REDES e SEGURANÇA DA INFORMAÇÃO

Autor: Leonardo Costa Passos

Resumo com o que há de mais importante da disciplina de REDES e SEGURANÇA para provas de Concursos Públicos com foco na banca CESGRANRIO.

Se o conteúdo for útil na sua jornada de estudos, você pode me agradecer fazendo um PIX de um valor que considere justo para a seguinte chave:

leonardx@gmail.com

Table of Contents

1. REDES E SEGURANÇA DA INFORMAÇÃO

Três principais pilares que compõem a base da Segurança da Informação

1. Confidencialidade – Aqui temos o princípio que visa zelar pela privacidade e sigilo dos dados de tal modo que estes devem ser acessados ou visualizados somente por aqueles de direito, ou seja, a informação só deve estar disponível para aqueles com a devida autorização.

2. Integridade (Confiabilidade) – No segundo princípio, temos como objetivo garantir que os dados trafegados sejam os mesmos do início ao fim de um determinado trecho, ou seja, que a mesma mensagem gerada na origem chegue ao destino de forma intacta.

3. Disponibilidade – Nesse princípio, temos como principal objetivo o fato de determinado recurso poder ser utilizado quando este for requisitado em um determinado momento, considerando a devida autorização do usuário requisitante. Desse modo, quando tentamos acessar o site da Receita Federal, por exemplo, no primeiro dia de declaração de Imposto de Renda, teremos a experiência por diversos usuários da violação do princípio da disponibilidade caso estes não consigam acessar o site ou enviar suas requisições por falha no sistema ou volume de acesso que consomem todos os recursos disponíveis, impedindo a utilização por novos usuários.

Outros conceitos também surgem com grande relevância:

1. Autenticidade – O princípio da autenticidade busca garantir que determinada pessoa ou sistema é, de fato, quem ela diz ser. Ou seja, quando utilizamos o simples recurso de inserir as informações de login e senha em um computador, estamos dizendo ao computador que realmente somos o usuário pois ele assume que somente o usuário legítimo em questão possui a informação de login e senha.

2. Não-Repúdio (Irretratabilidade) – Neste princípio, busca-se garantir que o usuário não tenha condições de negar ou contrariar o fato de que foi ele quem gerou determinado conteúdo ou informação, ou ainda que determinado receptor tenha, de fato, recebido certa mensagem. Tal princípio se aplica, por exemplo, na geração de uma autorização para compra de determinado produto e depois, o gestor responsável queira negar a autorização. Entretanto, utiliza-se mecanismos para que não haja possibilidade de haver a referida negação.

3. Legalidade – O aspecto de legislação e normatização é fundamental nos processos relacionados à Segurança da Informação. Desse modo, respeitar a legislação vigente é um aspecto fundamental e serve, inclusive, como base para o aprimoramento e robustez dos ambientes.

2. CONCEITOS DE SEGURANÇA DE REDES

- FURTO DE DADOS: informações pessoais e outros dados podem ser obtidos tanto pela interceptação de tráfego como pela exploração de possíveis vulnerabilidades existentes em seu computador;

- USO INDEVIDO DE RECURSOS: um atacante pode ganhar acesso a um computador conectado à rede e utilizá-lo para a prática de atividades maliciosas, como obter arquivos, disseminar spam, propagar códigos maliciosos, desferir ataques e esconder a real identidade do atacante;

- VARREDURA: um atacante pode fazer varreduras na rede, a fim de descobrir outros computadores e, então, tentar executar ações maliciosas, como ganhar acesso e explorar vulnerabilidades;

- INTERCEPTAÇÃO DE TRÁFEGO: um atacante, que venha a ter acesso à rede, pode tentar interceptar o tráfego e, então, coletar dados que estejam sendo transmitidos sem o uso de criptografia;

- EXPLORAÇÃO DE VULNERABILIDADES: por meio da exploração de vulnerabilidades, um computador pode ser infectado ou invadido e, sem que o dono saiba, participar de ataques, ter dados indevidamente coletados e ser usado para a propagação de códigos maliciosos. Além disto, equipamentos de rede (como modems e roteadores) vulneráveis também podem ser invadidos, terem as configurações alteradas e fazerem com que as conexões dos usuários sejam redirecionadas para sites fraudulentos;

- ATAQUE DE NEGAÇÃO DE SERVIÇO: um atacante pode usar a rede para enviar grande volume de mensagens para um computador, até torná-lo inoperante ou incapaz de se comunicar;

- ATAQUE DE FORÇA BRUTA: computadores conectados à rede e que usem senhas como métodos de autenticação estão expostos a ataques de força bruta. Muitos computadores, infelizmente, utilizam, por padrão, senhas de tamanho reduzido e/ou de conhecimento geral dos atacantes;

- ATAQUE DE PERSONIFICAÇÃO: um atacante pode introduzir ou substituir um dispositivo de rede para induzir outros a se conectarem a este, ao invés do dispositivo legítimo, permitindo a captura de senhas de acesso e informações que por ele passem a trafegar.

3. SEGURANÇA FÍSICA, LÓGICA E CTRL DE ACESSO

3.1 Segurança Física

Diz respeito aos aspectos tangíveis e que, de fato, podem ser tocados.

1. Unidade de Alimentação Ininterrupta (UPS) – São sistemas munidos de baterias que são capazes de armazenar energia e fornecer corrente elétrica aos demais equipamentos por um período limitado. Assim, em caso de ausência de energia, esses equipamentos possibilitam o funcionamento dos equipamentos por um período suficiente em que os administradores da rede podem atuar com vistas a mitigar perdas.

2. Gerador – Seguindo a mesma linha do IPS, o gerador também tem como propósito manter o sistema em operação frente à eventual falta de energia. Entretanto, estamos falando de um período muito mais de sustentação podendo ser prolongado facilmente, uma vez que se utiliza combustível como fonte de energia.

3. Site físico redundante – Busca-se criar outro ambiente que seja capaz de assumir a operação em caso de catástrofe que prejudique o ambiente principal. Para tanto, é muito importante que os dados sejam armazenados e replicados, seja online, ou em fitas e equipamentos disponibilizados em outro local.

4. CFTV – Temos aqui a utilização de câmeras para registro e visualização dos ambientes de uma organização. É um meio eminentemente reativo, uma vez que, na maioria das vezes, é utilizado para gravar o vídeo e ser utilizado posteriormente para análise e auditoria.

5. Travas de Equipamentos – As referidas travas podem ser utilizadas tanto para impedir a utilização de determinados recursos, como bloqueio de portas USB ou unidades de DVD, de forma física, como também no intuito de não possibilitar o furto de notebooks, por exemplo, através das conhecidas chaves kensington, que, literalmente, "prendem" o equipamento em uma localidade.

6. Alarmes – Temos aqui um sistema de aviso que pode ser considerando no seu aspecto físico, como alarmes de incêndio, como no aspecto lógico, como alarmes lógicos de rede.

7. Catracas – A partir da utilização de senhas, crachás, smartcards, entre outros, pode-se restringir o acesso somente a pessoas autorizadas em determinados locais.

8. Sala Cofre – As Salas Cofre são criadas para serem um ambiente seguro para datacenters, implementando diversos tipos de controles de segurança, de acesso, mecanismos de reação a catástrofes, entre outros.

3.2 Segurança Lógica

HARDENING: "endurecer" um servidor de tal modo a deixá-lo mais robusto e seguro.

1. Acesso de ROOT – Não se deve possibilitar a utilização do usuário ROOT de forma direta, ou seja, logando-se como ROOT. Para tanto, deve-se utilizar apenas o método de escalação de privilégios, ou seja, deve-se logar como determinado usuário para posterior mudança de privilégio e consequente

execução de comandos ou aplicações. Isto possibilita a geração de lastros e trilhas de auditorias, além de ser mais uma camada de segurança.

2. Redução de Serviços – Deve-se minimizar ao máximo a quantidade de serviços que estejam rodando em determinado servidor. Isto tem o intuito de reduzir a possibilidade de vulnerabilidades existentes nas aplicações e serviços, bem como aumentar o desempenho do servidor. Portanto, deve-se manter apenas os serviços e aplicações necessárias, nada mais.

3. Limitação de Acesso Remoto – Pode-se configurar o servidor de tal modo que este possibilite acesso remoto de forma segura, ou seja, utilizando protocolos seguros como SSH. Além disso, pode-se restringir a máquinas ou redes específicas que poderão acessar o referido servidor.

4. Atualização do Sistema – É um procedimento fundamental com vistas a reduzir falhas de segurança existente no sistema operacional e aplicações. Assim, deve-se manter e instalar as últimas versões e mais atualizadas.

3.3 Controle de Acesso

Temos aqui um método aplicado tanto no contexto físico e lógico, com vistas a estabelecer barreiras que podem restringir determinados acessos a locais, equipamentos, serviços e dados a pessoas. O controle de acesso está diretamente ligado ao princípio da autenticidade e autorização.

Existem três técnicas de controle e gerenciamento de acesso que são amplamente utilizadas nos ambientes de tecnologia da informação.

- Mandatory Access Control (MAC) – O administrador do sistema é responsável por atribuir as devidas permissões para os usuários. Este modelo utiliza o conceito de "label" para identificar o nível de sensibilidade a um determinado objeto. O label do usuário é verificado pelo gerenciador de acesso e através desta avaliação, é verificado o nível de acesso do usuário e quais recursos ele é capaz de usar.

- Discretionary Access Control (DAC) – Este é um modelo mais flexível quando comparado com o MAC e considerando o usuário que necessita compartilhar o recurso com outros usuários. Nesta técnica, o usuário tem o controle de garantir privilégios de acesso a recursos aos que estão sob seu domínio. Como exemplo desta técnica, podemos citar o próprio sistema de permissão do linux ou windows, por exemplo, em que o próprio usuário pode determinar as permissões do arquivo em que ele tem a posse.

- Role-Based Access Control (RBAC) – Também conhecido como controle baseado em papéis. Nesta técnica, o administrador garantir privilégios de acordo com a função exercida pelo usuário. Esta estratégia simplifica o gerenciamento das permissões dadas aos usuários.

4. AUTENTICAÇÃO E SEUS MECANISMOS

4.1 Fatores de autenticação

1. Algo que você sabe

Nesta categoria, busca-se determinar a autenticidade dos usuários baseado em alguma informação que seja de conhecimento único daquele usuário. Podemos utilizar, como exemplo clássico, a nossa senha de acesso à rede corporativa do local onde trabalhamos.

2. Algo que você tem

Quando se vincula a autenticação à alguma coisa que esteja sob a posse exclusiva do usuário, temos a aplicação desta categoria. Temos diversos exemplo, entre eles, a utilização de um token, crachá, smart card.

3. Algo que você é

Temos aqui, em regra, o mecanismo mais robusto na garantia do princípio da autenticidade. Aqui, uma característica específica e exclusiva dos usuários é utilizada como parâmetro. Os exemplos clássicos que se aplicam aqui é a utilização da biometria.

Um detalhe importante a se mencionar é que a biometria não se restringe à impressão digital. Pode-se utilizar a informação da Íris, padrão de voz, imagem da face, entre outros.

- 2FA (autenticação forte ou duplo faltor de autenticação): dividir a fase de autenticação em duas etapas. Destaca-se que esse processo deve, necessariamente, envolver a combinação de ALGO QUE VOCÊ SABE, ALGO QUE VOCÊ TEM ou ALGO QUE VOCÊ É.
- MFA (MULTIFATOR de autenticação): pode ter 2 ou mais fatores.
- Single Sign On (SSO): possibilitar a determinado usuário consumir recursos de diversos sistemas e serviços a partir de uma única camada de autenticação.
    - Ou seja, no seu serviço por exemplo, uma vez que você chegou e acessou a sua máquina com login e senha, a partir de então, você será capaz acessar os recursos de ponto eletrônico, email, serviço de diretórios, outros sistemas internos, sem ser necessário digitar novamente o login e a senha. Importante destacar que é um serviço que permite a integração de sistemas independentes.
    - O principal protocolo que roda por trás desse recurso é o LDAP, no âmbito corporativo. Uma implementação mais simples é por intermédio dos cookies dos browsers dos dispositivos. O conceito de Single Sign OFF também se aplica no sentido inverso.

4.2 SAML - Security Assertion Markup Language

Um padrão aberto que permite com que provedores de serviços e recursos de identidade passe credenciais de autorização para provedores de serviços

Acesso.gov, da plataforma Gov.br. Basicamente, a partir deste serviço, busca-se eliminar a múltiplas instâncias de identidade de diferentes órgãos e serviços, passando a responsabilidade pelo processo de gestão de identidade de forma centralizada, e, a partir daí, uma vez que o usuário é reconhecido, cabe a cada serviço ou dono do produto (no caso os ministérios), definirem se o mesmo possui ou não acesso para tal.

Bronze, Prata e Ouro. Tal definição reside basicamente do nível de confiabilidade que foi gerado no cadastramento e reconhecimento do usuário. Um modelo federado no fornecimento de informações e bases para a gestão de identidades.

- BRONZE: contempla usuários que cadastraram seu e-mail, responderam algumas perguntas básicas derivadas de uma inteligência de cruzamento de bases do Governo Federal, tendo gerado login e senha.
    - Exemplo, no ato do cadastro, são perguntas de registro do último emprego, data de nascimento, nome da mãe, e outras informações que o Governo Federal possui para reconhecer um cidadão. Caso todas essas perguntas sejam respondidas durante o processo de validação, tem-se um cadastro nível bronze.

- PRATA: utiliza o conceito de reconhecimento do usuário por meio da comprovação de documentos, sejam físicos ou digitais. Assim, caso haja esse reconhecimento em alguma medida, o usuário terá sua credencial nível prata.

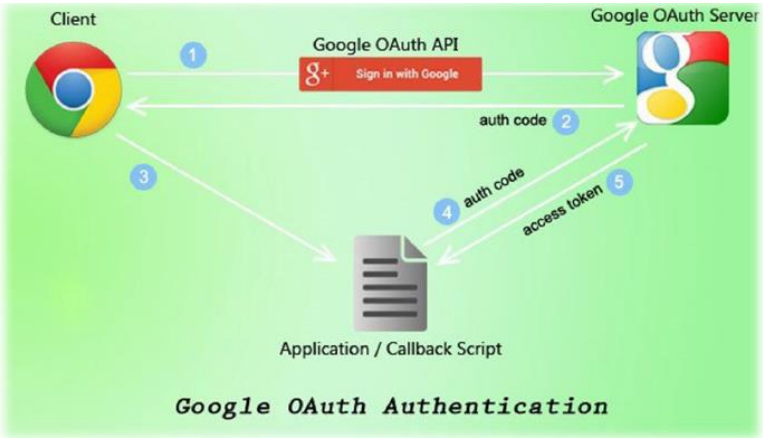
- OURO: envolve reconhecimento biométrico. Basicamente, o principal provedor dessa informação atualmente é o Tribunal Superior Eleitoral, que disponibiliza sua base biométrica para todo o Governo Federal.

Dessa forma, a partir dessa base centralizada de gestão de acesso e credenciais, os demais serviços do Governo Federal podem realizar seus critérios para definição do nível desejado para determinado tipo de serviço. A sensibilidade fica por conta do órgão, ao considerar o tipo de transação que pode ser feita. A título de exemplo, caso seja um serviço de consulta a informações de cunho social ou ainda o status de alguma requisição, pode-se aceitar o nível bronze.

Agora, caso seja um serviço por exemplo, de declaração de Imposto de Renda, com alta sensibilidade e criticidade, exige-se o nível Ouro, e por aí vai.

SAML não especifica ou define um método específico de autenticação no âmbito do Provedor de Identidade. Pode usar o modelo de Login e Senha mencionado anteriormente, ou qualquer outro modo de autenticação, inclusive, incorporando as técnicas de múltiplo fator de autenticação (MFA).

4.3 OAuth



1. Resource Owner - Basicamente é a pessoa que concede acesso aos seus dados. Quando clicamos na opção de login integrado com o Google, por exemplo, teremos que incluir nosso login e senha do google, a partir da chamada de serviço. Caso você tenha uma sessão já aberta do serviço, essa etapa não será necessária. O ponto é, após a inclusão das informações de login e senha, tem-se um processo de autorização, em que você autoriza a aplicação ou serviço, a obter suas informações do servidor OAuth. Na prática, temos aqui o DONO DO RECURSO.

2. Resource Server - Em resumo, é a camada de serviço/integração disponibilizada pelo provedor de identidades. Este serviço, com as devidas camadas de segurança, está exposto para a Internet, caso seja uma API Pública, a exemplo da Google, Twitter, Facebook, ou pode estar em um contexto mais restrito, como foi o caso do serviço do Acesso.Gov que mencionamos, que pode ser utilizado apenas por órgãos de Governo. O que importa é que, nesse processo, é necessário que o serviço que realiza chamada a essa API tenha um token emitido pelo servidor de autorização, que mencionaremos a seguir.

3. Authorization Server - Responsável por autenticação e emissão dos tokens de acesso (Access Token) para os Clients (aplicação requisitante). Estes recursos possuem informações dos Resource Owner (Usuários) e expõe no formato de Claims através do Bearer Token. Autentica e interage com o usuário após identificar e autorizar o client. Não vamos entrar em detalhes técnicos de implementação, mas registro apenas que o Bearer Token é referenciado em chamadas nos cabeçalhos HTTP e pode ser implementado de diferentes formas. No caso, tais chamadas são sempre realizados por meio de HTTPS, uma vez que o token é passado de forma aberta no cabeçalho HTTP. Esse ponto é fundamental para garantir a segurança do Oauth2.0.

4. Client - É a aplicação que interage com o Resource Owner. No caso de uma App Web, seria a aplicação do Browser. Na prática, é a camada que oferece os serviços requisitados pelos usuários.

ETAPA 1 - A aplicação (cliente) solicita autorização para o usuário, para que a aplicação possa interagir e solicitar informações de suas credenciais junto ao provedor de identidade.

ETAPA 2 - O Dono do Recurso (resource owner) realiza a autorização.

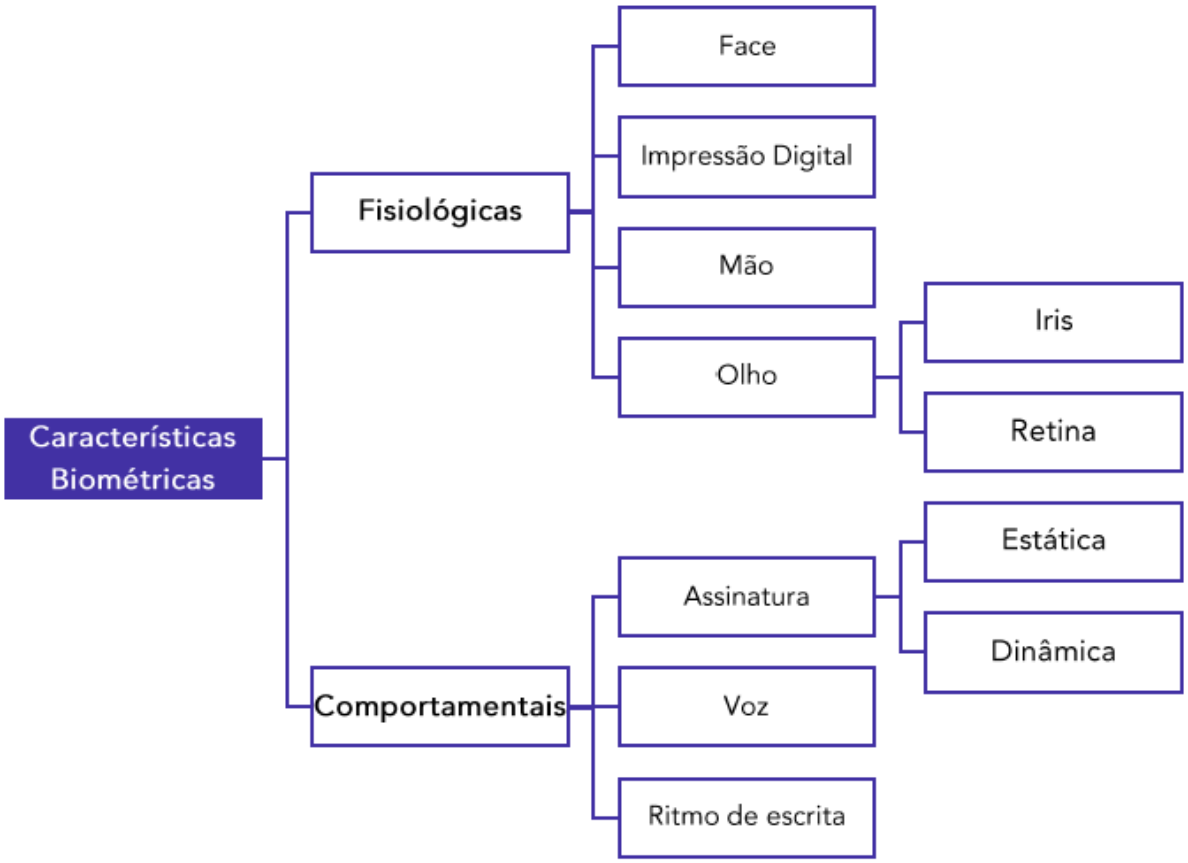
ETAPA 3 - De posse da autorização, esta é encaminhada pelo cliente ao Servidor de Autorização, responsável por viabilizar a passagem das credenciais de acesso aos serviços do provedor.

