Alguns programas de criptografia já podem estar embutidos nos programas de e-mails ou podem ser adquiridos separadamente e serem anexados posteriormente aos programas.

5. Principais Tipos de Ataques

5.1. Ataques de Dicionário

- Trata-se de um ataque baseado em senhas que consiste na cifragem das palavras de um dicionário e posterior comparação com os arquivos de senhas de usuários.

5.2. IP Spoofing

- Falsificação de endereço IP
- Utilizada em conjunto com outros ataques para esconder a identidade do atacante.
- Consiste na manipulação direta dos campos do cabeçalho de um pacote para falsificar o número IP máquina que dispara a conexão.
- Quando um host X quer se conectar ao host Y, a identificação é feita através do número IP que está no cabeçalho
- Se o IP do cabeçalho enviado pelo host X for falsificado (IP de um host hacker), o host Y acredita estar falando com o host X

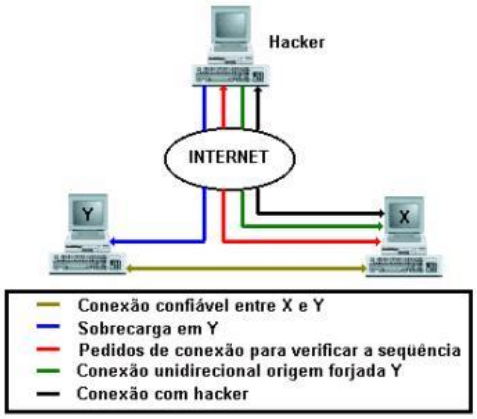

Figura 1 - IP Spoofing

Os pacotes IP possuem um endereço destino e um endereço origem. Normalmente o endereço origem reflete a realidade, mas nada impede que um hacker altere este pacote para que ele pareça ter vindo de outro lugar. Além de enganar o destino, neste caso o computador X, é necessário que se sobrecarregue o computador Y, para que ele não responda às mensagens de X, pois isso poderia cancelar a conexão.
Faz-se necessária, ainda, uma "previsão" do número de sequência mandado por X. Este número é enviado por X ao originador da conexão (supostamente o Y). Mas Y não irá responder, devido à sobrecarga explicada anteriormente. Então o hacker deve prever o número de sequência mandado por X para que

seja enviado novo pacote com estes números em sequência, fingindo novamente ter sido enviado por Y, e forjando a autenticação.
A previsão deste número de sequência é um processo demorado e criativo. Durante a negociação da conexão, os computadores trocam informações para efetuarem o "handshake" ou "aperto de mão". Dentre as informações trocadas estão os números de sequência, que devem ser repetidos para o destino, para que este se certifique da autenticidade da conexão.
O que o invasor faz é o seguinte: enviar, através de um pacote legítimo e com o endereço de origem verdadeiro, vários pedidos de conexão à X. Este responde com um número de sequência para que o invasor o repita e efetue a conexão, mas a máquina de origem (invasor) não tem privilégios e não lhe interessa fechar esta conexão. Então ele não responde a estes pacotes de X, apenas os guarda e verifica seu número de sequência.
Após vários pedidos de conexão com X, o invasor pode "aprender" como X gera seus números e então mandar um pedido de conexão, desta vez com o endereço de origem sendo Y (o computador confiável). Obviamente, o invasor não vai receber os pacotes de X com os números de sequência, pois estes irão para o endereço de origem (computador Y) que nesse momento deve estar sobrecarregado. Com base nos cálculos anteriores, o invasor prevê e manda o número de sequência correto para o computador X, fechando a conexão.

5.3. Ataque de Negação de Serviços

Os ataques de negação de serviço DoS (Denial of Service) têm como objetivos:

- Paralisar um serviço em um servidor;
- Gerar uma grande sobrecarga no processamento de dados de um computador, de modo que o usuário não consiga utilizá-lo;
- Gerar um grande tráfego de dados para uma rede, ocupando toda a banda disponível, de modo que qualquer computador desta rede fique indisponível.

- **Denial of Service (Dos)**: Neste ataque, apenas uma máquina estranha a rede ataca a máquina alvo.

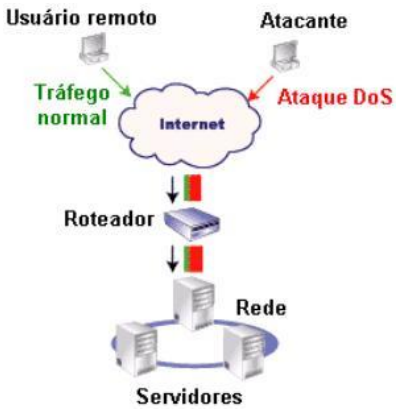

Figura 2 - DoS

- **Distributed Denial of Service (DDos)**: Este ataque utiliza várias máquinas em conjunto para atacar uma máquina alvo. O objetivo do ataque é esgotar algum recurso da máquina alvo.