ETAPA 4 - O provedor de credenciais passa o TOKEN, por meio de uma comunicação segura. De posse desse token, a aplicação poderá acessar os recursos do usuário requisitante. Aqui é onde temos a referência ao nosso BEARER TOKEN, que também será utilizado na etapa 5. São as credenciais em si usadas para acessar os recursos protegidos.

ETAPA 5 - Passa-se o token aos provedores de serviços que detêm os recursos protegidos dos usuários. Na imagem em questão, temos exemplo de serviços da google como o Google Drive ou Google Photo, que passa a ser acessado pelo Client com a devida autorização do usuário Dono do Recurso, realizado no passo 2.

ETAPA 6 - As informações e recursos protegidos são compartilhados com o Cliente. É nessa etapa que é possível, por exemplo, já ter a sua foto integrada com o serviço web requisitado, outras informações, como e-mail, dados de telefone, recursos específicos no Drive, lista de amigos e contatos, entre muitos outros.

4.4 Biometria



5. DIRETRIZES PARA O DEVLP DE SOFTWARE SEGURO

- SENHAS FORTES: as aplicações atuais buscam "obrigar" o usuário a cadastrar senhas que tenham parâmetros mínimos de segurança, conforme elencamos, além de considerar os tamanhos das senhas. Recomenda-se um tamanho mínimo de 8 caracteres, apesar de diversas aplicações aceitarem como quantidade razoável 6 caracteres.

- ATUALIZAÇÃO DE APLICAÇÕES: atualizações disponibilizadas pelos fabricantes não se restringem ao acréscimo de novas funcionalidades e recursos, mas também contemplam correções de bugs, falhas de segurança, entre outros.

- FUZZING (injeção de falhas, teste de validação robusta, teste de sintaxe ou teste de negação): enviar entradas randômicas para a aplicação. Fuzzing injetará informações incomuns como tamanhos diferenciados, caracteres não utilizados e, paralelamente, monitorará o comportamento da aplicação, pois esta poderá travar ou vazar dados de forma indevida. amplamente utilizado no processo de desenvolvimento de softwares seguros devido sua capacidade de detectar defeitos que usuários não descobrem com facilidade. Assim, caso este seja descoberto em ambiente de produção, pode gerar grandes danos aos usuários de determinada aplicação.

5.1 Boas práticas de Código Seguro:

- DOCUMENTAÇÃO – A documentação pode ser extremamente importante no diagnóstico e resolução de forma mais fácil e rápida de problemas.

- VALIDAÇÃO DE ENTRADA – Este processo consiste em inserir dados em pontos de entrada da aplicação e verificar se o comportamento está de acordo com o esperado pelo desenvolvedor, documentando todo o processo. Um típico exemplo é a utilização de máscaras que obrigam o usuário de inserir dados no formato esperado, como o CPF.

- MANIPULAÇÃO DE ERROS – O tratamento de erros é um ponto muito importante no desenvolvimento de aplicações seguras. Essas aplicações sempre estarão sujeitas a erros e, por medida de segurança, é importante que haja um padrão de mensagem de erro para o usuário que não vaze informações a respeito da aplicação, evitando assim que um atacante obtenha essas informações para aprimorar seus ataques. Sob a perspectiva do desenvolvedor em utilizar tais mensagens para correção, recomenda-se que este utilize logs das aplicações e controle de forma segura em um ambiente seguro.

- BASELINE DE CONFIGURAÇÃO DE APLICAÇÃO: As aplicações podem utilizar diversos componentes pelos quais possuem dependências para seu funcionamento. É importante identificar esses componentes e entender como as aplicações fazem uso dessas. A partir de então, pode-se trabalhar em cima dessas aplicações com configurações seguras que darão a devida base e sustentação da aplicação principal.

5.2 SDL (Security Development Lifecycle)

A) SECURE BY DESIGN (SEGURO POR DESENHO)

A arquitetura, o design e a implementação do software devem ser executados de forma a protegê-lo e proteger as informações que ele processa, além de resistir a ataques.

B) SECURE BY DEFAULT (SEGURO POR PADRÃO)

Na prática, o software não atingirá uma segurança perfeita; portanto, os designers devem considerar a possibilidade de haver falhas de segurança. Para minimizar os danos que ocorrem quando invasores miram nessas falhas restantes, o estado padrão do software deve aumentar a segurança. Por exemplo, o software deve ser executado com o privilégio mínimo necessário, e os serviços e os recursos que não sejam amplamente necessários devem ser desabilitados por padrão ou ficar acessíveis apenas para uma pequena parte dos usuários.

C) SECURE BY DEPLOYMENT (SEGURO NA IMPLANTAÇÃO)

O software deve conter ferramentas e orientação que ajudem os usuários finais e/ou administradores a usá-lo com segurança. Além disso, a implantação das atualizações deve ser fácil.

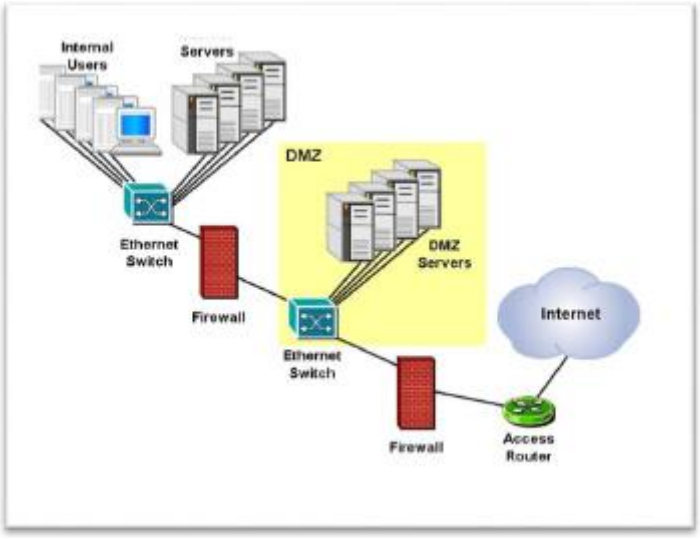
D) COMMUNICATIONS (COMUNICAÇÕES)

Os desenvolvedores de software devem estar preparados para a descoberta de vulnerabilidades do produto e devem comunicar-se de maneira aberta e responsável com os usuários finais e/ou com os administradores para ajudá-los a tomar medidas de proteção (como instalar patches ou implantar soluções alternativas).

6. FIREWALL

Firewall é o elemento de borda da rede que concentra a entrada e saída dos pacotes da nossa rede. Este é um princípio de segurança conhecido como “choke point” ou ponto único de entrada.

- Deverá ser capaz então de interpretar o tráfego que passa por ele e avaliar se a informação é legítima ou maliciosa.



6.1 Conceitos FIREWALL

- **Filtros**
  Capacidade de selecionar o tráfego que será aceito ou bloqueado pelo equipamento. Para tanto, deve-se obter informações dos pacotes a partir das informações dos cabeçalhos dos diversos protocolos utilizados. Pode-se inclusive considerar o estado da conexão conforme será visto posteriormente. É muito importante deixar claro que em nenhuma aplicação de firewall, nativamente, teremos a característica de antivírus, pois esse não é o papel do firewall. Em soluções modernas, temos a implementação de antivírus de forma conjugada em um mesmo equipamento ou appliance, porém, não é o seu papel nativo.

- **Proxies**
  São elementos que atuam como intermediários em uma comunicação. O proxy pode ser utilizado para uma política de acesso de clientes internos aos serviços externos, bem como para acesso de clientes externos aos serviços internos. Desse modo, não haverá comunicação direta entre os clientes e servidores nas duas perspectivas.

- **Bastion hosts**
- É um servidor especializado para fornecer serviços ao público externo. Desse modo, é muito bem customizado, com regras de segurança mais rígidas que mitiguem os possíveis riscos de comprometimento desses servidores. Como regra, é válido lembrar que deve ser instalado exclusivamente os serviços e recursos necessários para o provimento das funcionalidades esperadas, reduzindo assim as possibilidades de surgimento de vulnerabilidades.

- **HoneyPot**
  É um servidor criado especificamente para obter informações a respeito de possíveis atacantes. A ideia é replicar todos os serviços e principais elementos de implementação de serviços neste servidor, porém, sem dados sigilosos que possam gerar dano ou lesão à instituição. Busca-se ainda deixar algumas vulnerabilidades específicas como atrativos para os atacantes. Além disso, implementa-se uma série de elementos com vistas a monitorar, rastrear e obter o máximo de informações do atacante. Como o próprio nome diz, é um verdadeiro pote de mel para atrair os atacantes!

- **DMZ (Demilitarized Zone - Rede de Perímetro)**
  área de serviços comuns que podem ser acessados tanto por usuário externos (Internet – rede não confiáveis) como por usuários internos (Intranet – rede confiável). A grande vulnerabilidade se encontra nos serviços e servidores que possibilitam acessos externos. Desse modo, tira-se esses servidores da rede interna para, caso esses sejam comprometidos, não necessariamente implica em comprometimento dos usuários e serviços internos.

- **NAT**
  Apesar de o NAT ter sido criado para resolver o problema de esgotamento de endereços IPv4, o NAT possibilitou a criação de uma camada de segurança através do conceito de segurança por obscuridade. Dessa forma, usuários externos não conseguem identificar em um primeiro momento os endereços internos de uma rede corporativa pois só terá acesso ao endereço público utilizado por essa rede.

- **VPN**
  A rede privada virtual pode ser criada com uma terminação no firewall. Desse modo, podemos exemplificar com dois cenários. No primeiro, pode-se criar um túnel seguro entre os firewalls da matriz e de uma filial permitindo assim a extensão da rede interna da matriz até a rede da filial através da VPN. Outra aplicação seria o estabelecimento de um túnel seguro a partir de um empregado da empresa que esteja externo à rede. Assim, este pode criar um túnel diretamente no firewall da empresa para ter acesso aos recursos internos.

- Proteção DDoS - Busca ser o elemento de FRONT com alta capacidade de processamento para suportar grandes volumes de requisições que se enquadram nos ataques de negação de serviços distribuídos. Falamos sobre esse assunto em aula específica sobre ataques, caso esteja previsto em seu concurso.

- Firewall de Rede - Conforme já falamos, são os firewalls que atuam na camada de rede e transporte, com características próprias para segurança nessa camada.

- IDS/IPS - Geralmente são soluções acopladas (em paralelo ou em série) e que atuam em conjunto com o Firewall para análises mais elaboradas com foco em assinaturas e comportamentos. Falaremos um pouco mais sobre esse assunto nesta aula.

- Balanceador de Carga - Tem a função de distribuir as requisições entre os servidores de aplicação, com vistas a distribuir de maneira proporcional à capacidade de processamento de cada um deles.

- Web Application Firewall - Conforme já falamos, ele é último elemento de segurança na linha de defesa das aplicações, ficando mais próximos dos servidores de aplicação. Algumas soluções e empresas de segurança avaliam o posicionamento do WAF, às vezes colocando-o de maneira intercalada entre dois balanceadores de carga, ou ainda antes do próprio balanceador de carga, uma vez que o balanceador não é um elemento de segurança propriamente dito.

    - Um Firewall de Aplicação Web (WAF) é projetado para proteger aplicações web filtrando e monitorando o tráfego HTTP entre a aplicação web e a Internet. Ele pode ajudar a mitigar os riscos associados a ataques de injeção SQL, Cross-Site Scripting (XSS), Cookie Poisoning e outros tipos de ataques a aplicações web.

- O dispositivo de segurança capaz de atuar na camada de aplicação e inspecionar o conteúdo das mensagens é conhecido como gateway de nível de aplicação ou FIREWALL PROXY.

- Gateway VPN: Componente de rede responsável por conectar dois ou mais hosts (ou redes) em uma infraestrutura VPN.

- IDS: Sistema de detecção de intrusão, responsável por detectar atividades maliciosas na rede ou no host.

- Firewall sem estado: firewall que realiza a filtragem de pacotes com base nas informações de cabeçalho dos pacotes na camada de rede e camada de transporte.

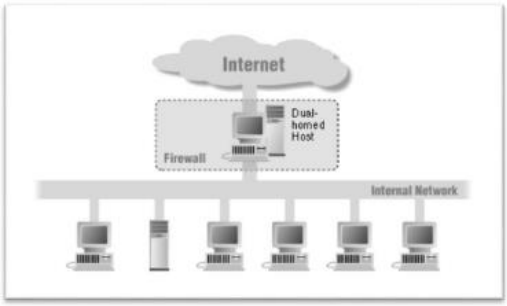
- Firewall com estado: Similar ao firewall sem estado, porém aplica as regras aos fluxos de redes (conexões), e não aos pacotes de forma individual.

    - FIREWALL STATEFUL analisa as conexões que são feitas durante o tráfego de pacotes entre a rede interna e externa, através das sessões que são criadas cada vez que uma conexão for estabelecida e, desta forma. é capaz de impedir o ingresso do tráfego TCP de ACK forjado por entidades hostis e destinado a entidades da rede interna, pois pode verificar o conteúdo do tráfego de conexão de rede.

6.2 Arranjo dos firewalls:

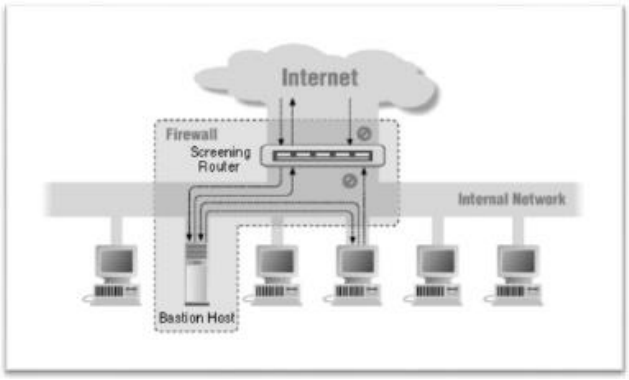
Dual-homed host:

É formado por um elemento que atua como firewall e possui duas interfaces, sendo uma para a rede externa e uma para a rede interna.



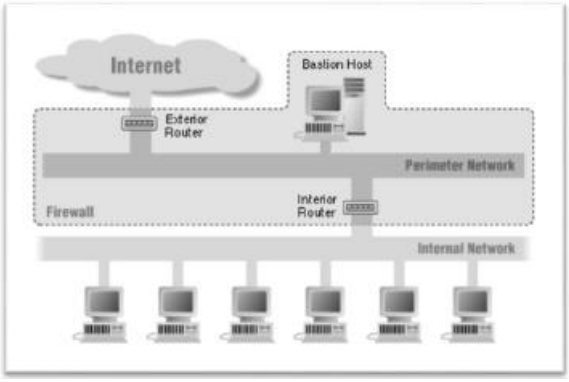
Screened host:

Formado por um firewall e um Bastion host, tipo de servidor que veremos mais à frente. Especificamente customizado para acessos externos a serviços de forma segura.



Screened-subnet host:

Tem-se o modelo específico de criação de uma subrede de segurança (DMZ) ou rede de perímetro, a partir da utilização de dois firewalls. Essa implementação pode ser dar também de forma virtual, onde, a partir de um único firewall físico, cria-se dois virtuais com interfaces físicas distintas que isolam complemente as redes.



6.3 Metodologias de Detecção

- Base de Conhecimento – A partir de uma lista específica de regras ou assinaturas, pode-se comparar determinados acessos ou pacotes que ali trafegam. Assim, se houver um "hit", isto é, caso as informações estejam nessa lista, o equipamento poderá tomar alguma atitude.

- Base de Comportamento – Nesse perfil, temos a análise das características e comportamento dos pacotes ou acessos. A partir de um histórico, pode-se determinar um comportamento considerado normal ou padrão. Caso haja algum acesso ou tráfego de pacote que fuja desse comportamento, considera-se um acesso indevido ou anômalo, cabendo ao equipamento tomar alguma atitude.

    - Tráfego Suspeito Detectado ou Verdadeiro-Positivo - Funcionamento normal do equipamento, onde o tráfego suspeito de fato foi detectado. Varíavel importante e, por isso, queremos aumentar seu resultado.

    - Tráfego Suspeito não Detectado ou Falso-Negativo - Ou seja, era para ser acusado como um tráfego suspeito, porém, não foi acusado. Em termos de analogia, imaginem que um penetra tenha entrado na festa sem ser percebido.

    - Tráfego Legítimo que o Equipamento acusa como suspeito ou Falso-Positivo - Percebam que agora, na nossa analogia, um convidado legítimo foi considerado penetra. Em condições normais e corretas, ele deveria ser capaz de passar sem problemas.

    - Tráfego Legítimo que o Equipamento considera legítimo ou Verdadeiro-Negativo - E para finalizar, temos o comportamento normal de um tráfego legítimo, passando sem nenhum problema pela linha de defesa do sistema. Também é uma varíavel que devemos aumentar sua ocorrência.

6.4 IDS (Intrusion Detecction System)

- ALARME: Quando algo acontece, ele acusa a ocorrência, porém, em regra, não atua diretamente. Um dos principais IDS's utilizados é o SNORT.

- O IDS é um sistema que monitora e analisa o tráfego de rede em busca de atividades suspeitas ou não autorizadas. Ele funciona como um alarme que alerta os administradores de rede quando detecta atividades potencialmente maliciosas, como tentativas de invasão, ataques de negação de serviço (DoS) e outras ameaças.

- Os IDS (Intrusion Detection System) são sistemas passivos de análise de tráfego na rede, já que não são capazes de bloquear o tráfego. Por intrusão, entende-se o monitoramento de eventos em busca de ações suspeitas. São sistemas que usam padrões de assinaturas, análise de fluxo de atividades na rede, entre outros processos de detecção de anomalias. Os mais comuns são os IDS de rede e os User-Based.
-
- O IDS de rede geralmente está entre o servidor e o firewall, até mesmo na DMZ e serve para identificar comportamentos suspeitos. São vários sensores que servem para espalhar as possibilidades de prevenção. É preciso relatar uma central, já que o IDS é nativamente passivo. Já o User-Based pode ser instalado de maneira individual, tanto para computadores corporativos dentro de uma rede empresarial, quanto para endpoints. Nessa utilização, o IDS trabalha com arquivos de logs, ou seja, registros de acessos e também com scanner de portas, para detectar possíveis atacantes.

6.4.1 Categorias de IDS:

- **Baseado em assinatura:**
  Compara o tráfego de rede com assinaturas conhecidas de ataques e ameaças. Quando uma correspondência for encontrada, o IDS gera um alerta.

- **Baseado em anomalia:**
  Estabelece uma linha de base do tráfego de rede normal e identifica desvios significativos, que podem indicar atividades maliciosas.

No entanto, o IDS é um sistema passivo, ou seja, apenas detecta e registra eventos suspeitos, sem tomar medidas para bloquear ou prevenir ataques.

SISTEMA DE DETECÇÃO DE INTRUSÃO:

- O componente responsável por farejar e analisar o tráfego da rede procurando por assinaturas que podem indicar uma atividade de reconhecimento ou tentativa de explorar uma vulnerabilidade.

- monitorar o tráfego de rede para identificar a ocorrência de atividades maliciosas e violações da política de segurança da empresa.

- O componente do perímetro de segurança capaz de executar essa tarefa com base na anomalia e na assinatura do tráfego de rede

O IDS pode ser categorizado ainda em três tipos:

- NIDS (Network-Based Intrusion Detecction System):

Esses sistemas buscam atuar a nível da rede, analisando o tráfego de entrada e saída. É o tipo mais utilizado.

Vantagens:

- Se bem planejado, pode-se utilizar NIDS em pontos estratégicos da rede, reduzindo custos e aumentando o grau de defesa;
- Atuando em modo passivo, não impactam no desempenho da rede;
- Difíceis de serem detectados por atacantes;

Desvantagens:

- o Diante de tráfego intenso, pode não ser muito eficiente;
- o Os switches e roteadores mais modernos já possuem recursos de NIDS embutidos;
- o Incapacidade de analisar informações criptografadas;
- o Incapacidade de bloquear o ataque, restando apenas a detecção;

- HIDS (Host-Based Intrusion Detecction System):
  Atua a nível de um host específico (servidor ou máquina de usuário) buscando analisar características de acesso indevido da máquina, como tentativas de mudanças de perfil, variações dos componentes físicos, entre outros.

  Vantagens:

  - Por monitorarem eventos localmente, os HIDS são capazes de detectar ataques mais específicos quando comparados com os NIDS.
  - Capacidade de tratar dados criptografados. Na origem antes de ocorrer a criptografia e no destino, após a decriptação.
  - Não são afetados por elementos de rede como switches ou roteadores.
  - O log do sistema fornece informações sobre a operação do computador em um determinado momento, ou seja, um registro de seu comportamento ao longo do tempo. Certamente, para um HIDS, essas informações serão bem úteis.

  Desvantagens:
  - Difícil configuração, pois, se deve considerar as características de cada estação;
  - Podem ser derrubados por DoS;
  - Degradação de desempenho na estação;

- IDS baseado em pilhas:
  É um modelo novo de implementação com grande dependência dos fabricantes, variando, portanto, de características. Entretanto, em regras gerais, tem-se a sua integração à pilha TCP/IP, permitindo a análise dos pacotes à medida que estes são desencapsulados nas diversas camadas. Assim, pode-se detectar ataques antes da informação passar para a camada superior, buscando evitar que chega até a aplicação ou Sistema Operacional.

6.5 IPS (Sistema de Prevenção de Intrusões)

O IPS, por outro lado, é um sistema ativo que não apenas detecta ameaças, mas também toma medidas para prevenir ou bloquear atividades maliciosas. Ele funciona como uma extensão do IDS, monitorando o tráfego de rede e, ao detectar um evento suspeito, toma ações corretivas, como bloquear o tráfego, encerrar conexões ou reconfigurar dispositivos de rede.

6.5.1 Categorias de IPS:

- Baseado em assinatura:
  Semelhante ao IDS baseado em assinatura, ele compara o tráfego de rede com assinaturas conhecidas de ataques e ameaças e toma medidas quando encontra uma correspondência.

- Baseado em anomalia:
  Semelhante ao IDS baseado em anomalia, estabelece uma linha de base do tráfego de rede normal e identifica desvios significativos, tomando ações preventivas quando necessário.

6.5.2 Comparação entre IDS e IPS

Embora ambos os sistemas sejam projetados para proteger redes e sistemas de informação, eles têm algumas diferenças fundamentais:

- **Abordagem:**
  O IDS é um sistema passivo que detecta e alerta sobre atividades maliciosas, enquanto o IPS é um sistema ativo que também toma medidas para prevenir ou bloquear ataques.

- **Impacto no desempenho:**
  Como o IPS é mais ativo e envolvido no tráfego de rede, pode ter um impacto maior no desempenho da rede em comparação ao IDS.

- **Complexidade:**
  O IPS geralmente é mais complexo e difícil de gerenciar, já que requer atualizações frequentes de assinaturas e regras para lidar com novas ameaças.

Taxa de falsos positivos:
O IPS pode gerar mais falsos positivos (atividades legítimas bloqueadas) devido à sua natureza proativa

7. ANTISPAM

7.1 Lista de Bloqueio

Método mais simples e básico de implementação. O bloqueio pode ser efetivado tanto em MUA's quanto MTA's baseado em endereços IP de servidores ou usuários suspeitos. Não possui recursos de verificação de conteúdo.

Essas listas podem ser compartilhadas entre diversos nós. Na prática, tem-se nós centralizados e de confiança que estão constantemente atualizando e distribuindo essas listas. Essa técnica está sujeita a geração de falsos positivos, ou seja, endereços legítimos podem ser bloqueados de forma indevida.

- **Blacklists (Listas Negras):**
  Os endereços pertencentes a essas listas serão bloqueados. Todas as demais mensagens estarão liberadas para trafegar. Geralmente, os MTA's e PROXIES abertos figuram nessas listas.
  Como vimos, diversos servidores corporativos são conhecidos e disponibilizam essas listas para livre utilização. Alguns podem cobrar como um serviço de conhecimento especializado.

- **Whitelists (Listas Brancas):**
  Lista permissiva, ou seja, é o inverso da BLACKLIST. Os endereços pertencentes a essas listas são considerados legítimos não sendo necessário a verificação e validação destes.

- **Greylists:**
  É uma técnica que conjuga características das duas técnicas anteriores. São implementadas nos MTA's exclusivamente. Para que uma mensagem seja devidamente enviada, depende de um reenvio por parte de um servidor legítimo.

7.2 Filtros de Conteúdo

Uma das técnicas mais conhecidas e eficientes. Possui a capacidade de atuar de forma dinâmica, incluindo na sua verificação o conteúdo e anexo das mensagens trafegadas. Seu princípio de funcionamento reside na busca de padrões de e-mails categorizados como SPAM.

Possui certa similaridade de funcionamento quando comparado ao IPS para tráfego de rede. Pode-se também gerar falsos positivos. Além disso, tem-se um alto custo de processamento, uma vez que todas as mensagens devem ser verificadas.

O principal filtro utilizado é o filtro bayesiano. Este filtro utiliza probabilidades e estatísticas com o objetivo de aprender de forma dinâmica e prever o futuro, ou seja, detectar possíveis mensagens falsas.

7.3 Técnica SPF (Sender Policy Framework)

Conforme vimos, um tipo de ataque é o spoofing de e-mail, ou seja, a falsificação do remetente. É nesse cenário que foi criado a técnica SPF. O seu princípio básico é buscar garantir a legitimidade do remetente. É capaz de combater a falsificação de endereços de retorno dos e-mails (return-path), através da validação de endereços IP's.

Utiliza o conceito de criação de políticas SPF. Essas políticas visam delimitar os endereços autorizados a enviar e-mails dentro de regras muito bem estabelecidas de aceitação desses e-mails. Essas duas características são independentes, podendo ser usadas em conjunto ou não.

O SPF implementa ainda a técnica SRS (Sender Rewriting Scheme). Permite ao MTA intermediário (relay) reescrever o endereço do remetente no envelope e encapsule o endereço original. Esse fato evita que mensagens redirecionadas sejam bloqueadas por outros MTA's intermediários, uma vez que o endereço do relay é confiável.

7.4 Técnica DKIM (Domain Keys Identified Email)

Possui uma estrutura mais robusta baseada na autenticação com a utilização de chaves públicas. Dessa forma, cada MTA pode utilizar sua chave privada para assinar as mensagens garantindo a autenticidade das mensagens, e chave pública permite a verificação da assinatura. Diferentemente do SPF, essa técnica averigua as informações de cabeçalho e de conteúdo, enquanto o SPF verifica apenas o endereço IP.

7.5 Gerência da Porta 25

Essa é a técnica da vez, ou seja, é a metodologia que tem sido fortemente divulgada e incentivada pelos principais órgãos responsáveis pela segurança na Internet.

É uma ação que depende da participação e interação dos provedores de acesso à Internet e as operadoras de Telecomunicações. Os provedores de acesso WEB implementam a nova regra e política instruindo aos seus clientes a forma de atuação.

A principal característica desse modelo é caracterizar o envio de e-mail em duas fases: Do usuário para o provedor de acesso (Submissão) e comunicação direta entre os servidores de e-mail (Transporte)

7.6 Mail Submission Agent (MSA)

Camada de segurança que atua entre o MUA e o MTA. Como vimos, o SMTP usa como padrão a porta 25, porém, nesse novo modelo, instrui-se a utilização da porta 587. A porta 25 passa a ser reservada para comunicação entre os MTA's de forma autenticada obrigatoriamente.

7.7 Mail Delivery Agent (MDA)

Essa camada é implementada no momento de entrega dos e-mails às caixas postais.

8. ANTIVIRUS

inicialmente os antivírus trabalhavam com as características de assinaturas. Ou seja, busca-se nas aplicações e programas códigos pré-determinados que coincidiam com as bases de vírus existentes.
Assim, ao verificar o fluxo dos programas, um antivírus seria capaz de detectar o código malicioso.

Atualmente, os antivírus já implementam os modelos comportamentais, conforme já mencionamos no contexto do IDS e IPS.

9. DLP – DATA LOSS PREVENTION

- Foco é na privacidade, com vistas a evitar vazamentos de informações ou obtenção desses dados por outros meios internos ou externos, que podem trazer prejuízos ou algum tipo de dano à instituição.

- necessidade do INVENTÁRIO E CLASSIFICAÇÃO DOS DADOS da organização.

9.1 Técnicas DLP

- **Baseado em regras ou Rule-based:**
  A partir da análise do conteúdo de documento, com o uso de regras específicas ou expressões regulares, por exemplo, com vistas a identificar dados pessoais, informações ou referências financeiras, máscaras específicas de cartões ou contas bancárias, ou ainda dados previdenciários, por exemplo. Claramente, é uma abordagem mais inicial e mais fria, com menor poder de detalhamento, mas ajuda a aplicar uma linha de base para filtro comum de tráfego e conteúdo. Essa abordagem é muito eficaz como filtro inicial, pois é fácil de configurar e processar, mas geralmente é combinada com técnicas adicionais.

- **Dicionários ou Dictionaries ou Keyword Matching:**
  A partir do uso de dicionários, taxonomias e regras lexicais, a solução DLP pode identificar conceitos que indicam informações confidenciais em dados não estruturados. Isso requer uma personalização cuidadosa dos dados de cada organização.

- **Correspondência exata de dados ou Exact data matching:**
  Utilizando uma espécie de "impressão digital" dos dados, passa-se à procura de correspondências exatas em um dump ou carga de banco de dados ou ainda de um banco de dados quente, ou seja, em execução. No entanto, esse processo de carga de dados ou acesso a bancos de dados ativos pode prejudicar o desempenho — tem-se, portanto, uma desvantagem dessa técnica.

- **Correspondência exata de arquivos ou Exact file matching:**
  Cria-se um hash de todo arquivo para posterior procura de arquivos que correspondam a esse hash. Essa técnica é muito precisa, mas não pode ser usada para arquivos com várias versões ou ainda para toda a organização. Sua aplicação acaba sendo mais restrita, com a garantia e precisão das funções HASH para identificação de arquivos que são, de fato, os mesmos da organização, no qual busca-se zelar pela sua privacidade.

- **Correspondência parcial de documentos ou Partial document match:**
  Seguindo a filosofia do método anterior, pode-se identificar arquivos onde há uma correspondência parcial; por exemplo, o mesmo formulário preenchido por usuários diferentes.

- **Análise estatística ou Statistical analysis:**
  Pode usar algoritmos de aprendizado de máquina para análise Bayesiana para identificar conteúdo que viola uma política ou contém dados confidenciais. A eficácia dessas técnicas pode ser aumentada alimentando mais dados rotulados ao algoritmo para treinamento. Técnicas como modelo supervisionado também podem ajudar. Importante sempre lembrar que, soluções que usem técnicas de inteligência artificial para monitoramento de comportamentos podem gerar falsos positivos, prejudicando a experiência dos usuários e o uso das aplicações e serviços da instituição. Portanto, a calibragem bem-feita dessas soluções é fundamental.

10. EDR (Endpoint Detection and Response):

- EDR é uma solução de segurança que monitora e protege os dispositivos finais (endpoints), como computadores, laptops e dispositivos móveis, em uma rede.

- A função principal do EDR é detectar ameaças avançadas, analisar e investigar incidentes e responder a ataques em tempo real.

- Essa tecnologia permite às empresas terem maior visibilidade e controle sobre suas redes, detectando atividades suspeitas, identificando e remediando ameaças e fornecendo informações detalhadas sobre incidentes de segurança.

11. WAF (Web Application Firewall):

- O WAF é uma solução de segurança que protege aplicações web contra ataques e vulnerabilidades comuns, como SQL Injection, XSS, CSRF, entre outros.

- Ele funciona como um firewall, monitorando, filtrando e bloqueando tráfego HTTP e HTTPS malicioso para prevenir o acesso não autorizado e a exploração de vulnerabilidades.

- WAFs podem ser implementados como soluções baseadas em nuvem, hardware ou software e são configuráveis para se adequar às necessidades específicas de uma organização.

12. CASB (Cloud Access Security Broker):

- CASB é uma solução de segurança que atua como intermediário entre os usuários de uma organização e os provedores de serviços em nuvem.
- O objetivo do CASB é garantir a segurança e conformidade das informações armazenadas e processadas na nuvem.
- Ele oferece visibilidade do uso da nuvem, controle de acesso, prevenção contra perda de dados (DLP), detecção de ameaças e outras funcionalidades de segurança.
- O CASB pode ser implementado como um serviço em nuvem, gateway on-premise ou uma combinação de ambos, permitindo que as empresas protejam seus dados e cumpram as políticas de segurança, mesmo quando utilizam aplicações e serviços em nuvem.

13. ATAQUES A REDES DE COMPUTADORES

Um ataque pode ser dividido em algumas etapas:

1. Identificação e reconhecimento do ambiente;
2. Identificação de vulnerabilidade;
3. Análise da melhor estratégia;
4. Aplicação do ataque;

- Ataques ativos são os que buscam afetar o funcionamento dos dispositivos de uma rede, seja através da desativação de serviços críticos em servidores, comprometimento de informações do alvo, desperdício de recursos, destruição de informações e até comprometimento físico dos recursos de um sistema. Ataques ativos são exemplificados pela pichação de sites, destruição intencional de dados, desperdício de recursos do sistema (processamento, memória, documentos de impressão), suspensão dos serviços e até desativação por completo de um alvo, e, potencialmente, danos físicos ao equipamento envolvido.
    - Disfarce: Tentativa de se fazer passar por outro usuário ou dispositivo, frequentemente para ganhar acesso não autorizado a informações ou sistemas. É considerado um ataque ativo.
    - Negação de serviço: Tentativa de tornar um recurso de rede indisponível para seus usuários pretendidos, geralmente inundando o recurso com tráfego desnecessário. É considerado um ataque ativo.
    - Modificação de mensagem: Alterar o conteúdo de uma mensagem sem o consentimento do remetente ou do destinatário. É considerado um ataque ativo.
- Ataques passivos são aqueles que buscam obter informações de um sistema, evitando influenciar o funcionamento do sistema afetado. Furtos de senhas, de endereços de e-mails, espionagem digital, fraude bancária e esquemas de desvio de dinheiro são exemplos de ataques do tipo passivo. As entidades que são mais vulneráveis a este tipo de invasão são as instituições financeiras (bancos, companhias de cartão de crédito), instituições privadas (empresas, sociedades) e departamentos governamentais. Estas instituições são mais visadas devido ao tipo de informação que trafegam, pois o mesmo representa ganhos imediatos para o atacante (por exemplo: desvio de fundos, espionagem industrial, hostilidades internacionais).

- Inspeção de conteúdo: Análise do conteúdo das mensagens em busca de informações sensíveis ou de interesse. É considerado um ataque passivo.

- Análise de tráfego: Monitoramento das características do tráfego de rede, como padrões de uso, para ganhar informações úteis. É considerado um ataque passivo.

- controle de acesso visa a impedir o uso não autorizado de recursos, o que requer prévia autenticação de entidades ou indivíduos.

13.1 Testes de penetração (“Pentesters”)

Para se efetuar um pentest é preciso, antes de qualquer coisa, saber o escopo que se quer analisar. Da mesma forma, um atacante pode realizar os ataques com base em algumas premissas. Chamamos de tipo de conhecimento adquirido. Isso porque um atacante pode ser alguém totalmente externo à corporação, pode ser alguém de dentro da corporação, ou ainda algum parceiro que possui informações parciais.

Três premissas básicas de pentests:

- Blackbox

Como o próprio nome diz, é o teste da caixa preta. Nesse tipo de teste, não se tem nenhum tipo de informação da rede ou do ambiente da organização. Então o teste de exploração deve cumprir todas as etapas que apresentamos anteriormente. Começando pela identificação e exploração do ambiente para fins de adquirir conhecimento. Nesse tipo de teste, as principais portas de entrada, como veremos adiante, são os ataques de engenharia social e phishing. Aqui busca-se avaliar, inicialmente, o princípio da segurança de obscuridade, que é justamente não fornecer ou divulgar informações sobre a rede para fora.

- Whitebox

Nesse tipo de ataque, fornece-se ao pentester todas as informações básicas necessárias de conhecimento da rede, pulando, portanto, a etapa de identificação. Esse tipo de ataque busca verificar a robustez de configurações dos equipamentos e a inexistência de exploits conhecidos para as soluções.

- Greybox

É um modelo intermediário. Fornece-se algumas informações básicas que são facilmente descobertas e não fazem parte do escopo do princípio da obscuridade.

- REDTEAM,

trata de profissionais focados em pentester e invasão, em busca de brechas e vulnerabilidades no ambiente de rede e sistemas em geral.

- BLUETEAM

que estará focado em manter o ambiente seguro na perspectiva de defesa, buscando eliminar constantemente as brechas existentes e descobertas pelo próprio time, ou derivado das descobertas do REDTEAM.

Ainda, importante destacar um ponto importante nessa dinâmica que é avaliar como o BLUETEAM reagirá em eventual descoberta de ataque frente a sucessos totais ou parciais do REDTEAM. Avaliar se as políticas e processos estabelecidos serão respeitados e surtirão os efeitos desejados.

13.2 STRIDE

Modelo de ameaças (model of threats), como acrônimo para os 6 tipos de ameaças:

- Spoofing
- Tampering
- Repudiation
- Information disclosure
- Denial of Service
- Elevation of Privilege

Spoofing - Personificar algo ou outra pessoa: Autenticação
Tampering - Modificar dados ou código: Integridade
Repudiation - Alegar não ter realizado uma ação: Não repúdio
Information disclosure - Expor informações a alguém não autorizado a vê-las: Confidencialidade
Denial of Service - Negar ou degradar o serviço aos usuários: Disponibilidade
Elevation of Privilege - Obter recursos sem a autorização adequada: Autorização

13.3 Varredura em Redes – Scan

A varredura em redes é uma técnica que geralmente antecede ataques. Essa técnica visa a obtenção de informações que subsidiarão as ações dos atacantes, como a busca de vulnerabilidades.

Como exemplos, podemos citar a obtenção de informações dos sistemas operacionais dos servidores e de suas atualizações. Caso se verifique que o servidor está com as atualizações defasadas, pode-se buscar vulnerabilidades a serem exploradas.

Outro exemplo de varredura é com vistas a se obter informações dos serviços e portas utilizadas por um servidor. Assim, pode-se utilizar portas "abertas" de forma indevida para gerar acessos indevidos a essa máquina.

Uma das principais ferramentas utilizadas para este fim é o NMAP. Esta ferramenta pode ser facilmente instalada em um dispositivo e a partir deste, insere-se um IP que será o alvo da varredura. Quando executado internamente em uma rede, pode-se obter informações extremamente relevantes do ambiente. Quando rodados externamente, tende a sofrer bloqueio ou filtragem de firewall que reconhecem a varredura.

13.4 Spoofing

- entidades hostis produzirem pacotes com endereços de origem falsificados
- ataques de spoofing se caracterizam pelo atacante fingir ser quem não é, como ocorre no MAC Spoofing ou IP Spoofing.

Diretamente relacionado ao assunto de falsificação ou adulteração de alguma informação com vistas a alteração de algum tipo de identidade ou identificador. Duas são as principais intenções com isso:

1. Se passar por alguma pessoa, instituição ou dispositivo que possua certo grau de confiabilidade e legitimidade para dar confiança à informação enviada. Por exemplo, posso enviar e-mails em nome da Receita Federal para obter informações dos usuários.

2. Esconder informações da origem de tal forma que não seja possível a identificação ou o rastreamento do atacante.

13.5 Man in the Middle

A sua principal característica é a capacidade de se inserir no meio de uma comunicação entre dois nós.

- A forma de ataque na qual o atacante pode interceptar e modificar seletivamente dados comunicados para se passar por uma ou mais das entidades envolvidas em uma comunicação;

Desse modo, o atacante consegue ter acesso a todos os dados trafegados na comunicação. Assim, ele pode ainda agir de algumas formas:

- Pode simplesmente acessar e extrair os dados violando a confidencialidade. Para mitigar esse tipo de ataque, pode-se utilizar a criptografia para tornar os dados ilegíveis;

- Pode modificar os dados, ainda que não consiga ter acesso ao conteúdo de forma direta, violando assim a Integridade. Para mitigar esse tipo de ataque, pode-se utilizar recursos que visam controlar a integridade dos dados como cálculos de verificação ou funções HASH;

    - HASH: assegurar a integridade do conteúdo digital, mostrando que não houve alteração desse conteúdo desde a criação da assinatura digital pelo signatário.

- Pode simplesmente escolher quais mensagens devem ou não chegar até o destino, eliminando as demais, violando assim o princípio da Disponibilidade. Para mitigar esse tipo de ataque, pode-se utilizar técnicas de controle semelhantes às que são implementadas pelo protocolo TCP para confirmação de recebimento;

- Pode usar a identidade do usuário para realizar a autenticação em serviços diversos, violando o princípio da autenticidade. Esse tipo de ataque, também é conhecido como ataque REPLAY. Para mitigar esse tipo de ataque, pode-se utilizar de chaves dinâmicas de sessão com prazo curto e temporário de validade.

13.6 ARP Spoofing ou ARP Poisoning

ARP tem a característica de traduzir endereços IP para endereços MAC. O procedimento padrão do ARP é o envio de um ARP request para todos da rede de tal modo que somente o "dono" de determinado endereço IP deveria responder com a informação de seu endereço MAC através da mensagem ARP REPLY.

Entretanto, no ARP Poisoning, não é isso que acontece. O objetivo aqui é assumir a identidade de outro host da rede com vistas a interceptar o tráfego que deveria ser direcionado à vítima passando a obter informações privadas.

13.7 IP Spoofing

Objetivo de mascarar ataques de rede com o intuito de não deixar rastros que possam incriminar um atacante.

Ou seja, digamos que determinado atacante queira fazer uma varredura em um firewall de uma instituição. Nesse caso, adultera-se os pacotes IP de tal modo a mascarar o IP real do atacante.

O mesmo princípio se aplica quando se objetiva a derrubada de um servidor, através de DoS, por exemplo, que veremos mais à frente.

Se um volume muito grande de requisições parte de um mesmo host, gera-se uma suspeita de que está sendo realizado um ataque. Assim, pode-se adulterar os pacotes dando a impressão que são vários hosts realizando requisições distintas.