Figura 3 - DDoS

Vulnerabilidades Exploradas

- Falhas em softwares
- Falhas de Protocolo
- Esgotamento de recursos

- **SYN Flood**

  - Consiste no envio de um grande número de pacotes de abertura de conexão, com um endereço de origem forjado (IP Spoofing), para um determinado servidor.
  - O servidor ao receber os pacotes, coloca uma entrada na fila de conexões em andamento, envia um pacote de resposta e fica aguardando uma confirmação da máquina cliente.
  - Como o endereço de origem dos pacotes é falso, a confirmação nunca chega ao servidor.
  - A fila de conexões no servidor fica lotada e, a partir daí, todos os pedidos de abertura de conexão são descartados e o serviço paralisado.
  - A paralisação persiste até o tempo para o servidor identificar a demora e remover a conexão em andamento da lista.

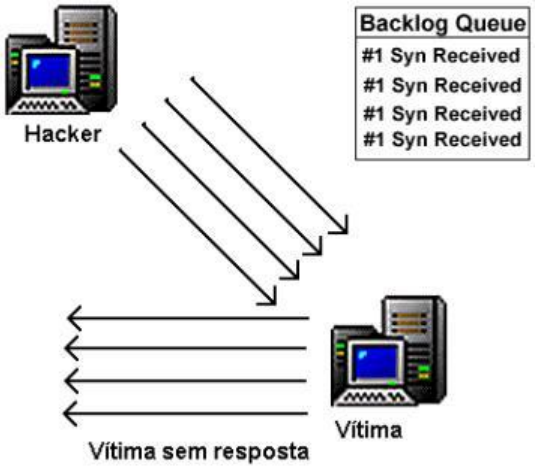

Figura 4 - SYN Flood

5.4. Ataque de LOOP

Consiste em mandar para um host um pacote IP com endereço de origem e destino iguais, ocasionando um loop na tabela de conexões de uma máquina atacada.

5.5. Ataques via ICMP

- O protocolo ICMP (Internet Control Message Protocol) é utilizado no transporte de mensagens de erro e de controle.

- O ICMP não tem garantias se a informação recebida é verdadeira, e por este motivo, um atacante pode utilizar as ICMP para interromper conexões já estabelecidas.

5.6. Ataque de Ping (Smurf Atack)

- Envia pacotes ICMP de echo request para um endereço de broadcast da rede

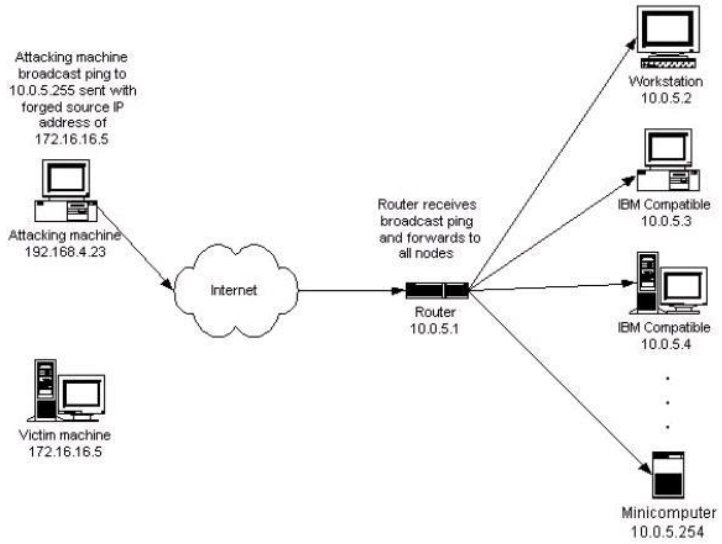

Figura 5 – Ping (Smurf Ataque)

- Redireciona todas as respostas (através de IP Spoofing) para a máquina atacada, causando um volume grande de conexões de *echo reply* para a mesma.