13.8 Sniffing: Interceptação de tráfego

Interceptação de tráfego, ou sniffing, é uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de sniffers (Ex. Wireshark e TCPDump). Esta técnica pode ser utilizada de forma:

> Legítima: por administradores de redes, para detectar problemas, analisar desempenho e monitorar atividades maliciosas relativas aos computadores ou redes por eles administrados.
>
> Maliciosa: por atacantes, para capturar informações sensíveis, como senhas, números de cartão de crédito e o conteúdo de arquivos confidenciais que estejam trafegando por meio de conexões inseguras, ou seja, sem criptografia.

Note que as informações capturadas por esta técnica são armazenadas na forma como trafegam, ou seja, informações que trafegam criptografadas apenas serão úteis ao atacante se ele conseguir decodificá-las.

13.9 Força Bruta

Busca descobrir uma senha ou alguma outra informação através do método de tentativa e erro de forma exaustiva.

O grau de desempenho desse ataque está diretamente relacionado à capacidade de processamento computacional de um atacante.

As tentativas de adivinhação baseiam-se em:

- Dicionários de diferentes idiomas e que podem ser facilmente obtidos na Internet;
- Listas de palavras comumente usadas, como personagens de filmes e nomes de times de futebol;
- Substituições óbvias de caracteres, como trocar "a" por "@" e "o" por "0"';
- Sequências numéricas e de teclado, como "123456", "qwert" e "1qaz2wsx";
- Informações pessoais, de conhecimento prévio do atacante ou coletadas na
- Internet em redes sociais e blogs, como nome, sobrenome, datas e números de documentos.

13.10 Desfiguração de página (Defacement)

Desfiguração de página, defacement ou pichação, é uma técnica que consiste em alterar o conteúdo da página Web de um site. Possui um caráter unicamente de vandalismo.

13.11 Phishing

Copiar uma página legítima e divulgar às vítimas para obtenção de informações privadas. O principal meio de divulgação das páginas falsas é por e-mail através de SPAM.

Assim, pode-se gerar um aviso de um banco, por exemplo, para que a vítima acesse a página e regularize determinada condição. A vítima, ao clicar no link enviado pelo atacante, será redirecionado para a página falsa, sendo um clone da página legítima do banco.

A vítima então acaba incluindo os seus dados bancários de acesso à conta na página falsa dando acesso ao atacante à sua conta bancária. Assim, é muito importante estarmos atentos às URL's, de fato. Verificar sempre se estas correspondem aos endereços legítimos dos sites.

Outro conceito atrelado ao Phishing é o Spear Phishing. Esse tipo de ataque é similar ao Phishing com a diferença de ter um destino específico, como uma empresa ou órgão governamental, produzindo assim um ataque customizado através da falsificação de e-mails.

13.12 Negação de Serviço (Denial of Service – DoS)

Para se retirar um serviço do ar, deve-se esgotar algum tipo de recurso de determinado sistema que inviabilize o atendimento de novas requisições. Isso pode acontecer por uma indisponibilidade total (desligamento ou travamento de sistemas), ou com funcionalidade intermitente, de tal modo que o sistema fique tão lento que inviabilize sua utilização.

Este tipo de ataque pode se dar das seguintes formas:

- Envio de um grande volume de requisições para um serviço específico (como acesso à uma página WEB), consumindo seus recursos de processamento, quantidade de sessões suportadas, banda de internet, memória, disco, entre outros;

- Exploração de vulnerabilidade em programas causando sua indisponibilidade.

- *SYN flooding* consiste no envio de uma grande quantidade de pacotes de sincronia de um cliente mal intencionado a um servidor: o servidor responderá a todos estes pacotes de sincronia, e ficará no aguardo da confirmação de conexão com todas as solicitações, que não serão respondidas pelo cliente. Como todas as conexões disponíveis do servidor atacado serão dedicadas ao cliente mal intencionado, outros clientes bem intencionados não conseguirão se conectar com o servidor.

- SMURF ATTACK: se envia um pacote (conhecido como ICMP Echo Request) para o broadcast de uma rede, fazendo com que todos os computadores dessa rede respondam para esse direcionado broadcast, causando crash da mesma.

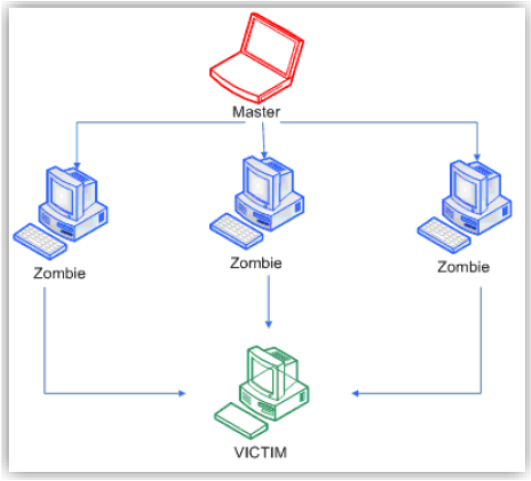
13.13 Negação de Serviço Distribuído (Distributed Denial of Service)

Antes de efetuar esse tipo de ataque, um atacante precisa controlar uma rede de computadores zumbis, muitas vezes chamadas de botnets. Desse modo, o atacante envia o comando para que todos os dispositivos controlados enviem requisições de forma simultânea a um host específico (vítima), gerando indisponibilidade do serviço.

Este tipo de ataque tem um alto grau de sucesso devido à grande dificuldade de se detectar e reagir a tempo a esse tipo de ataque. Na maioria das vezes a ação é reativa com vistas a mitigar o prejuízo. A principal reação se dá através do contato com a operadora responsável pelo provimento do acesso à Internet com vistas a bloquear determinada região ou rota BGP que está originando esse grande volume de requisições.

- Para identificar esse ataque, os componentes de segurança devem utilizar técnicas para determinar anomalia de tráfego na rede.

A figura abaixo nos traz uma representação visual de um ataque do tipo DDoS



13.14 DrDoS (Distributed Reflection Denial of Service)

DrDoS significa ataque de negação de serviço por reflexão distribuída. As técnicas de DrDoS geralmente envolvem várias máquinas de vítimas que involuntariamente participam de um ataque DDoS ao alvo do invasor. As solicitações para as máquinas do host da vítima são redirecionadas ou refletidas dos hosts da vítima para o destino. Normalmente, eles também provocam uma quantidade amplificada de tráfego de ataque.

Distributed Reflected Denial-of-Service (DRDoS) é semelhante ao DDoS, mas onde o atacante pode enviar pacotes forjados para outra rede e permitir que esta rede realize o ataque. Por isto, as máquinas zumbis geram pacotes com uma solicitação de resposta, que possuem o endereço do alvo no campo de origem dos pacotes.

O anonimato é uma vantagem do método de ataque DrDoS. Em um ataque DrDoS, o site de destino parece ser atacado pelos servidores da vítima, não pelo invasor real. Essa abordagem é chamada de falsificação. Envolve falsificar a origem da solicitação.

A amplificação é outra vantagem do método de ataque DrDoS. Ao envolver vários servidores de vítimas, a solicitação inicial de um invasor produz uma resposta maior do que a enviada,

aumentando assim a largura de banda do ataque, aumentando a probabilidade de causar uma interrupção de negação de serviço.

13.15 Ransomware - Sequestro de dados

Um ataque que tem ganhado cada vez mais expressão é o de sequestro de dados. Neste tipo de ataque, o atacante obtém acesso privilegiado ao sistema da vítima e realiza criptografia dos dados da vítima. Assim, os dados passam a estar inacessíveis, dependendo da inserção da chave criptográfica para decriptar os dados.

O atacante então exige um valor a ser pago para disponibilização da chave à vítima para que ela possa acessar seus dados novamente.

Além disso, o atacante geralmente agrega ameaças de destruição dos dados e que o "resgate" deve ser pago em um período específico, geralmente, 3 dias.

A imagem a seguir representa um exemplo desse tipo de ataque:

14. MALWARES (MALICIOUS SOFTWARE)

formas que esses MALWARES infectam os dispositivos:

- Exploração de vulnerabilidades intrínsecas em programas:
  - Aqui temos a importância de manter programas atualizados e sempre utilizar programas legítimos.

- Pela execução automática de mídias removíveis infectadas, como pen-drive:
  - Recomenda-se desabilitar a auto execução de mídias para evitar este tipo de ataque. Caso tenha um arquivo infectado, ele dependerá de execução para se propagar, ou seja, sem a auto execução, já teremos um fator de dificuldade para o sucesso do MALWARE;

- Pelo acesso a Páginas Web Maliciosas:
    - Vários pontos podem ser explorados ao se acessar uma página desse tipo, seja através da exploração de vulnerabilidade do próprio Browser, ou downloads de arquivos infectados, entre outros;

- Pela ação direta de atacantes que ao invadir os computadores, inserem códigos e programas indesejados;
    - Devemos ter senhas de acesso mais complexas, controlar as portas de acesso aos dispositivos, entre outras técnicas que dificultam o acesso indevido às máquinas. A esses procedimentos damos o nome de HARDENING. Ou seja, busca-se "endurecer" o servidor de tal forma que ele não fique tão vulnerável;

14.1 VÍRUS

Código que pode ser representado por um programa ou parte de um programa com a capacidade de gerar cópias de si mesmo e se inserindo em outros programas ou arquivos, além de executar tarefas específicas no computador da vítima como deleção de arquivos, instalação de outros programas, redução de configurações de segurança, desestabilização do sistemas e ocupação de espaço de armazenamento.

Um termo chave do VÍRUS é que este depende de uma ação direta do usuário ou do SO em termos de execução do programa ou abertura de um arquivo infectado. Então o simples fato do arquivo está no seu computador não implica que você tenha necessariamente sido infectado.

Vírus de Boot:
Infecta a área de inicialização dos sistemas operacionais, também conhecido como MBR (Master Boot Record) do disco rígido. Esse tipo de vírus não corrompe arquivos específicos, mas sim, todo o disco. Os antivírus comuns de sistemas operacionais não são capazes de detectar esse tipo vírus, sendo necessário uma varredura antes da inicialização do sistema para sua detecção.

Vírus de Arquivo:
Infecta arquivos de programas executáveis, geralmente, nas extensões .EXE e .COM. Ao se executar o referido programa, ativa-se o vírus.

Vírus Residente:
Este é carregado diretamente na memória RAM do SO toda vez que o SO é iniciado. Este tipo de vírus pode ser extremamente danoso, bloqueando acessos à memória RAM, interromper determinados processos e funções a serem executadas e inclusive, alterar tais funções para fins maliciosos.

Vírus propagado por e-mail:
recebido como um arquivo anexo a um e-mail cujo conteúdo tenta induzir o usuário a clicar sobre este arquivo, fazendo com que seja executado. Quando entra em ação, infecta arquivos e programas e envia cópias de si mesmo para os e-mails encontrados nas listas de contatos gravadas no computador.

Vírus de script:
escrito em linguagem de script, como VBScript e JavaScript, e recebido ao acessar uma página Web ou também por e-mail, como um arquivo anexo ou como parte do próprio e-mail escrito em formato HTML. Pode ser automaticamente executado, dependendo da configuração do navegador Web e do programa leitor de e-mails do usuário.

Vírus de macro:
tipo específico de vírus de script, escrito em linguagem de macro (série de comandos e instruções que podem ser agrupadas em um simples comando), que tenta infectar arquivos manipulados por aplicativos que utilizam esta linguagem como, por exemplo, os que compõe o Microsoft Office (Excel, Word e PowerPoint, entre outros). Geralmente são escritas em linguagens como Visual Basic para Aplicações (VBA) e ficam armazenadas nos próprios documentos. Este é o motivo das MACROS serem bloqueadas nativamente por estes programas devendo o usuário habilitá-la manualmente para macros legítimas.

Vírus de telefone celular:
vírus que se propaga de celular para celular por meio da tecnologia bluetooth ou de mensagens MMS (Multimedia Message Service). A infecção ocorre quando um usuário permite o recebimento de um arquivo infectado e o executa. Após infectar o celular, o vírus pode destruir ou sobrescrever arquivos, remover ou transmitir contatos da agenda, efetuar ligações telefônicas e drenar a carga da bateria, além de tentar se propagar para outros celulares.

14.2 WORM

Possui como principal característica a capacidade de se propagar pela rede de computadores através do envio de cópias de seu código a outros dispositivos. Além disso, o Worm busca explorar vulnerabilidades específicas dos sistemas, diferentemente do Vírus.

Devido ao seu grande poder de propagação na rede, acaba por gerar um grande consumo de processamento e banda, prejudicando bastante a qualidade dos sistemas e da rede. Pode ter uma propagação a nível global ao longo da Internet nos casos da existência de vulnerabilidades presentes nos mais diversos sistemas.

14.3 SPYWARE

Foca na obtenção de informações de um host ou sistemas através do monitoramento de suas atividades. Assim, pode-se enviar informações a um terceiro qualquer para consolidar os dados obtidos e tentar coletar informações relevantes para outros fins.

Assim como já vimos anteriormente, pode ser dividido em uso legítimo e malicioso. O primeiro, pode ser instalado pelo próprio usuário para monitorar ações em seu dispositivo por outros usuários ou ainda com o consentimento deste para monitoramento de uma instituição de trabalho, por exemplo.

Já o modo malicioso fere o princípio da privacidade da pessoa ou do usuário, podendo ser obtidas senhas de acesso e outras informações privilegiadas.

Keylogger:
Capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Sua ativação, em muitos casos, é condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de Internet Banking.
Por esse motivo, foi desenvolvido o teclado virtual, de tal modo que o usuário não necessita digitar senhas diretamente em sem teclado, mas sim, através de cliques do mouse. Assim, caso haja um Keylogger na máquina do usuário, este não será capaz de coletar as informações digitas.

Screenlogger:
similar ao Keylogger é capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em

teclados virtuais, disponíveis principalmente em sites de Internet Banking. Desse modo, podemos considerar inclusive como sendo uma evolução do Keylogger.
Para evitar este tipo de ataque, foi desenvolvido teclados virtuais que "embaralham" os caracteres em cada acesso, ou seja, a sequência de digitação da senha nunca será a mesma, inviabilizando, portanto, a dedução dos números e letras pela posição do teclado virtual.

Adware:

Projetado especificamente para apresentar propagandas direcionadas ao perfil do usuário. Pode ser usado para fins legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos (como o google adwords). Aqui, muitos usuários não concordam com essa política do google, entretanto, ao instalar seu navegador ou SO ou outros sistemas, muitos de nós damos o devido consentimento ao marcar a opção "Eu li e aceitos os termos."

- Também pode ser usado para fins maliciosos, quando as propagandas apresentadas são direcionadas, de acordo com a navegação do usuário e sem que este saiba que tal monitoramento está sendo feito.

- Alguns Adwares mais complexos e danosos possuem a capacidade de sequestrar e invadir os navegadores dos usuários. Assim, altera-se páginas iniciais de acesso, mecanismos de pesquisas, redirecionamentos automáticos, entre outros, com a finalidade de controlar, até certo ponto, a navegação do usuário.

- Importante delimitar a ação desse tipo de ataque, pois a finalidade não é criar zumbis ou inserir vírus, entre outros.

14.4 CAVALO DE TRÓIA (TROJAN)

- Programas que entram no sistema operacional com outros programas escondidos dentro de si.

- O usuário recebe um programa imaginando que este foi desenvolvido para determinado propósito, porém, escondido dentro dele, há um código malicioso.

- Um detalhe a ser observado é que, de fato, o programa principal executará as operações esperadas trazendo alguma credibilidade ao usuário para que ele não desconfie.

- Típicos cavalos de Tróia que são amplamente divulgados são programas para "craquear" produtos originais através da geração de códigos ou números de série.

- Outros tipos bastante difundidos são aqueles mascarados sobre produtos desenvolvidos para aumentar o desempenho de seu computador ou até mesmo antivírus ou antimalwares. Ele de fato pode realizar buscar e achar aspectos legítimos, porém, sempre mascarando seu verdadeiro propósito com algum malware.

14.5 BACKDOOR

- Algum meio para acesso futuro de um atacante.

- A ideia aqui não é somente invadir um sistema, mas manter o acesso.

- O programa que permite o retorno de um invasor a um equipamento comprometido, por meio da inclusão de serviços criados ou modificados para esse fim, é classificado como BACKDOOR.

- Após alguma invasão, como por exemplo, um cavalo de Tróia, o atacante instala um backdoor que abrirá alguma porta no dispositivo para acesso futuro, podendo agregar outros códigos e tomar controle total da vítima.

14.6 ROOTKIT

- Conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.

- Seu foco não é na invasão em si, mas sim na manutenção do acesso indevido.

Busca realizar operações como:

1. Remover evidências de registros em arquivos de logs;
2. Instalar outros códigos maliciosos, como backdoors;
3. Esconder atividades e informações como arquivos, diretórios, processos, entre outros;
4. Mapear potenciais vulnerabilidades a serem exploradas em outros computadores na rede a qual a vítima está inserida e capturar informações através da interceptação de tráfego;

Tais ações são possíveis após a invasão e escalada de privilégios em um Sistema Operacional, obtendo o maior nível de acesso possível em um computador. Nos casos de ambientes UNIX, temos o modo ROOT. Para ambientes Windows, temos o modo SYSTEM.

Diversos tipos de Rootkits podem ser carregados em um sistema, como por exemplo:

- Kernel Rootkits: carregado no Kernel do SO;
- Virtual Rootkits: Agem na camada de virtualização de um sistema;
- Firmware Rootkit: Agem nos componentes de hardware, como placas de vídeo, controladoras, etc;
- Library Rootkit: Carregado no módulo de bibliotecas de um SO.

14.7 BOT e BOTNET

- Bot é um código engaja um computador em uma armada que permite a realização de tarefas de forma automatizada para atacar alvos determinados por criminosos cibernéticos, sem o conhecimento do dono do computador.

- É um código que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Um computador infectado vira zumbi em um rede (BotNet)

A sua propagação se dá de modo semelhante ao Worm, através da replicação de seus códigos e envio pela rede, e-mail ou outros meios.

Desse modo, havendo o controle por parte do invasor, este poderá disparar diversos tipos de ataques utilizando o sistema da vítima, como ataques de negação de serviço, furto de dados de outras vítimas e envios de SPAM, contando com a dificuldades de se rastrear a origem real do ataque.

Esses BOTS são conhecidos como zumbis (Zombies), uma vez que tal programa fica inerte até que haja o interesse do invasor para utiliza-lo para algum fim específico.

Desse modo, ao se construir diversos controles de vários BOTS, cria-se, portanto, uma BOTNET, ou seja, uma rede de BOTS ou zumbis, que podem, por exemplo, serem usadas em ataques DDoS. A ideia é controlar cada vez mais vítimas com vistas a potencializar ainda mais os ataques. Essas redes são inclusive comercializadas no mercado negro.

Códigos Maliciosos							
	Virus	*Worm*	*Bot*	*Trojan*	*Spyware*	*Backdoor*	*Rootkit*
Como é obtido:							
Recebido automaticamente pela rede		✓	✓				
Recebido por *e-mail*	✓	✓	✓	✓	✓		
Baixado de *sites* na Internet	✓	✓	✓	✓	✓		
Compartilhamento de arquivos	✓	✓	✓	✓	✓		
Uso de mídias removíveis infectadas	✓	✓	✓	✓	✓		
Redes sociais	✓	✓	✓	✓	✓		
Mensagens instantâneas	✓	✓	✓	✓	✓		
Inserido por um invasor		✓	✓	✓	✓	✓	✓
Ação de outro código malicioso		✓	✓	✓	✓	✓	✓
Como ocorre a instalação:							
Execução de um arquivo infectado	✓						
Execução explícita do código malicioso		✓	✓	✓	✓		
Via execução de outro código malicioso						✓	✓
Exploração de vulnerabilidades		✓	✓			✓	✓
Como se propaga:							
Insere cópia de si próprio em arquivos	✓						
Envia cópia de si próprio automaticamente pela rede		✓	✓				
Envia cópia de si próprio automaticamente por *e-mail*		✓	✓				
Não se propaga				✓	✓	✓	✓
Ações maliciosas mais comuns:							
Altera e/ou remove arquivos	✓			✓			✓
Consome grande quantidade de recursos		✓	✓				
Furta informações sensíveis			✓	✓	✓		
Instala outros códigos maliciosos		✓	✓	✓			✓
Possibilita o retorno do invasor						✓	✓
Envia *spam* e *phishing*			✓				
Desfere ataques na Internet		✓	✓				
Procura se manter escondido	✓				✓	✓	✓

15. ATAQUES NA CAMADA DE APLICAÇÃO

15.1 XSS (Cross-site Scripting):

O XSS é uma técnica de obter informações do usuário após este ser persuadido a entrar em um site com scripts que são executados no computador da vítima. Uma vez que se executa tal script, com os devidos privilégios de usuário, pode ser executadas rotinas diversas no dispositivo.

Esse tipo de ataque tem crescido bastante, se tornando como um dos principais na atualidade.

Dois são os principais tipos de ataques XSS. O primeiro, é conhecido como não persistente e o segundo, persistente.

Esses ataques exploram uma vulnerabilidade no servidor de aplicação de determinado sistema e modificam o código inserindo código malicioso. A partir de então, todos que entrarem nesse link, que até um primeiro momento é legítimo, será afetado.

Os ataques de XSS são frequentemente utilizados para causar danos, seja através da obtenção de dados dos usuários, como o prejuízo de imagem da instituição que está "hospedando" o código malicioso.

Percebam que, apesar do código residir no servidor de aplicação, a atuação do XSS não é contra o servidor de aplicação, mas sim, aos usuários daquele serviço, onde de fato o script será executado.

Assim, pode-se sequestrar as sessões dos usuários através de cookies, alterar códigos HTML no lado do cliente, redirecionar usuários para sites maliciosos (phishing) e alterar os objetos para captura de entradas de usuários.

Para se evitar esse tipo de ataque podemos extrair do guia OWASP, o seguinte.

"Deve-se separar os dados não confiáveis do ativo no navegador".

Como exemplos, temos:

- Filtrar adequadamente todos os dados não confiáveis com base no contexto HTML (corpo, atributo, Javascript, CSS ou URL)
- Criar Listas Brancas ou de entradas positivas. Entretanto, não possui uma defesa completa, uma vez que muitas aplicações requerem caracteres especiais em sua entrada. Tal validação deve, tanto quanto possível, validar o tamanho, caracteres, formato, e as regras de negócio sobre os dados antes de aceitar a entrada.
- Para conteúdo do tipo RICH, considere o uso de bibliotecas de auto sanitização. Ou seja, deve-se realizar filtros que consigam remover TAGS potencialmente danosa, validando de forma adequada as entradas de dados dos usuários.
- Implementação de CSP – Content Security Policy em todo o site."

Podemos encontrar ainda diversas técnicas em sites especializados de segurança, o qual correlaciono também a seguir:

Para minimizar a vulnerabilidade de cross-site scripting, os desenvolvedores/proprietários de sites devem:

- Garantir que qualquer página em seu site que aceite entrada do usuário filtre as entradas de código, como HTML e JavaScript.
- Faça a varredura em busca de vulnerabilidades de aplicativos da Web e conserteas de acordo.
- Atualize seu site e software de servidor para evitar a exploração futura de vulnerabilidades que podem ser visadas por um ataque XSS.

Para evitar ser vítima de um ataque XSS, os usuários individuais devem:

- Desativar os scripts em páginas em que eles não são necessários ou desativá-los completamente.
- Evitar clicar em links de e-mails ou postagens suspeitas em painéis de mensagens, pois eles podem levar a páginas comprometidas. Acessar sites diretamente digitando o URL em seu navegador, em vez de por meio de uma fonte ou link de terceiros.
- Manter o software atualizado para se beneficiar das últimas correções de bugs e patches de segurança. Atualizar regularmente o software reduzirá significativamente as vulnerabilidades que deixam um site ou aplicativo aberto a ataques XSS.
- Fazer a auditoria de aplicativos para determinar quais são necessários e quais raramente são usados. Livrar-se de aplicativos que você não usa reduz o número de vulnerabilidades potenciais.

Ainda, o XSS possui uma classificação própria, dividida em três categorias. Vejamos:

1. Cross-site scripting armazenado (XSS Persistente ou armazenado)

Tem a característica de ser o mais danoso. Envolve uma entrada do usuário direto para o processamento em uma página web. Geralmente associada a fóruns de mensagens ou redes sociais, por meio dos comentários e interações. O atacante, conforme vimos, injeta o código malicioso no servidor, provedor do serviço. Essa carga está armazenada no servidor e será processada, tão logo seja acessado, pelo cliente no navegador da própria vítima.

2. Cross-site scripting refletido (XSS Não persistente ou refletido)

Não sendo o mais danoso, porém, o mais comum. Nesse caso, a carga não é armazenada no servidor, e, portanto, deverá fazer parte da carga envolvida na requisição do usuário. Por isso é conhecido como refletido, pois parte do próprio usuário, para ele mesmo. Na prática, a resposta HTTP inclui a carga útil da solicitação HTTP.
Tal processo geralmente é deflagrado por uma interação anterior da vítima com algum site ou serviço malicioso. Por não ser um ataque persistente, o invasor precisa que a carga útil maliciosa seja repassada a cada vítima. Vejam a diferença do XSS persistente, onde basta que a carga útil maliciosa seja inserida no servidor, não tendo que ser propagada para cada potencial vítima.

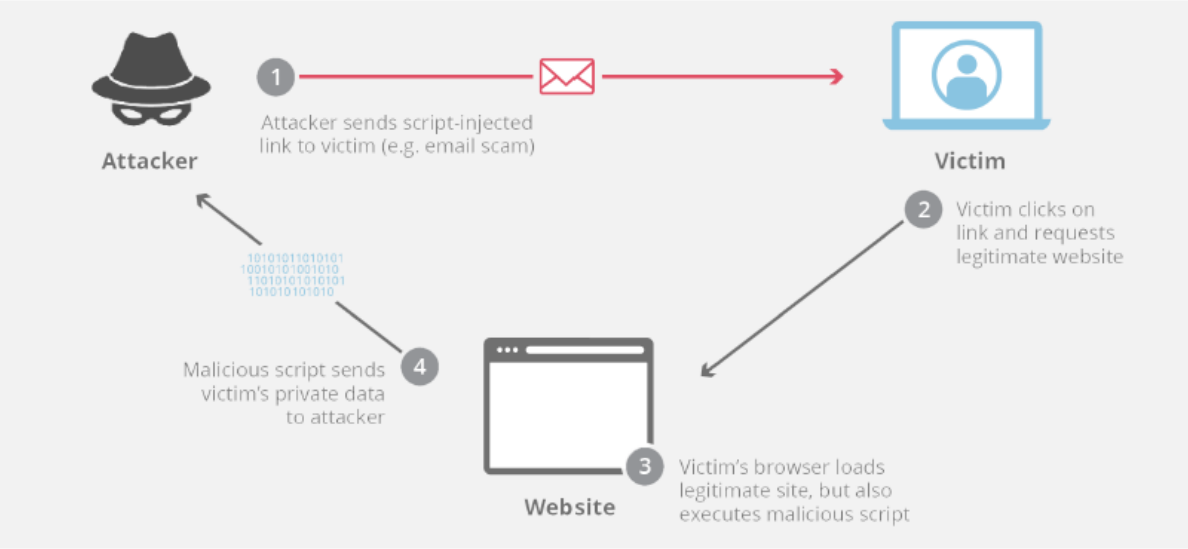
3. Cross-site scripting baseado em DOM - Document Object Model

Neste caso, fica associado direto ao DOM e não ao HTML. Em ataques de cross-site scripting refletidos e armazenados, você pode ver a carga útil da vulnerabilidade na página de resposta, mas no cross-site scripting baseado em DOM, o código-fonte HTML do ataque e a resposta serão os mesmos, ou seja, a

carga útil não pode ser encontrada na resposta. Ele só pode ser observado em tempo de execução ou investigando o DOM da página.

Geralmente o ataque é aplicado diretamente e exclusivamente no lado do cliente, não sendo enviada ao servidor.

O XSS é um ataque que explora vulnerabilidades em aplicações web, permitindo que um invasor injete código malicioso (geralmente JavaScript) no conteúdo das páginas visitadas por outros usuários. Existem três tipos principais de XSS: Refletido, Armazenado e DOM-based. O objetivo desse ataque é roubar informações confidenciais, como cookies de sessão, dados pessoais ou credenciais de acesso.

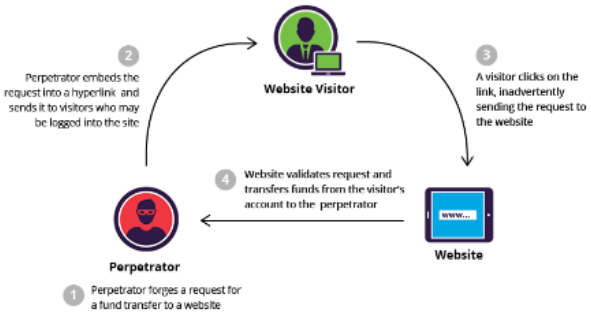


15.2 CSRF (Cross-Site Request Forgery) ou XSRF

O CSRF é um ataque que força a execução de ações não autorizadas em nome de um usuário autenticado, sem que ele saiba.

- O invasor cria um link ou uma página maliciosa que, quando acessado pelo usuário, faz com que o navegador envie uma requisição para a aplicação web alvo, realizando ações não autorizadas, como alterar senhas, fazer transferências bancárias, entre outras.

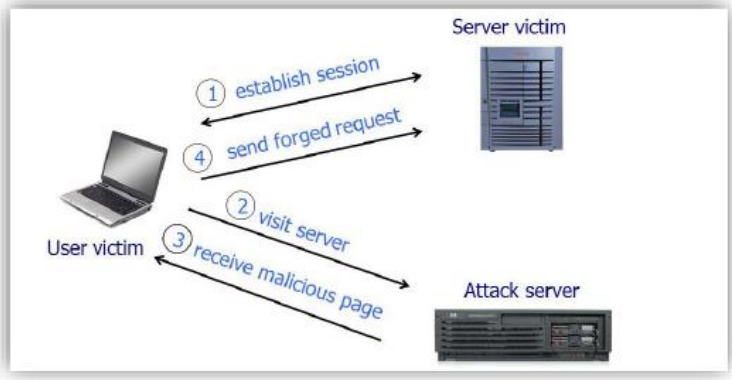
Medidas de proteção contra CSRF incluem o uso de tokens anti-CSRF e a verificação do cabeçalho 'Referer' ou 'Origin'.



Diferentemente do XSS, o CSRF não busca obter informações ou roubar dados, mas tão somente redirecionar ações legítimas do usuário, transformando-as, e aplicando no serviço em questão.

Assim, basicamente, em uma visão bancária, um aluno muito feliz com sua aprovação após a leitura do material do professor André Castro, resolve fazer a transferência de R$10.000,00 para o Professor André Castro. Entretanto, infelizmente (para mim e para a vítima), o aluno foi alvo do ataque CSRF e agora a transferência continua acontecendo na sessão autenticada do usuário, mas o atacante manipula a requisição e altera o destino da transferência, agora para a conta do atacante.

Então de uma maneira genérica, podemos dizer que o ataque força a vítima a realizar ações indesejadas em aplicações WEB nas quais está autenticada. Basicamente, a partir de engenharia social, como envio de links, a vítima, ao clicar no link, se torna vítima em todos os ambientes no qual está autenticado, passando a estar suscetível a qualquer manipulação das requisições.



Vejam que na etapa 1, há uma conexão legítima com um servidor correto. Já na etapa 2, em paralelo, o próprio usuário acessar um outro site/serviço malicioso. Na etapa 3, ele recebe o conteúdo malicioso, geralmente uma página, em que, ao acessar, passa a estar vulnerável. A partir daí, já na etapa 4, o atacante é capaz de forjar as requisições a partir da etapa 1, que foi o estabelecimento de uma conexão/sessão.

Então é nesse sentido onde um atacante consegue fazer as requisições forjadas a partir da sessão aberta e autenticada de um usuário.

- EXEMPLO CSRF: Um usuário realizou a autenticação na aplicação Web de um banco. Durante a utilização dessa aplicação, o usuário sofreu um ataque de engenharia social que o fez clicar em um link presente numa mensagem de e-mail com conteúdo HTML e cuja URL corresponde a uma requisição válida na aplicação Web do banco. Essa URL foi processada pelo navegador do usuário, e a requisição foi enviada e executada com sucesso em nome do usuário da aplicação Web.

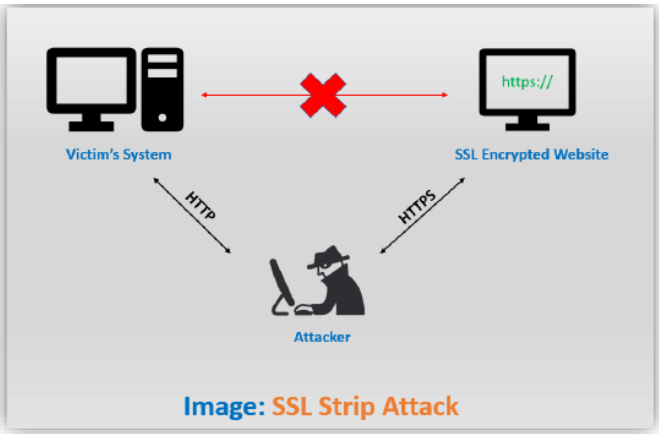


Image: SSL Strip Attack

Avançando um pouco mais na nossa discussão, sem dúvida a principal técnica atualmente utilizada reside na criação/utilização de tokens anti-csrf. Basicamente esse token busca garantir que o usuário autenticado é, de fato, quem deve realizar as requisições. A segurança reside na geração desse token para cada sessão aberta a partir do nó do usuário e somente é alterado no ato da renovação da sessão do próprio usuário.

Ainda, vou elencar algumas outras medidas de prevenção que são difundidas na WEB para que saibam das existências, pois, sabemos que, em muitas ocasiões, a banca simplesmente realizada a cópia desses textos.

- Exigindo um segredo, específico do token do usuário em todas os formulários de submissões e o efeito colateral das URLs impedem o CSRF; o site do invasor não pode colocar o token direto nas suas alegações;
- Exigir que o cliente forneça dados de autenticação na solicitação HTTP mesmo se utilizado para realizar qualquer operação com implicações de segurança (transferência de dinheiro, etc);
- Limitar o tempo de vida de cookies da sessão;
- Verificando o cabeçalho HTTP Referer;
- Assegurando que não há nenhum arquivo clientaccesspolicy.xml para a concessão de acesso não intencional aos controles Silverlight;
- Assegurando que não há nenhum arquivo crossdomain.xml concedendo acesso não intencional de vídeos em Flash;

O atacante, apesar de não conhecer a senha da vítima, consegue se utilizar das identidades dela para gerar o ataque. É como se o atacante pegasse um cheque em branco, devidamente assinado, mas não sabe falsificar a assinatura, ok?

15.3 Injeção SQL (SQL Injection):

- Esse tipo de ataque permite que determinado usuário malicioso manipule as entradas de banco de dados nos envios de requisições ou consultas à base de dados de alguma aplicação.
- Caso não haja o devido bloqueio de operações, pode-se, por exemplo, complementar um comando de consulta a uma tabela que visa retornar uma lista, com um “DROP TABLE”, podendo gerar perda de todos os dados ali armazenados.
- Ataque bastante conhecido e difundido, porém, com grande nível de sucesso atualmente. Esse tipo de ataque também explora uma vulnerabilidade da aplicação (página web, por exemplo).

15.4 Path Traversal (Directory Traversal):

- O Path Traversal é um ataque que explora vulnerabilidades em aplicações web para acessar arquivos e diretórios fora do escopo pretendido pelos desenvolvedores.
- Geralmente, o invasor manipula a entrada de dados (ex: URL ou parâmetros) para navegar pelos diretórios do sistema e obter acesso a informações confidenciais, como arquivos de configuração ou dados pessoais.

- Para mitigar esse tipo de ataque, é importante validar e filtrar as entradas dos usuários e usar funções de gerenciamento de arquivos seguras.

16. TÉCNICAS DE DESENVOLVIMENTO SEGURO:

O desenvolvimento seguro refere-se às práticas, processos e técnicas utilizadas para criar software livre de vulnerabilidades e seguro contra ataques. Algumas dessas técnicas incluem a revisão de código, treinamento em segurança para desenvolvedores, integração de segurança desde o início do ciclo de desenvolvimento, teste de segurança contínuo e uso de ferramentas de análise de código automático.

16.1 SAST (Static Application Security Testing):

- O SAST é uma abordagem de teste de segurança que analisa o código-fonte, bytecodes ou binários de uma aplicação em busca de vulnerabilidades, sem a necessidade de executar a aplicação.
- O SAST identifica problemas no código, como uso de funções inseguras, vazamento de informações e erros de lógica, antes que o software seja implantado.
- Essa técnica permite que desenvolvedores corrijam vulnerabilidades durante o processo de desenvolvimento, reduzindo os riscos de segurança.

16.2 DAST (Dynamic Application Security Testing):

- O DAST é uma abordagem de teste de segurança que analisa uma aplicação em execução, identificando vulnerabilidades ao interagir com a aplicação como um invasor faria.
- O DAST é usado para detectar problemas que só podem ser identificados durante a execução do aplicativo, como falhas de configuração, problemas de autenticação e autorização e vulnerabilidades relacionadas à entrada de dados.
- Essa técnica ajuda a identificar falhas que podem ser exploradas por atacantes em tempo real.

16.3 IAST (Interactive Application Security Testing):

- O IAST combina aspectos do SAST e DAST para fornecer uma análise de segurança mais abrangente.
- O IAST utiliza instrumentação do código e análise em tempo real para identificar vulnerabilidades durante a execução da aplicação.
- Ele é capaz de identificar problemas no código e no comportamento da aplicação, fornecendo informações detalhadas sobre o contexto e a localização das vulnerabilidades, facilitando a correção por parte dos desenvolvedores.

16.4 Controles OWASP (Open Web Application Security Project):

- OWASP é uma organização sem fins lucrativos que se dedica a melhorar a segurança das aplicações web.
- Eles publicam o "OWASP Top Ten", uma lista das dez vulnerabilidades de segurança mais críticas em aplicações web, juntamente com diretrizes e recursos para mitigá-las.
- Além disso, o OWASP fornece outras orientações de segurança, como o "OWASP Application Security Verification Standard (ASVS)" e o "OWASP Security Knowledge Framework (SKF)", que oferecem práticas recomendadas, controles e requisitos para garantir a segurança das aplicações durante todo o ciclo de desenvolvimento.
- O OWASP Top 10 é um documento de conscientização padrão para desenvolvedores e segurança de aplicativos da web. Ele representa um amplo consenso sobre os riscos de segurança mais críticos para aplicativos da web.
- Reconhecido globalmente pelos desenvolvedores como o primeiro passo para uma codificação mais segura.
- As empresas devem adotar este documento e iniciar o processo de garantir que suas aplicações web minimizem esses riscos. Usar o OWASP Top 10 talvez seja o primeiro passo mais eficaz para mudar a cultura de desenvolvimento de software em sua organização para uma que produza um código mais seguro.
- O OWASP Top 10 é baseado, essencialmente, em submissões de dados de empresas especializadas na área da segurança aplicacional e em inquéritos realizados a profissionais individuais do setor. Estes dados refletem as vulnerabilidades identificadas em centenas de organizações, aplicações e APIs reais. Os tópicos do Top 10 são selecionados e ordenados de acordo com a sua prevalência, combinada com uma estimativa ponderada do potencial de abuso, detecção e impacto.
- O principal objetivo do OWASP Top 10 é o de educar programadores, desenhadores e arquitetos de aplicações, bem como gestores e as próprias organizações sobre as consequências dos problemas de segurança mais comuns e mais importantes no contexto das aplicações web. O Top 10 oferece não só técnicas básicas para proteção nestas áreas problemáticas e de elevado risco, mas também direções sobre onde encontrar informação adicional sobre estes assuntos.

17. EQUIPAMENTOS DE REDE

17.1 Switches:

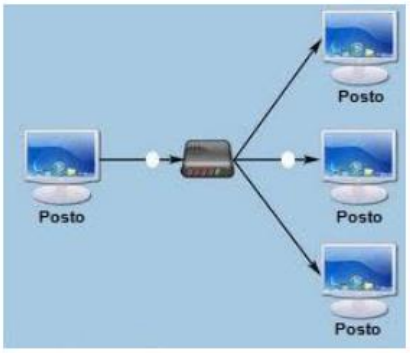
os switches também possuem a finalidade de interligar segmentos de rede. Porém, possui o recurso de isolar os domínios de colisão em cada uma de suas portas. Isto é, um switch de 24 portas possui 24 domínios de colisão. Entretanto, em sua camada 2 (enlace) nativa no modelo OSI, não realiza roteamento, apenas comutação dos quadros e, portanto, possui apenas um domínio de broadcast. Assumimos que não há implementação de VLANs, assuntos que veremos em outra aula.

O switch é capaz de gerar 3 tipos de tráfegos: UNICAST (1 origem para 1 destino), BROADCAST (1 origem para todos os destinos possíveis) e MULTICAST (1 origem para um grupo de destinos).

A sua capacidade de isolar domínio de colisão reside no fato do switch interpretar os endereços MAC de cada placa de rede conectada nos segmentos de rede e encaminhar os pacotes recebidos

para as portas específicas conforme o destino de cada quadro. Logo, se “A” encaminha um quadro para “B”, o switch sabe em qual porta se encontra o destinatário “B” e passa o quadro apenas para a respectiva porta.

A tabela em que o switch mantém essas informações é chamada de tabela CAM (Content Addressable Memory). Caso o endereço de destino seja desconhecido, o switch encaminha o quadro para todas as portas com vistas a mapear àquele dispositivo que responder a requisição.



Entretanto, ainda se pode ter um problema de incapacidade de encaminhamento dos quadros devido a diferentes velocidades das portas, causando uma sobrecarga do buffer de armazenamento do Switch. Quando isso acontece ele passa a funcionar como HUB para não descartar os quadros recebidos por falta de buffer. O recurso de buffer para as portas com larguras de bandas diferentes é chamado de comutação assimétrica.

Outro equipamento que vale mencionar é o BRIDGE. Este está para o switch assim como o repetidor está para o hub. Entretanto, possui algumas motivações a mais para o seu uso como separar o tráfego entre os dois segmentos de rede e compatibilizar diferentes padrões de rede que venham a ser empregados. Isto é, o tráfego só passará de um segmento para o outro se houver uma comunicação entre dispositivos de segmentos diferentes.