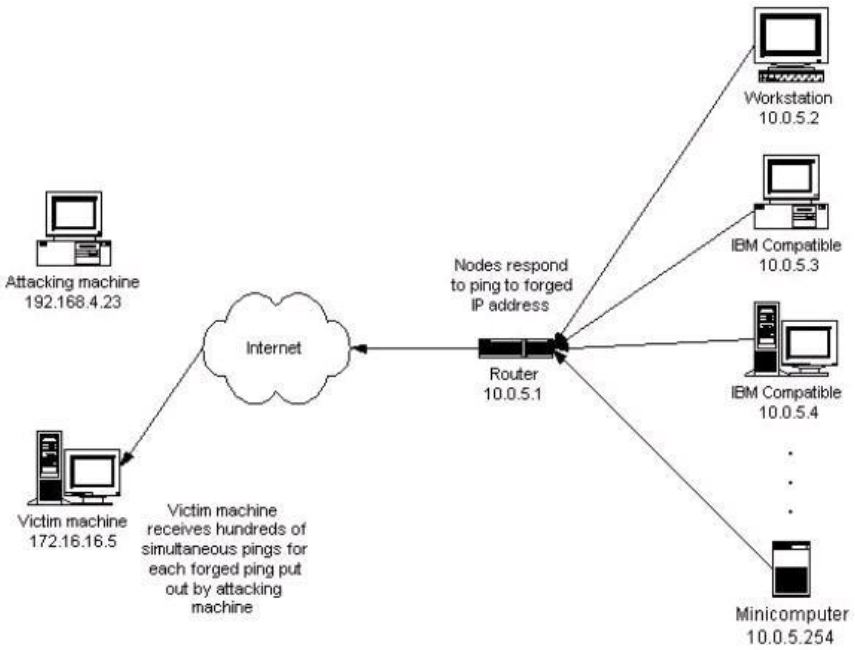

Figura 6 – Redirecionamento via ping

5.7. Ataque de Ping of Death

- Consiste em enviar um pacote IP com tamanho maior que o máximo permitido (65.535 bytes) para a máquina atacada. O pacote é enviado na forma de fragmentos (porque nenhuma rede permite o tráfego de pacotes deste tamanho).

- O dano é causado quando uma máquina destino tenta montar os fragmentos.

6. Engenharia social

A expressão Engenharia Social é muito empregada entre os profissionais das áreas de segurança e de redes para definir a técnica de obtenção de informações importantes de uma empresa, através da manipulação de seus usuários e colaboradores. Essas informações podem ser obtidas pela ingenuidade ou confiança das pessoas. As investidas desta natureza podem ser feitas através de telefonemas, envio de mensagens por correio eletrônico, salas de bate-papo e até mesmo pessoalmente.
Um exemplo típico da utilização da engenharia social é quando uma pessoa desconhecida liga para a empresa / casa de um funcionário e se diz do suporte técnico do seu provedor. Nesta ligação ele convence o funcionário de que sua conexão com a Internet está problemática e pede sua senha para corrigir o problema. Como sempre, o bom senso nestes casos é tudo. A providência a adotar nesse tipo de abordagem é entrar em contato com o help desk do provedor avisando do ocorrido.
Quando falamos de redes corporativas, que são os alvos preferidos desses invasores, o perigo é ainda maior e pode estar até sentado ao lado. Sabe-se que muitos dos ataques sofridos em redes partem de funcionários ou ex-funcionários insatisfeitos. Outro exemplo de ataque de engenharia social diz respeito às entrevistas para emprego, onde muitas vezes o candidato à vaga passa várias informações da empresa em que trabalha. Pode não existir vaga alguma para o cargo. Apenas a empresa, que supostamente abriu a vaga, está tentando levantar informações dos seus concorrentes.
Kevin Mitnick, um famoso hacker declarou em uma entrevista que nada adianta as empresas se preocuparem com seus sistemas de segurança se deixarem de lado o principal perigo: a engenharia social. Mitnick declarou que as empresas ficam expostas aos hackers porque não têm consciência das técnicas de engenharia social que são usadas pelos atacantes mais perigosos, por exemplo, a manipulação. "A maioria das pessoas acha que, por não se considerarem ingênuas, não podem ser manipuladas. Mas nada está mais longe da verdade do que isto", afirmou. Em um trecho do livro “O Jogo do Fugitivo”, de Jonathan Littman – Ed. Rocco, Mitnick descreve como fazia sua engenharia social para descobrir segredos das empresas que invadia: “Aos 13 anos eu já revirava lixeiras perto de companhias telefônicas para encontrar manuais técnicos jogados fora”.
A tecnologia avança e passos largos, mas a condição humana continua na mesma em relação a critérios éticos e morais. Enganar os outros deve ter sua origem na pré-história, portanto o que mudou foram apenas os meios para isso. Em redes corporativas, que são alvos prediletos para os invasores, o perigo é ainda maior e pode estar ao lado. Um colega de trabalho poderia tentar obter sua senha de acesso mesmo tendo uma própria, pois uma sabotagem feita com sua senha parece bem mais interessante do que com a senha do próprio autor.