Atualmente já existem switches que exercem as funcionalidades de um roteador Switch L3, portanto trabalham também na camada 3 (camada de rede) do modelo TCP/IP. Este utiliza os endereços IP de destino para realizar o encaminhamento dos pacotes. Dessa forma, pode-se reduzir o número de equipamentos em uma rede, eliminando o roteador que possui uma quantidade menor de portas como mencionado a frente e fazendo com que o switch L3 exerça as funções de roteamento.

Devido a utilização de circuitos integrados conhecidos como ASICs, o processamento dos pacotes e o roteamento é efetuado a nível de hardware, diferentemente dos roteadores que atuam em nível de software. Por esse motivo, o desempenho dos Swichtes L3 é superior ao dos roteadores, além de possuir uma praticidade e facilidade maior na configuração das regras de encaminhamento.

Entretanto, esses equipamentos não são aplicados em rede WAN.

Um outro ponto a se considerar, é que já existem Swiches que atuam em todas as camadas do modelo OSI, isto é, até a sétima camada que é a de aplicação. Estudaremos esse modelo mais adiante.

17.2 Roteadores:

Estes são dispositivos de redes tradicionais e nativos da camada 3 (camada de rede) do modelo OSI. Assim como os switches utilizavam os endereços MAC para definir as portas para enviar os quadros, o roteador também se utiliza de endereços, mas aqui se fala de endereçamento IP. Falaremos das características do IP mais tarde. Por agora, ficaremos com a informação de que cada dispositivo de rede possui um endereço lógico.

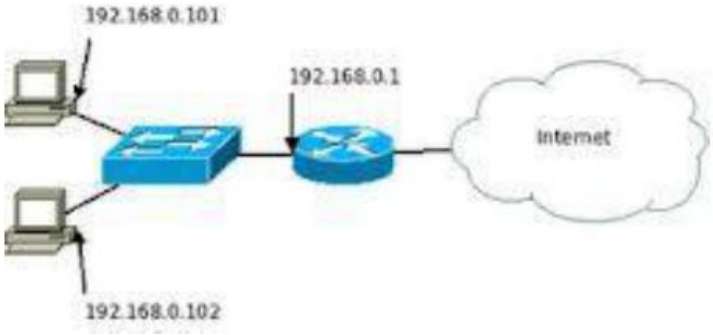
Os roteadores possuem uma quantidade reduzida de portas quando comparados com os switches. A título de parâmetro, geralmente estes possuem 24 a 48 portas, já aqueles possuem de 2, 4 ou 8 portas.

Dessa forma, o roteador é capaz de montar uma tabela com as informações dos IP's e das redes como um todo, sabendo assim qual porta deve usar para encaminhar o pacote e um pouco mais, é capaz de determinar o melhor caminho para se alcançar o destino final baseado nas suas regras e políticas de roteamento, bem como das informações trocadas com outros roteadores.

Essas informações são trocadas a partir de algoritmos de roteamento, objeto de estudo nas próximas aulas. Apenas para introduzir, menciono alguns exemplos de protocolos de roteamento que vocês já devem ter ouvido falar: RIPv1, RIPv2, OSPF, EIGRP, BGP, IS-IS.
O roteador segmenta totalmente as redes, gerando assim domínios de broadcast diferentes, bem como domínios de colisão isolados. Por esse motivo, aumenta o desempenho dos segmentos a ele conectados e diminui a quantidade de colisões. Esse assunto simplesmente despenca em provas!!!

Outro recurso interessante do roteador é a sua capacidade de interconectar enlaces com tecnologias diferentes de camada 2 do modelo OSI. Isto é, em uma porta podemos ter a tecnologia Ethernet de acesso à rede e na outra porta a tecnologia Token-Ring. Veremos estas tecnologias posteriormente.

A imagem abaixo representa um cenário de conexão de dois computadores, um switch e um roteador, da esquerda para a direita.



Importante destacar também que algumas bancas têm cobrado a composição física do roteador. Assim, destaca-se que este é composto por:
I. Portas de Entrada;
II. Portas de Saída;
III. Matriz de Comutação;
IV. Processador de Roteamento;

18. MODELO DE REFERÊNCIA ISO/OSI

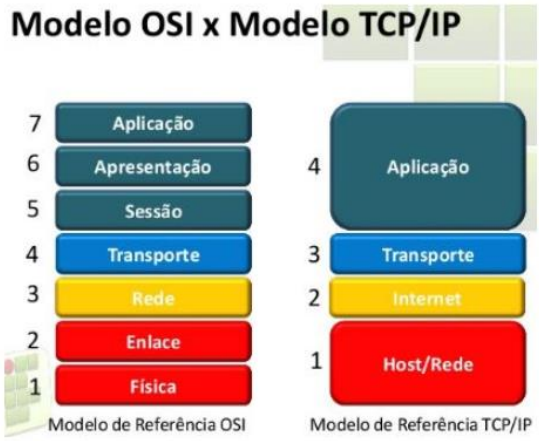
O modelo OSI foi criado sob três conceitos principais bem definidos:

- Serviços – Cada camada presta serviços à camada superior, fornecendo determinados recursos. Nesse sentido, define-se quais serviços serão prestados.

- Interfaces – Determina a forma de interação entre as camadas, ou seja, como a camada superior pode acessar a camada inferior para utilizar os

serviços. São definidos parâmetros a serem fornecidos bem como os resultados esperados conforme recursos ofertados.

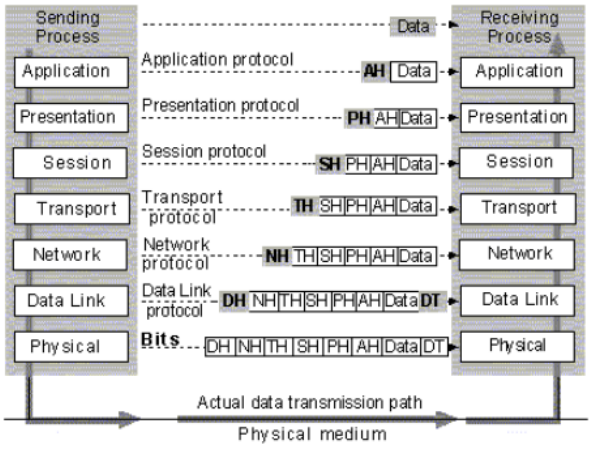
- Protocolos – É a implementação dos serviços propriamente dito. Os protocolos podem implementar totalmente ou parcialmente determinados serviços.



Podemos dizer que as 4 camadas superiores são consideradas camadas de host e as 3 camadas inferiores são consideradas camadas do meio de transmissão. Em regra, a camada superior utilizará os recursos providos pela camada inferior, ou seja, a camada de REDE vai utilizar os recursos providos pela cada de ENLACE.

As camadas inferiores utilizam as técnicas de encapsulamento de forma a abstrair a informação das camadas superiores. Assim, cada camada no momento de sua atuação, agrega ao bloco de dados inicial um cabeçalho com informações relativas à própria camada. Esse é um ponto chave do modelo!!!

PDU (protocol data unit – unidade de dados do protocolo): conjunto dado pela parcela de dados da camada superior acrescido do cabeçalho da respectiva camada.



a camada inferior sempre encapsulará os dados da camada superior.

18.1 CAMADA FÍSICA

Recursos de controle de fluxo, início e término da comunicação a nível de bit. Definirá ainda a forma em que esses bits utilizarão o meio, a saber:

● Simplex – Define uma via unidirecional entre origem e destino. É utilizado em sistemas de fornecimento de informação sem a necessidade de retorno, como as transmissões de rádio e TV.

● Half duplex – Neste caso, o fluxo de bits acontece nos dois sentidos, porém, não de forma simultânea. Imagine uma ponte sobre um rio que permite a passagem de uma pessoa por vez. Nesse caso, ela pode ir e voltar, porém em momentos distintos.

Atualmente, os serviços da Nextel funcionam dessa forma, semelhante a um "walkie Talkie", ou seja, enquanto um ponto está falando, o outro está apenas escutando, podendo inverter o sentido, porém um por vez.

O padrão Ethernet de 10Mbps funciona no sistema Half Duplex.

● Full duplex – Neste caso, o fluxo de bits funciona nos dois sentidos de forma simultânea. Entretanto, é importante mencionar que se necessita usar 2 canais diferentes, ou seja, 2 canais operando em modo simplex para cada sentido.

- As evoluções do padrão Ethernet, como o FastEthernet e o GigabitEthernet utilizam essa forma de alocação do canal.

- Na comunicação bidirecional (full duplex), sempre que um quadro é recebido, o receptor espera e não envia o quadro de controle (confirmação ou ACK) de volta ao remetente imediatamente. O receptor aguarda até que sua camada de rede passe no próximo pacote de dados. A confirmação atrasada é então anexada a esse quadro de dados de saída. Essa técnica de atrasar temporariamente a confirmação para que ela possa ser vinculada ao próximo quadro de dados de saída é conhecida como PIGGYBACKING.

- Hubs: esse dispositivo opera na camada física do modelo OSI, que é a camada 1.

- Ao tentar diagnosticar a causa do desempenho ruim de um equipamento da rede, o analista de suporte acaba descobrindo que um dos conectores de um cabo categoria 5 estava com mau contato, o que ocasionava um problema intermitente. ERRO NA CAMADA FÍSICA.

18.2 CAMADA DE ENLACE

É responsável por prover um meio confiável entre os dispositivos.

Para isso, utiliza técnicas de detecção e correção de erros que podem ocorrer no meio físico.

- A IEEE manteve a camada física similar ao modelo de referência OSI e, para facilitar na substituição de redes locais (rede ethernet que é a mais comum entre redes locais cabeadas, o WiFi, etc), dividiu a camada de enlace em 2:

- Logical Link Control (LLC) – IEEE 802.2: subcamada superior do enlace. Seus serviços são: serviço de datagrama não-confiável, serviço de datagrama com confirmação, serviço confiável orientado a conexões, multiplexação e controle de fluxo. Todos os serviços são genéricos para que diferentes protocolos da subcamada MAC não afetem a LLC.
- Medium Access Control (MAC): é a subcamada inferior da rede. Seu objetivo é definir o acesso à rede mesmo que as características sejam diferentes entre os diversos protocolos. Ela também é responsável pelo endereçamento físico, o MAC.

- Switch Ethernet: switches de conexão ethernet operam na camada de enlace do modelo OSI, que é a camada 2.

Quatro técnicas que pode sem utilizadas, quais sejam:

1. Contagem de Caracteres – Por ser extremamente sensível a erros, não é mais utilizado hoje em dia.

2. Bytes de flags, com inserção de bytes – Sensíveis a uma sequência de dados repetidos que surgem de padrões acidentalmente. Assim, o método se perde e gera flags que não deveriam existir.

3. Flags iniciais e finais, com inserção de bits – Menos sensível ao problema da repetição devido à inserção de "stuffed bits". É o método utilizado pelo padrão Ethernet.

4. Violações de codificação da camada física – Método aplicável somente a redes nas quais a decodificação no meio físico contém algum tipo de redundância.

18.3 CAMADA DE REDE

A PDU da camada de rede, que é o pacote, também pode ser chamada de DATAGRAMA. Possui como característica a capacidade de encaminhar os datagramas entre dois dispositivos que se encontrem em redes distintas, diferentemente da camada de enlace que interliga pontos em uma mesma rede.

- Roteador: esse equipamento opera na camada de rede do modelo OSI, que é a camada 3.

Ela é capaz de aplicar diversas técnicas de roteamento e encaminhamento de pacotes, podendo ou não garantir um nível mínimo de qualidade de serviço.

- O ICMP e o IP são ambos protocolos da camada inter-redes (ou camada de rede, no modelo OSI/ISO). O ICMP é usado para enviar mensagens de erro e operacionais referentes a serviços de IP.

Possui ainda como característica a capacidade de fragmentar pacotes e remontá-los entre os nós de forma a adequá-los às capacidades do enlace, o qual chamamos de MTU (Max Transfer Unit). Essa unidade define a quantidade de bytes o enlace suporta desconsiderando o cabeçalho da camada de enlace apenas.

Possui a capacidade de trocar mensagens de controle entre os nós. São os roteadores que atuam nessa camada que permitem a interligação entre as diversas redes através da utilização de endereços lógicos, premissa para que os roteadores sejam capazes de identificar os pontos na rede e realizar o roteamento.

18.4 CAMADA DE TRANSPORTE

A camada responsável pela comunicação fim a fim (ou comunicação final) entre processos/serviços de diferentes sistemas é a de TRANSPORTE - que oferece tanto serviços orientados à conexão (confiáveis), os quais garantem a entrega das informações, como serviços não orientados à conexão (não confiáveis).

Há dois principais protocolos da camada TRANSPORTE, tanto no Modelo OSI/ISO, quanto no Modelo TCP/IP (pilha de protocolos):

- TCP (do inglês "Transmission Control Protocol"), o qual implementa mecanismos de controle de fluxo e de erros, bem como retransmissão de dados. Trata-se, pois, de um protocolo orientado à conexão (confiável) - o qual realiza, inclusive, o controle dos estados dessa conexão. O início da transmissão de dados se dá, comumente, por uma técnica denominada "Handshake de Três Vias", com o emprego de flags (SYN, ACK e FYN).
    - O processo inicia (primeiro passo) com o cliente solicitando uma conexão ao servidor ao enviar um segmento SYN, o servidor então responde (segundo passo) ao cliente com um segmento SYN-ACK, e finalmente o cliente confirma a conexão (terceiro passo) com um segmento ACK, estabelecendo a conexão.
    - O *Transmission Control Protocol* (TCP), ou protocolo de controle de transmissão, localiza-se na camada de transmissão do modelo OSI e, por ser um protocolo orientado a conexão, provê uma conexão segura para a troca de dados entre hosts diferentes. Com esse protocolo, todos os pacotes são sequenciados e identificados e, um circuito virtual é estabelecido para comunicações
    - técnicas para controle de fluxo e controle de erro conhecidas como janela deslizante e reconhecimento
- UDP (do ingles "User Datagram Protocol"), o qual não implementa controle de fluxo e nem de erros (salvo o uso opcional de checksum). Assim, considera-se um protocolo não orientado à conexão (e não confiável). Havendo erros de transmissão, comumente dá-se continuidade ao processo de envio, sem possibilitar a recuperação e retransmissão de dados perdidos.
    - O protocolo UDP fornece um serviço de pacotes sem conexão que oferece entrega com base no melhor esforço, ou seja, UDP não garante a entrega ou verifica o sequenciamento para qualquer pacote. Um host de origem que precise de comunicação confiável deve usar TCP ou um programa que ofereça seus próprios serviços de sequenciamento e confirmação. As mensagens UDP são encapsuladas e enviadas em datagramas IP.

Possui como PDU o segmento. Estes são definidos através da segmentação dos dados recebidos da camada de sessão, ou seja, dos respectivos processos abertos em um terminal. Nesse contexto, tem-se o conceito de multiplexação de demultiplexação dos processos em relação às portas utilizadas para comunicação. Mais detalhes de portas serão vistos quando abordamos especificamente os principais protocolos dessa camada.

Essa camada permite recursos de controle de fluxos, ordenação de pacotes, detecção e correção de erros e detecção de perda de pacotes. Para tanto, ela utiliza características que são orientadas à conexão, como o protocolo TCP que veremos nas próximas aulas.

Entretanto, em determinadas ocasiões, e que não são poucas, os serviços pretendem apenas que a informação seja entregue o mais rápido possível e por esse motivo podem optar por funcionalidade que não sejam orientadas à conexão, como o protocolo UDP, que também veremos nas próximas aulas. Nesses casos não há controle de erro de conteúdo e serviço de confirmação de recebimento por parte do destinatário.

Assim como a camada de rede trabalha com o parâmetro MTU, conforme vimos anteriormente, a camada de transporte possui uma unidade semelhante, chamada de MSS (Max Segment Size). Esse parâmetro define o tamanho máximo do segmento conforme informações obtidas do MTU da camada inferior.

A principal função do MSS é evitar a fragmentação dos pacotes por parte da camada de rede de forma que os segmentos já estejam devidamente ajustados às capacidades dos enlaces, otimizando assim a comunicação e envio dos pacotes pela rede. Nesse caso, não há necessidade de consumo de recursos nos roteadores intermediários para fragmentação e remontagem dos pacotes.

18.5 CAMADA DE SESSÃO

A camada de sessão possui como PDU os dados. Provê recursos para o estabelecimento e suporte das sessões dos serviços requisitados pelas camadas superiores. Diz-se que essa camada gerencia a comunicação entre as aplicações nos dispositivos após o estabelecimento da sessão.

Além disso, segundo Tanenbaum:

"Uma sessão oferece diversos serviços, inclusive o controle de diálogo (mantendo o controle de quem deve transmitir em cada momento), o gerenciamento de símbolos ou tokens (impedindo que duas partes tentem executar a mesma operação crítica ao mesmo tempo) e a sincronização (realizando a verificação periódica de transmissões longas para permitir que elas continuem a partir do ponto em que estavam ao ocorrer uma falha)."

18.6 CAMADA DE APRESENTAÇÃO

A camada de apresentação também possui como PDU os dados. É responsável pela formatação dos dados recebidos da camada de aplicação em um formato comum e compreensível pelos protocolos utilizados por ambos, origem e destino.

Possui recursos de compressão e criptografia. O primeiro garante uma maior eficiência na transmissão dos dados enquanto o segundo garante uma maior segurança dos dados.

- A camada de Apresentação no modelo OSI/ISO é responsável pela representação dos dados, incluindo a conversão de códigos de caracteres, a codificação e decodificação de dados e a compressão e descompressão de dados. Portanto, se o software precisa lidar com a codificação e decodificação das estruturas de dados entre dois sistemas com representações internas diferentes, essa é a camada que ele precisa tratar.

18.7 CAMADA DE APLICAÇÃO

Possui como PDU os dados. Esta camada é a que atua de forma mais próxima do usuário, permitindo a comunicação dos processos de aplicações e usuários com os serviços de rede. Todos os recursos dessa camada atuam no âmbito de software.

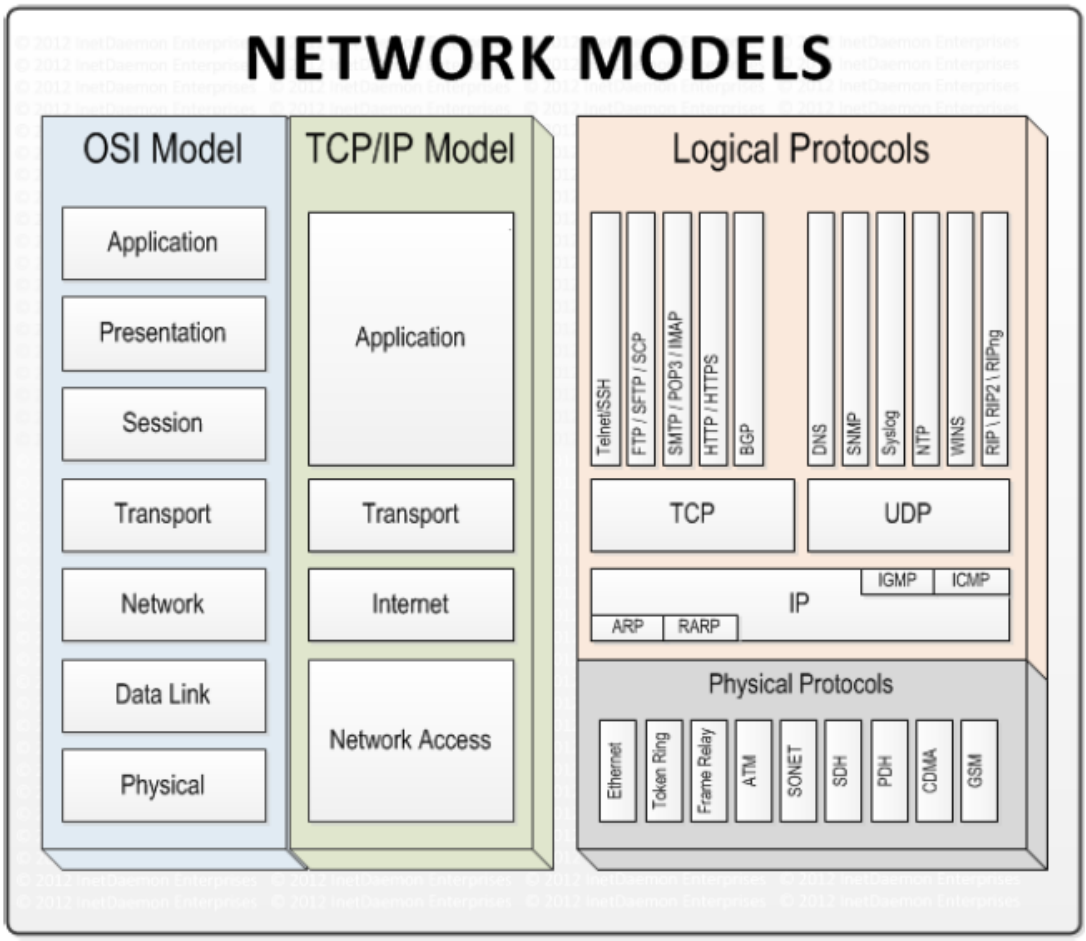
Possui diversas funcionalidades que são definidos pelos seus diversos protocolos como: Acesso remoto, terminais virtuais, mensagens eletrônicas (e-mail), serviços de diretório, compartilhamento de recursos, entre outros. Veremos estes serviços nas próximas aulas com mais detalhes.

- Servidor de correio eletrônico: um servidor de correio eletrônico utiliza os protocolos SMTP e POP3/IMAP e opera na camada de aplicação do modelo OSI, que é a camada 7.

- Servidor de páginas www: assim como o servidor de correio eletrônico, esse servidor opera na camada de aplicação, que é a camada 7

19. ARQUITETURA TCP/IP

Camada 4 – Camada de Aplicação
Camada 3 – Camada de Transporte
Camada 2 – Camada de Internet, Inter-Redes ou Rede.
Camada 1 – Camada de Acesso à Rede, Interface de Rede ou host/rede



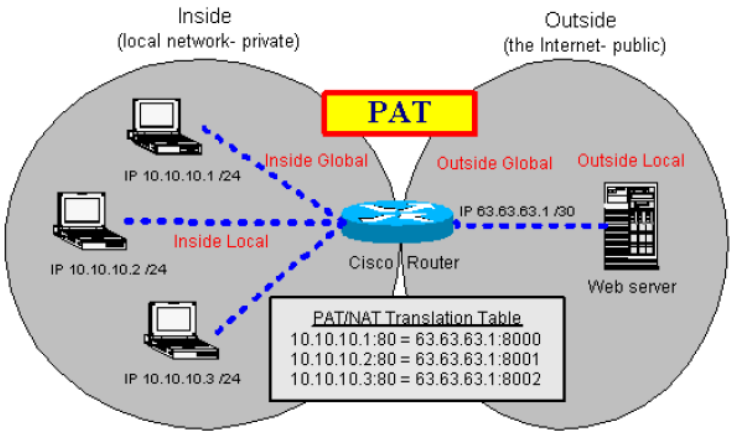
20. NAT e PAT:

20.1 NAT (Network Address Translation)

- Converter um endereço em outro endereço
- Na maioria dos casos, o seu funcionamento permite o fornecimento para determinadas empresas de apenas um endereço público (ou alguns), ainda que este possua centenas ou milhares de dispositivos em sua rede interna.
- O Network Address Translation (NAT) é uma técnica amplamente adotada para gerenciar e economizar endereços IP públicos em redes de computadores.
- Essencialmente, o NAT permite que dispositivos pertencentes a uma rede privada se comuniquem com a Internet utilizando um único endereço IP público, facilitando a interação entre as redes privadas e a Internet.
- Comumente implementado em roteadores e firewalls.
    - NAT estático: estabelece uma correspondência um-para-um entre endereços IP privados e públicos;
    - NAT dinâmico: múltiplos endereços IP privados são mapeados para um único endereço IP público;

20.2 PAT (Port Address Translation)

- O Port Address Translation (PAT) é um subconjunto específico do NAT, que, além de traduzir endereços IP, também traduz os números de porta dos dispositivos envolvidos na comunicação.
- Essa abordagem permite que várias conexões originárias de diferentes dispositivos sejam associadas a um único endereço IP público, aumentando ainda mais a eficiência no uso de endereços IP.
- Ademais, o PAT sempre emprega uma relação muitos-para-um, otimizando a alocação de recursos e garantindo a comunicação eficiente entre as redes privadas e a Internet.
- Assim como o NAT, o PAT pode ser implementado em dispositivos como roteadores e firewalls.



21. PROTOCOLO IPV6

- Solução definitiva para a escassez de endereços IPv4, e não mais paliativa como o NAT.
- O protocolo IPV6 utiliza endereços de 128 bits. Isso permite uma versatilidade de endereçamento muito grande, sendo possível aplicar o princípio surgido pelo IPV4 de endereçar de forma pública e visível na Internet todo e qualquer dispositivo na rede.
- Esses endereços são escritos na forma hexadecimal, diferentemente do IPv4, que utilizava o formato decimal.

2001:0DB8:00AD:000F:3456:AF42:CDCC:0001

- O protocolo IPv6 possui implementações de segurança de forma nativa através do suporte ao protocolo IPSec, sendo este obrigatório. No IPv4, este procedimento de segurança é opcional e utilizou os conceitos e técnicas criadas para o IPv6.
- Percebam que não há mais o campo de tamanho do pacote, que antes limitava o tamanho dos pacotes IPv4 a 65536 bytes ou também dito de 64 kb. O IPv6 suporta os conhecidos jumbograms, que são aqueles maiores que 64 kb.

21.1 TIPOS DE TRANSMISSÃO IPV6

- UNICAST
  - Neste tipo de transmissão o emissor envia os dados contendo informações o mesmo número de vezes que clientes necessários, ou seja, os dados são enviados várias vezes tendo o número de transmissões igual ao número de destinatários. Sua vantagem é que as informações chegam apenas aos destinatários, porém tem a desvantagem de que a largura de banda da rede é desperdiçada, pois as mesmas informações são enviadas várias vezes pelo mesmo link.

- ANYCAST
  - O IPv6 define um importante tipo de endereço, chamado de anycast. De forma geral, um endereço de anycast define um grupo de nós, como faz o modo multicast. Entretanto, de forma diferente do modelo multicast, um pacote destinado a um endereço através de anycast é entregue apenas a um dos membros do grupo anycast, sempre o mais próximo (aquele que possui a rota mais curta). Um uso possível do modelo é alocar um endereço anycast a todos os roteadores de um ISP que cobrem uma grande área lógica na Internet. Os roteadores fora do ISP entregam um pacote destinado ao ISP para o roteador do ISP mais próximo. Nenhum bloco é atribuído a endereços anycast.

- MULTICAST:
  - Outro método de transmissão de dados, porém considerado mais eficiente que os demais. Assim como o broadcast, a transmissão das informações é feita para múltiplos destinos ao mesmo tempo, entretanto os destinatários são organizados em grupos de transmissão. Sua principal importância é que os dados são enviados apenas uma única vez e apenas ao conjunto de destinatários interessados na transmissão, não havendo tráfego desnecessário de informações.

- BROADCAST
  - Sua tradução literal significa transmissão, e seu uso na internet ou em telecomunicação significa o método de transmissão ou difusão de informações a partir de qualquer tipo de mídia para vários receptores ao mesmo tempo. Sua principal vantagem é que os dados são enviados apenas uma vez pela rede, não havendo duplicação como ocorre com Unicast, entretanto as informações são levadas a todos os dispositivos da rede, sendo eles destinatários ou não, provocando sobrecarga de informações em todos os hosts da rede.

IPv4	IPv6
Endereço de 32 bits	**Endereço de 128 bits**
IPSec opcional	**IPSec obrigatório**
Implementação restrita de QoS	**Utiliza o campo Flow Label para QoS**
Fragmentação nos roteadores	**Fragmentação somente na origem**
Possui campo opcional no cabeçalho	**Requisitos opcionais são implementados em cabeçalhos de extensão**
ARP utiliza Broadcast	**Utiliza mensagens Neighbor Discovery**
IGMP utilizado em grupos em redes locais	**Utiliza agora o Multicast Listener Discovery**
Utiliza conceito de Broadcast	**Não existe mais Broadcast, sendo agora o Multicast. Acrescentou o conceito de anycast.**
Endereço configurado manualmente ou via servidor externo	**Suporte à autoconfiguração e descoberta automática**

22. ARP E RARP

- Quando um pacote tem como destino redes distintas, utiliza-se o endereço IP para se chegar até a rede local de destino à qual a estação de destino pertence.

- Uma vez que esse pacote esteja nessa rede, ou seja, o roteador de borda (gateway da rede) recebeu esse pacote, a partir de então, o encaminhamento se dará a nível da camada de enlace, ou seja, baseado no endereço MAC, pois os switches da rede local não operam na camada de rede para interpretar endereços IP.

- É nessa hora que temos a atuação e importância do protocolo ARP (Address Resolution Protocol). Este protocolo é responsável por mapear e converter os endereços IP em endereços MAC, ou seja, passar do nível da camada de rede para a camada de enlace.

- Atenção para o detalhe de que a atuação do protocolo ARP é a nível de uma MESMA REDE!!!

- Os endereços físicos aprendidos pelos dispositivos são armazenados em uma tabela, conhecida como tabela ARP. Dessa forma, caso o dispositivo já possua determinado endereço IP mapeado nessa tabela, não há necessidade de se realizar uma nova consulta e descoberta. Diz-se então que o armazenamento é feito via cache no dispositivo.

- O protocolo RARP realiza a função inversa do protocolo ARP, ou seja, sabe-se o endereço MAC e necessita-se descobrir o endereço IP.

23. SEGURANÇA EM LAN'S SEM FIO

As redes sem fio têm se tornado cada vez mais populares devido à sua conveniência e flexibilidade, permitindo a conexão de dispositivos à Internet sem a necessidade de cabos físicos. Vamos explorar os conceitos básicos de funcionamento, segurança, tecnologias e protocolos de redes sem fio, incluindo padrões e protocolos da família 802.1x, EAP, WEP, WPA e WPA2.

Funcionamento e tecnologias:

Redes sem fio operam com base em protocolos e padrões que determinam a forma como os dispositivos se comunicam entre si e acessam a Internet. A família de padrões IEEE 802.11 é a mais comum para redes sem fio locais (WLANs), incluindo 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac e 802.11ax. Esses padrões definem a taxa de transferência de dados, alcance e frequências de operação (2,4 GHz ou 5 GHz) para dispositivos compatíveis.

Segurança e protocolos:

A segurança é uma preocupação fundamental em redes sem fio, uma vez que a transmissão de dados ocorre pelo ar, podendo ser interceptada por invasores. Vários protocolos e padrões foram desenvolvidos para garantir a segurança das redes sem fio:

- Família 802.1x: Refere-se a um conjunto de padrões IEEE que fornecem autenticação e controle de acesso em redes. O 802.1X atua como um framework para autenticação de dispositivos e usuários antes de conceder acesso à rede.

- EAP (Extensible Authentication Protocol): É um protocolo de autenticação usado em redes sem fio e sistemas de comunicação por cabos. O EAP fornece um mecanismo para autenticar usuários e dispositivos, suportando vários métodos de autenticação, como senhas, certificados e tokens.

- WEP (Wired Equivalent Privacy): É um protocolo de segurança antigo e vulnerável que foi projetado para fornecer um nível básico de privacidade em redes sem fio. O WEP utiliza

criptografia RC4 e autenticação de chave compartilhada, mas apresenta várias falhas de segurança que facilitam sua quebra por invasores.

- WPA (Wi-Fi Protected Access): Foi introduzido como uma solução mais segura em relação ao WEP. O WPA utiliza o protocolo Temporal Key Integrity Protocol (TKIP) para criptografia e oferece suporte ao EAP para autenticação. No entanto, o WPA ainda apresenta algumas vulnerabilidades.

- WPA2 (Wi-Fi Protected Access 2): É a evolução do WPA e é considerado o padrão atual para segurança em redes sem fio. O WPA2 utiliza criptografia AES-CCMP, que é mais robusta que o TKIP, e oferece suporte a métodos avançados de autenticação, como o EAP-TLS. O WPA2 possui duas variantes: WPA2-Personal, para uso doméstico e de pequenas empresas, e WPA2-Enterprise, para ambientes corporativos que exigem maior segurança.

Ao compreender e aplicar corretamente esses conceitos, protocolos e tecnologias de segurança, é possível criar e gerenciar redes sem fio seguras e eficientes. Entretanto, é importante destacar que, mesmo com a implementação dos padrões e protocolos mencionados, a segurança em redes sem fio continua sendo um desafio. Para garantir uma rede sem fio segura, é fundamental combinar práticas de segurança sólidas, como o uso de senhas fortes, atualizações regulares de firmware, segmentação de rede e monitoramento constante das atividades na rede.

Além disso, a indústria continua evoluindo, e novos padrões e protocolos estão sendo desenvolvidos para melhorar a segurança e o desempenho das redes sem fio. Um exemplo é o WPA3, que está sendo implementado como a próxima geração de segurança Wi-Fi, oferecendo melhorias na criptografia e na autenticação, além de outras funcionalidades avançadas de segurança.

Em resumo, é essencial compreender os conceitos básicos de funcionamento, segurança, tecnologias e protocolos de redes sem fio, como a família 802.1x, EAP, WEP, WPA e WPA2, para garantir a criação e manutenção de redes sem fio seguras e eficazes. Além disso, é crucial manter-se atualizado sobre os desenvolvimentos e avanços da indústria para enfrentar os desafios contínuos da segurança em redes sem fio.

24. CRIPTOGRAFIA

A criptografia é um conjunto de técnicas que visa garantir a confidencialidade, integridade e autenticidade das informações por meio da transformação de dados legíveis (texto claro) em dados cifrados (texto cifrado).

A criptografia pode ser dividida em dois tipos principais: criptografia simétrica e criptografia assimétrica. Ambas possuem diferenças, pontos fortes e fracos, bem como casos de utilização específicos.

24.1 CRIPTOGRAFIA SIMÉTRICA

A criptografia simétrica possui como princípio o fato de se utilizar a mesma chave para o procedimento de criptografia e descriptografia. Isso implica que as partes envolvidas na comunicação devem compartilhar a chave secreta de forma segura antes de trocar informações criptografadas.

Desse modo, a ideia é pegar um texto em claro que se deseja enviar a um destinatário e aplicar um algoritmo de criptografia simétrica sobre ele. Esse algoritmo depende da inserção de uma chave que será utilizada nos cálculos matemáticos para gerar uma mensagem que não seja interpretada facilmente.

No destinatário, deve-se aplicar o algoritmo com vistas a descriptografar a mensagem, ou seja, a partir da mensagem criptografada, busca-se obter a mensagem original. Esse processo depende da inserção da MESMA CHAVE utilizada no processo de criptografia. A imagem a seguir nos apresenta o modelo:

Percebam que para o perfeito funcionamento do algoritmo, tanto o emissor quanto o receptor necessitam conhecer a chave simétrica utilizada e isso gera um problema na utilização do algoritmo. Como trocar as informações da chave de um modo seguro?

A criptografia simétrica visa garantir apenas o princípio da confidencialidade. Os demais não podem ser garantidos, pois não há mecanismo que garanta que a mensagem não será alterada no caminho, podendo gerar um resultado de decriptação diferente da mensagem original. Não há como garantir de que a pessoa que aplicou a chave simétrica no processo de encriptação é quem ela diz ser. Veremos com detalhes cada um dos principais algoritmos de criptografia simétrica.

- Pontos fortes: A criptografia simétrica geralmente é mais rápida e eficiente em termos computacionais em comparação à criptografia assimétrica. Algoritmos populares de criptografia simétrica incluem o AES (Advanced Encryption Standard), DES (Data Encryption Standard) e o RC4.

- Pontos fracos: O principal desafio da criptografia simétrica é a necessidade de compartilhar a chave secreta entre as partes de forma segura. Se a chave for interceptada por um invasor, a segurança da comunicação será comprometida. Além disso, a quantidade de chaves necessárias cresce exponencialmente com o aumento do número de participantes na rede.

- Utilização: A criptografia simétrica é frequentemente usada em situações onde a velocidade e a eficiência são prioridades, como na criptografia de dados em repouso (armazenados em dispositivos) e em comunicações internas dentro de uma organização.

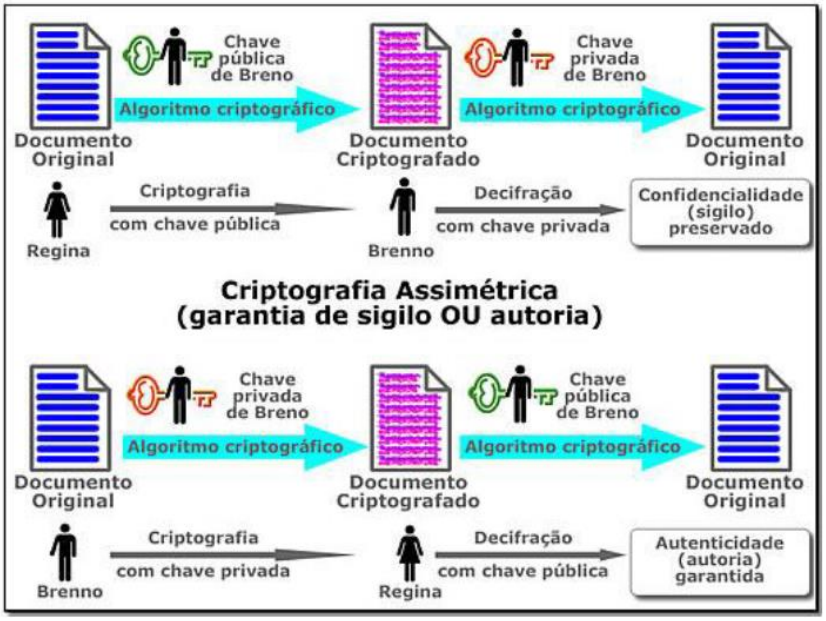
A criptografia Simétrica está fundamentada na técnica de SUBSTITUIÇÃO:

- A substituição é um método de codificação que busca alterar um caractere, símbolo ou dado em algum outro. É o método mais simples e fácil de executar. Porém, tende a ser o mais fácil de ser quebrado.

    - O principal exemplo desse método é a CIFRA DE CÉSAR, utilizado ainda no período do Império Romano. A sua rotina era definida de tal modo que cada letra da mensagem original era substituída pelo correspondente a três letras depois no alfabeto.

24.2 Criptografia Assimétrica:

Na criptografia assimétrica, também conhecida como criptografia de chave pública, são utilizadas duas chaves distintas: uma chave pública, que pode ser compartilhada livremente, e uma chave privada, que deve ser mantida em sigilo pelo proprietário. A chave pública é usada para cifrar os dados, enquanto a chave privada é usada para decifrá-los.



- Pontos fortes: A criptografia assimétrica elimina a necessidade de compartilhar uma chave secreta, já que a chave pública pode ser distribuída sem comprometer a segurança das informações. Além disso, a criptografia assimétrica permite a implementação de sistemas de assinatura digital para garantir a autenticidade e a integridade das informações. Algoritmos populares de criptografia assimétrica incluem o RSA, o DSA e o ECC (Elliptic Curve Cryptography).

- Pontos fracos: A criptografia assimétrica é geralmente mais lenta e computacionalmente mais exigente do que a criptografia simétrica. Além disso, a segurança da criptografia assimétrica depende do tamanho das chaves e da robustez dos algoritmos utilizados.

- Utilização: A criptografia assimétrica é amplamente utilizada em situações em que a segurança e a autenticidade são prioridades, como na troca segura de chaves em protocolos de comunicação (por exemplo, SSL/TLS), na assinatura digital de documentos e na autenticação de usuários e dispositivos. Um exemplo comum de utilização da criptografia assimétrica é o protocolo de e-mail seguro PGP (Pretty Good Privacy).

A criptografia Assimétrica está fundamentada na técnica de TRANSPOSIÇÃO:

- A transposição foca no simples embaralhamento das letras segundo alguma rotina. Veremos mais à frente que os algoritmos de criptografia geralmente utilizam esse recurso dividindo a mensagem original em blocos de tamanhos iguais. Um exemplo simples seria transpor cada sílaba de cada palavra (bloco) para esquerda, mantendo a rotação de cada bloco. Assim, facilmente lemos:

    - Você pode ler facilmente esta mensagem?

    - cêVo depo ler cilmentefa taes sagemmen?

Em muitas aplicações práticas, a criptografia simétrica e a criptografia assimétrica são combinadas para aproveitar as vantagens de cada uma delas. Por exemplo, em um protocolo de comunicação como o SSL/TLS, a criptografia assimétrica é usada para estabelecer uma conexão segura e compartilhar uma chave secreta, que será utilizada na criptografia simétrica dos dados transmitidos entre as partes. Essa abordagem híbrida oferece uma solução eficiente e segura para a troca de informações confidenciais.

Em resumo, a criptografia simétrica e a criptografia assimétrica são técnicas fundamentais para garantir a segurança das informações em ambientes digitais. Enquanto a criptografia simétrica é mais rápida e eficiente em termos de recursos, a criptografia assimétrica oferece maior segurança e flexibilidade na troca de informações. A escolha entre as duas técnicas depende das necessidades específicas de cada caso e, muitas vezes, uma combinação das duas abordagens é a solução ideal para garantir a segurança e a privacidade das comunicações.

24.3 HASH

As funções HASH são algoritmos criptográficos unidirecionais. Utiliza-se funções matemáticas que permitem gerar um resultado de tamanho fixo independentemente do tamanho do conteúdo de entrada.

Desse modo, por ser unidirecional, isso quer dizer que, a partir de um resultado, não há algoritmos ou chave que retorne à mensagem original.

Para se ter uma ideia, podemos aplicar um algoritmo HASH (MD5) a uma sequência como "123456" e teremos como resultado o texto "e10adc3949ba59abbe56e057f20f883e". Mesmo que alguém tenha acesso ao último conteúdo, não há como saber que foi a mensagem "123456" que gerou tal resultado.

As principais aplicações das funções HASH são para garantir os princípios de integridade, autenticidade e confidencialidade. Vamos citar alguns exemplos. Para fins de confidencialidade e autenticidade, podemos citar o logins com a utilização de senhas que fazemos em sites. Os servidores de dados que armazenam as informações de LOGIN e SENHAS não armazenam os dados diretamente. Eles armazenam o resultado do HASH das senhas. Isto é, vamos supor que eu tenha uma senha do tipo "senhapadrão".

O valor HASH MD5 desse texto é "aa52af9c01caa48a0d2958c961112b5b". Assim, o valor que o servidor armazenará é o HASH. Na próxima vez que eu fizer o login, digitarei meu nome de usuário e senha normalmente. Porém, para verificar se minha senha é válida, o servidor calculará novamente o HASH da senha digitada e comparará com o valor HASH armazenado. Como o algoritmo é padrão, logo, teremos sempre o mesmo valor HASH para a mesma entrada.

A confidencialidade pode ser garantida nesse caso na hipótese de violação da base de dados do servidor. Assim, caso as mensagens em claro fossem armazenadas, o atacante teria obtido facilmente todas essas informações. Mas, como o que está armazenado é somente o valor do HASH, isso dificultará o processo de obtenção das senhas por parte do atacante.

Para fins de integridade, temos uma mensagem que deve ser enviada a um destinatário. Desse modo, envia-se a mensagem e o resultado do HASH da referida mensagem. Quando o destinatário receber essas duas informações, ele pegará o texto em claro e fará o cálculo da função HASH dessa mensagem e comparará com a outra mensagem recebida. Caso sejam idênticas, quer dizer que, de fato, não houve alteração na mensagem recebida. Caso seja diferente, assume-se que houve uma violação à integridade dos dados. Esse modelo é muito utilizado na assinatura digital e certificado digital.

Outras características que surgem nas funções de HASH é que estas devem apresentar modelos matemáticos e cálculos simples que exijam pouco processamento das informações. Além disso, o conceito de difusão diz que deve ser impossível modificar a mensagem original sem modificar o resultado do HASH desta mensagem.

25. CERTIFICAÇÃO DIGITAL E ASSINATURA DIGITAL

São conceitos relacionados à segurança e autenticidade de informações em ambientes eletrônicos. Eles são fundamentais para garantir a integridade e a confidencialidade das comunicações e transações digitais.

25.1 Certificação Digital:

A Certificação Digital é um processo que utiliza certificados digitais para verificar a identidade de indivíduos, organizações ou dispositivos em redes eletrônicas. Um certificado digital é um documento eletrônico que contém informações sobre a entidade à qual ele pertence, como nome, endereço de e-mail e chave pública, além de informações sobre a autoridade certificadora (CA) que emitiu o certificado.

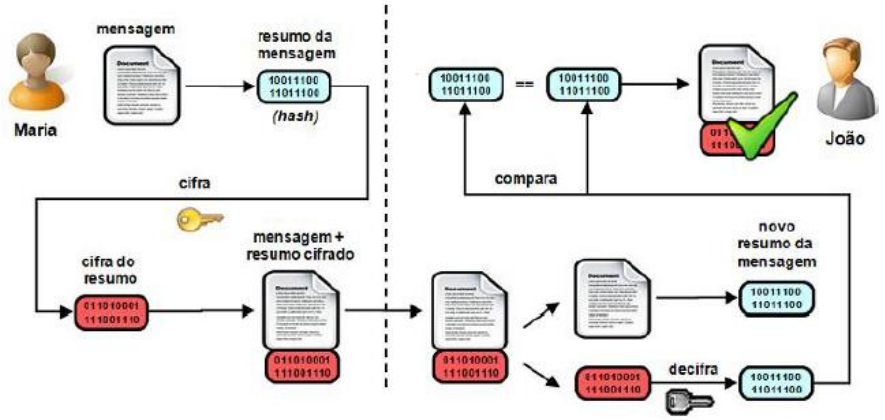
ICP (Infraestrutura de Chaves Públicas): O ICP é um conjunto de políticas, processos e tecnologias que permitem a criação, distribuição, gerenciamento e revogação de certificados digitais. A ICP é composta por Autoridades Certificadoras (CAs), que são organizações responsáveis pela emissão e gerenciamento de certificados digitais, e Autoridades de Registro (ARs), que são responsáveis por validar a identidade dos solicitantes de certificados digitais.

Principais componentes da Certificação Digital:

- Autoridade Certificadora (CA): Entidade responsável pela emissão e gerenciamento de certificados digitais.
- Autoridade de Registro (AR): Entidade que valida a identidade dos solicitantes de certificados digitais e encaminha as solicitações para a CA.
- Repositório de Certificados: Um banco de dados ou serviço de diretório onde os certificados digitais e informações relacionadas são armazenados e podem ser consultados.
- Lista de Certificados Revogados (CRL): Um registro que lista todos os certificados digitais revogados, informando às partes interessadas que esses certificados não devem mais ser considerados válidos.

25.2 Assinatura Digital:

- A Assinatura Digital é um mecanismo criptográfico que permite a autenticação de documentos ou mensagens digitais, garantindo a integridade e a autenticidade das informações.
- A assinatura digital é gerada a partir de um algoritmo de hash aplicado ao conteúdo do documento, juntamente com a chave privada do remetente. O resultado é um valor único (assinatura) que é anexado ao documento.



Conceituação de Assinatura Digital:

A assinatura digital serve para confirmar a identidade do remetente e garantir que o conteúdo do documento não foi alterado durante a transmissão. Para verificar a autenticidade de uma assinatura digital, o destinatário aplica o algoritmo de hash ao conteúdo do documento e utiliza a chave pública do remetente para verificar se o resultado corresponde ao valor da assinatura. Se os valores coincidirem, a assinatura é considerada válida e o documento autêntico.

Em resumo, a Certificação Digital e a Assinatura Digital são fundamentais para garantir a segurança e a autenticidade das comunicações e transações em ambientes eletrônicos. A Certificação Digital, por meio da ICP, fornece uma estrutura confiável para a emissão e gerenciamento de certificados digitais, enquanto a Assinatura Digital permite a autenticação e verificação da integridade de documentos e mensagens digitais.

26. PLANO DE CONTINUIDADE DE NEGÓCIO E CONTINGÊNCIA

Plano de Continuidade de Negócios (PCN): Desenvolvimento preventivo de um conjunto de estratégias e planos de ação de maneira a garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre, até o retorno à situação normal de funcionamento da empresa dentro do contexto do negócio do qual faz parte.

Um primeiro ponto a se destacar é que a maneira mais básica de você combater a perda de informação é duplicá-la. Ou seja, uma informação armazenada em um disco rígido pode ser copiada para outro para prevenir falhas no disco e perder a informação.

Entretanto, colocar os dois discos em um mesmo servidor pode não ser suficiente, uma vez que um problema grave nesse servidor pode danificar os dois discos. Então, nessa perspectiva, coloca-se a informação em discos diferentes e em servidores diferentes.

Novamente, podemos ter um novo problema. E se o Datacenter em questão pega fogo e destrói todos os servidores?

Nesse sentido, é o caso de pensar em duplicar o Datacenter... Agora, ao duplica-lo, é necessário mantê-lo ativo e compartilhando os recursos?

Todas essas questões devem ser consideradas quando se busca construir um PCN. Bem como um plano de recuperação de desastres justamente para definir a forma como agir em determinadas circunstâncias.

Para já adiantarmos um conceito que recorrentemente cai em prova, quando falamos de duplicar um DATACENTER, podemos aplicar algumas técnicas:

1. HOT SITE – Neste caso, os dois DATACENTERS ficam funcionando ativamente e compartilhando recursos. No caso da falha de um, não há qualquer prejuízo dos dados e, inclusive, da disponibilidade dos serviços que estão sendo providos pelos DATACENTERS.

2. COLD SITE - Neste caso, tem-se um outro ambiente com a infraestrutura necessária e suficiente para o reestabelecimento do serviço sem prejuízo das informações. Este novo ambiente não está ativo e compartilhando recursos como o ambiente original como o HOTSITE. Ou seja, em caso de falha do primeiro, tem-se um pequeno intervalo de indisponibilidade, que seria o tempo necessário para "ligar" o novo DATACENTER que já estava preparado.

Um ponto que devemos ressaltar é que a utilização de ambientes temporário para essa finalidade não é uma OBRIGAÇÃO. Portanto, eles podem ou não ser utilizados a depender da criticidade.

Lembrando que tudo envolve custos a serem considerados nas estratégias das organizações. Partindo das nossas considerações feitas até agora, um outro ponto que surge para nossa atenção diz respeito à distância entre estes SITES ou DATACENTERS.

Como a ideia é justamente suportar grandes catástrofes, a recomendação é que fiquem em distâncias consideráveis para suportar eventuais catástrofes que venham a dizimar uma cidade inteira.

Pessoal, um ponto que merece o nosso destaque é referente à necessidade de se validar e verificar se os planos estão devidamente escritos e são executáveis.

A título de exemplo, no ambiente COLDSITE, é importante que de vem em quando se faça a atividade de subir o ambiente e verificar se tudo está funcionando e, se os tempos previstos, ações, pessoas e todo o resto envolvido está dentro das conformidades.

Alguns autores tratam esse processo no âmbito de auditoria do PCN, outros consideram como simples ação de monitoramento e operação do PCN. Imagine todo o investimento feito para, no caso da necessidade, descobrir que as baterias de um no-break por exemplo, estavam descarregadas.

Então é muito importante verificar e testar o plano de maneira periódica. No que tange ao plano, precisamos saber também a sua composição em termos dos subplanos:

Plano de Contingência (emergência) – PC

Deve ser utilizado em último caso, quando todas as prevenções tiverem falhado. Define as necessidades e ações mais imediatas.

Plano de Administração de Crises – PAC

Define funções e responsabilidades das equipes envolvidas com o acionamento das ações de contingência, antes durante e após a ocorrência.

Plano de Recuperação de Desastres – PRD

Determina o planejamento para que, uma vez controlada a contingência e passada a crise, a empresa retome seus níveis originais de operação.

Plano de Continuidade Operacional - PCO

Seu objetivo é reestabelecer o funcionamento dos principais ativos que suportam as operações de uma empresa, reduzindo o tempo de queda e os impactos provocados por um eventual incidente. Um exemplo simples é a queda de conexão à internet.

Além disso, o PCN deve considerar os aspectos abaixo em seus respectivos PLANO DE AÇÕES:

- como o PCN é ativado;
- as pessoas responsáveis por ativar o plano de continuidade de negócios;
- o procedimento que esta pessoa deve adotar ao tomar esta decisão;
- as pessoas que devem ser consultadas antes desta decisão ser tomada;
- as pessoas que devem ser informadas quando a decisão for tomada;
- quem vai para onde e quando;
- quais serviços estão disponíveis, aonde e quando, incluindo como a organização mobilizará seus recursos externos e de terceiros;
- como e quando esta informação será comunicada e
- se relevante, procedimentos detalhados para soluções manuais, recuperação dos sistemas etc.

26.1 Norma ABNT NBR ISO/IEC 22301:

A norma ISO/IEC 22301 é uma norma internacional que estabelece os requisitos para um Sistema de Gestão de Continuidade de Negócios (SGCN). Essa norma fornece um conjunto de diretrizes e melhores práticas para auxiliar as organizações na identificação de riscos, desenvolvimento de estratégias de recuperação e implementação de um PCN eficiente e eficaz.

26.2 Norma ABNT NBR ISO/IEC 22313:

A norma ISO/IEC 22313 é um guia prático que complementa a ISO/IEC 22301, fornecendo orientações detalhadas sobre a implementação de um SGCN. A norma aborda aspectos como a análise de impacto nos negócios, avaliação de riscos, estratégias de continuidade, exercícios e testes, revisão e melhoria contínua do PCN.

26.3 Norma ABNT NBR ISO/IEC 27031:

A norma ISO/IEC 27031 é uma norma específica da área de Tecnologia da Informação e Comunicação (TIC) que trata da continuidade dos negócios. Ela fornece diretrizes para a implementação de um Plano de Continuidade de TIC (PCTIC), que busca garantir a resiliência e recuperação dos sistemas, redes e serviços de TIC em caso de interrupções. A norma aborda aspectos como a análise de impacto nos negócios de TIC, a identificação de recursos críticos de TIC, a definição de estratégias de recuperação e a realização de exercícios e testes.

27. NORMA ABNT NBR ISO/IEC 27701:2019

A norma ABNT NBR ISO/IEC 27701:2019, também conhecida como ISO/IEC 27701, é uma extensão à norma ISO/IEC 27001 e ISO/IEC 27002, que fornece orientações específicas para a implementação de um Sistema de Gestão de Privacidade da Informação (SGPI). Essa norma foi desenvolvida para ajudar as organizações a estabelecer, manter e melhorar continuamente a gestão da privacidade da informação no contexto da proteção de dados pessoais.

Objetivos e Princípios:

A ISO/IEC 27701 tem como principal objetivo fornecer um conjunto de requisitos e recomendações para que as organizações possam gerenciar efetivamente os riscos associados à privacidade da informação e garantir a conformidade com as regulamentações de proteção de dados, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia e a Lei Geral de Proteção de Dados (LGPD) do Brasil. Essa norma baseia-se em princípios fundamentais de privacidade, como minimização de dados, limitação de finalidade, transparência, integridade e confidencialidade.

Estrutura e Requisitos:

A ISO/IEC 27701 é organizada em seções que abordam diferentes aspectos do SGPI, incluindo:

- Requisitos Gerais: Definição do escopo do SGPI, estabelecimento de políticas e objetivos de privacidade, e identificação das partes interessadas e requisitos legais e regulatórios aplicáveis.
- Avaliação e Tratamento de Riscos: Identificação, análise e tratamento de riscos relacionados à privacidade da informação, levando em consideração o contexto organizacional e as necessidades das partes interessadas.
- Controles de Privacidade: Implementação de controles de privacidade específicos, de acordo com as recomendações da ISO/IEC 27002, para garantir a proteção adequada dos dados pessoais.
- Monitoramento e Melhoria Contínua: Estabelecimento de processos de monitoramento, medição, análise e avaliação do desempenho do SGPI, bem como a identificação e implementação de ações corretivas e de melhoria contínua.
- Benefícios e Certificação: A adoção da ISO/IEC 27701 oferece diversos benefícios às organizações, como maior confiança das partes interessadas, redução de riscos associados à privacidade da informação, conformidade com regulamentações de proteção de dados e melhoria contínua das práticas de privacidade. Além disso, a obtenção de uma certificação ISO/IEC 27701 pode servir como uma prova de conformidade com os requisitos da norma e demonstrar o compromisso da organização com a proteção da privacidade da informação.
- Integração com outras normas: A ISO/IEC 27701 foi projetada para ser integrada a outras normas de sistemas de gestão, como a ISO/IEC 27001 (Sistema de Gestão de Segurança da Informação) e a ISO 9001 (Sistema de Gestão da Qualidade). Isso permite que as organizações estabeleçam um SGPI em conjunto com outros sistemas de gestão existentes,

proporcionando uma abordagem holística para a proteção da informação e a melhoria contínua dos processos.

- Implementação e Manutenção: A implementação da ISO/IEC 27701 envolve várias etapas, como a definição do escopo do SGPI, a identificação das partes interessadas e requisitos legais e regulatórios aplicáveis, a avaliação e tratamento de riscos, a implementação de controles de privacidade e a criação de processos de monitoramento e melhoria contínua. A manutenção e melhoria do SGPI requerem o estabelecimento de um ciclo de revisão e aprimoramento contínuo, incluindo a realização de auditorias internas e externas, a análise crítica pela direção e a identificação de oportunidades de melhoria.

Em resumo, a norma ABNT NBR ISO/IEC 27701:2019 é uma importante extensão das normas ISO/IEC 27001 e ISO/IEC 27002, que fornece um conjunto de requisitos e orientações para a implementação e gestão efetiva da privacidade da informação. A adoção dessa norma ajuda as organizações a garantir a proteção dos dados pessoais, gerenciar os riscos associados à privacidade da informação e alcançar a conformidade com as regulamentações de proteção de dados. Ao adotar a ISO/IEC 27701, as organizações demonstram seu compromisso com a proteção da privacidade da informação e ganham a confiança das partes interessadas, incluindo clientes, funcionários e parceiros de negócios.

Em suma, a norma ABNT NBR ISO/IEC 27701:2019 fornece um conjunto de requisitos e orientações abrangentes para a implementação de um Sistema de Gestão de Privacidade da Informação. Ao adotar essa norma, as organizações demonstram seu compromisso com a proteção da privacidade da informação e a conformidade com as regulamentações de proteção de dados. A certificação ISO/IEC 27701 pode ajudar a aumentar a confiança das partes interessadas e a garantir a proteção adequada dos dados pessoais no ambiente digital atual.

28. A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) Nº 13.709/2018

A Lei Geral de Proteção de Dados (LGPD) nº 13.709/2018 é uma legislação brasileira que entrou em vigor em setembro de 2020 e tem como objetivo regulamentar o tratamento de dados pessoais de indivíduos no Brasil. A LGPD foi inspirada pelo Regulamento Geral de Proteção de Dados (GDPR) da União Europeia e estabelece diretrizes e obrigações às organizações que coletam, armazenam, processam e compartilham dados pessoais.

Princípios da LGPD:

A LGPD estabelece dez princípios fundamentais que devem ser seguidos durante o tratamento de dados pessoais: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

Direitos dos Titulares dos Dados:

A LGPD garante aos titulares dos dados uma série de direitos relacionados ao tratamento de seus dados pessoais, incluindo o direito de acesso, retificação, eliminação, anonimização, portabilidade, informação, revogação do consentimento e oposição ao tratamento de dados.

Agentes de Tratamento:

A LGPD define dois agentes de tratamento de dados pessoais: o controlador, que é a entidade responsável por tomar as decisões relacionadas ao tratamento de dados, e o operador, que realiza o tratamento dos dados pessoais em nome do controlador.

Consentimento e Legitimação do Tratamento de Dados:

A LGPD estabelece que o tratamento de dados pessoais deve ser baseado no consentimento expresso e inequívoco do titular dos dados, a menos que haja outra base legal que permita o tratamento sem o consentimento, como o cumprimento de uma obrigação legal, a execução de contrato, proteção da vida, tutela da saúde, interesse legítimo, entre outros.

Transferência Internacional de Dados:

A LGPD estabelece requisitos específicos para a transferência internacional de dados pessoais, como garantir que o país ou organização receptora ofereça um nível adequado de proteção aos dados ou a utilização de cláusulas contratuais específicas, garantindo a proteção dos dados pessoais.

Autoridade Nacional de Proteção de Dados (ANPD):

A ANPD é o órgão responsável por fiscalizar o cumprimento da LGPD, emitir normas, orientações e aplicar sanções em caso de violação da lei. As sanções podem incluir advertências, multas e até a proibição parcial ou total do tratamento de dados pessoais.

Encarregado de Proteção de Dados (DPO):

A LGPD exige que as organizações nomeiem um Encarregado de Proteção de Dados (DPO), responsável por orientar e supervisionar as atividades relacionadas ao tratamento de dados pessoais e servir como canal de comunicação entre a organização, os titulares dos dados e a ANPD.

Relatório de Impacto à Proteção de Dados Pessoais (RIPD):

A LGPD prevê a elaboração de um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) para avaliar os riscos e medidas de mitigação associados ao tratamento de dados pessoais, especialmente em situações de alto risco, como tratamento de dados sensíveis ou em larga escala.

Programa de Governança em Privacidade:

A LGPD recomenda que as organizações implementem um Programa de Governança em Privacidade para garantir o cumprimento dos requisitos legais e regulatórios relacionados à proteção de dados

pessoais. Este programa deve incluir políticas, procedimentos, treinamentos e mecanismos de monitoramento e avaliação do desempenho das práticas de privacidade.

Boas Práticas e Certificações:

A LGPD incentiva as organizações a adotarem boas práticas e certificações que demonstram o compromisso com a proteção de dados pessoais e o cumprimento das normas estabelecidas pela legislação. A adoção de normas internacionais, como a ISO/IEC 27701, pode ajudar as organizações a estabelecer um Sistema de Gestão de Privacidade da Informação (SGPI) e garantir a conformidade com a LGPD.

Em resumo, a Lei Geral de Proteção de Dados nº 13.709/2018 é uma legislação abrangente que visa proteger a privacidade e os direitos dos titulares dos dados no Brasil. A LGPD estabelece princípios, direitos, obrigações e mecanismos de fiscalização para garantir a proteção adequada dos dados pessoais e incentivar a transparência e responsabilidade das organizações que tratam dados pessoais. A conformidade com a LGPD é crucial para as organizações que operam no Brasil, a fim de evitar sanções e garantir a confiança dos titulares dos dados e das partes interessadas.

Em conclusão, a Lei Geral de Proteção de Dados nº 13.709/2018 é uma legislação fundamental para proteger os direitos e a privacidade dos titulares de dados no Brasil. A LGPD estabelece princípios, direitos, obrigações e mecanismos de fiscalização que devem ser seguidos pelas organizações que tratam dados pessoais. O cumprimento da LGPD é essencial para evitar sanções e garantir a confiança dos titulares dos dados, bem como para promover a transparência e a responsabilidade das organizações envolvidas no tratamento de dados pessoais.