TEMA 07
Segurança em Redes de Computadores e Dispositivos Móveis

Habilidades:

- Entender a importância da integridade e confidencialidade dos dados.
- Aprender a elaborar e decifrar armadilhas digitais e falsificações.
- Compreender e elaborar perfis para evitar golpes de engenharia social

Segurança em redes de computadores e dispositivos móveis é um conjunto de práticas e medidas implementadas para proteger informações e sistemas contra ameaças cibernéticas. Isso envolve a aplicação de técnicas como **criptografia, autenticação, controle de acesso e monitoramento para garantir a confidencialidade, integridade e disponibilidade dos dados**.

Em redes de computadores, são utilizados firewalls, antivírus e detecção de intrusões para prevenir e detectar ataques. Em dispositivos móveis, são adotadas medidas como atualizações de software, autenticação forte, proteção contra malware e backup de dados para garantir a segurança dos dispositivos e das informações armazenadas neles. A segurança em redes de computadores e dispositivos móveis é fundamental para proteger dados pessoais e corporativos, evitar violações de privacidade e assegurar um ambiente digital seguro.

A popularidade dos dispositivos móveis como smartphones, notebooks, tablets e wearables (dispositivos vestíveis como relógios inteligentes) nunca esteve tão alta no nosso cotidiano. Através deles, é possível desempenhar boa parte das tarefas de trabalho, estudo e entretenimento, que há alguns anos atrás apenas PC's faziam e com muito esforço.

Da mesma maneira que protegemos nossos dispositivos físicos e a rede que se conectam, não podemos deixar de dar a devida atenção à segurança dos dispositivos móveis, já que passam pelos mesmos riscos. O objetivo é basicamente o mesmo da segurança em redes de computadores: impedir que pessoas mal-intencionadas acessem os dados e informações contidos nestes aparelhos por meio da rede e aplicações indesejadas e evitar a perda destes dados por qualquer tipo de acidente.

Para os métodos de segurança de redes surtirem efeito de fato, as políticas de segurança da informação devem estar em plena sintonia, pois reforçará o controle hierárquico de acesso aos usuários e a devida instrução. Tanto os **usuários comuns como os colaboradores de uma empresa devem estar atentos às orientações** referentes a todos os métodos e adotar as boas práticas de segurança para não ficarem vulneráveis e sofrerem prejuízos.

Existem alguns riscos e ameaças que reforçam a importância de uma implementação da segurança de rede em qualquer lugar. Todos irão explorar algum tipo de vulnerabilidade ou falta de atenção do usuário. São eles:

Malwares

Malwares são softwares ou trechos de códigos desenvolvidos com um intuito malicioso por trás. São feitos com o objetivo de invadir sistemas, espionar, roubar dados e informações e até mesmo destruir por completo um sistema. Ele pode **afetar** computadores, servidores e até mesmo smartphones e podem ser transmitidos através de uma rede.

Existem diversos tipos de malwares. Dentre os mais populares, podemos citar:

Vírus – Como o próprio nome sugere, o vírus é um software capaz de se multiplicar e infectar, desde documentos, até mesmo outras aplicações instaladas no dispositivo. Ele fica dentro do arquivo e ao ser aberto, o vírus se espalha ainda mais, o que pode comprometer totalmente uma rede de computadores.

Ransomware – Vem ganhando popularidade devido ao grande número de ataques atualmente. É uma ameaça que realiza, literalmente, o sequestro de todos os dados e informações de um sistema operacional ou aplicação através de uma criptografia de alta complexidade.
Geralmente uma mensagem ao usuário é exibida, o que impede o uso do equipamento e informa sobre o ataque juntamente com o passo a passo de resgate. Caso o usuário não realize o pagamento deste resgate, todos os arquivos e documentos são definitivamente apagados.

Spyware – É um software que tem como objetivo analisar e coletar os dados e informações da vítima, sem a sua autorização. O atacante, através do spyware, consegue receber essa coleta de maneira remota.
De modo geral, os spywares aparecem na forma de screenloggers, o qual captura imagens da tela do usuário, e indica ao atacante onde a vítima está clicando, ou keyloggers, que capturam as teclas digitadas pela vítima. Através destas ferramentas, o hacker consegue obter acesso a senhas e outros dados confidenciais.

Backdoor – Backdoor ou "porta dos fundos" é um código que explora falhas já existentes no sistema e é capaz de criar novas brechas de segurança a partir delas. A finalidade é fragilizar o ambiente para que se torne vulnerável a ataques maiores.

Cavalo de Troia – É um software que o próprio usuário instala, e acredita (técnicas de Engenharia Social) ser uma aplicação original/legítima e vai lhe trazer alguma utilidade. São capazes de liberar o acesso aos dados e informações pertinentes à vítima.

Rootkit – É um malware dedicado a conceder ao atacante o acesso total a um dispositivo, de modo remoto e sem ser detectado.

Bot – São códigos capazes de conceder o acesso remoto de computadores e outros dispositivos ao atacante. Através dele, é possível inserir outros códigos maliciosos que podem comprometer o funcionamento ou coletar dados e informações da vítima.

Worm – Semelhante ao vírus, os Worms são softwares capazes de criar cópias de si de maneira autônoma e se espalhar pela rede de computadores ou internet. A diferença dele para o vírus é que ele não precisa se hospedar em nenhum arquivo, ou seja, não depende de que o usuário interaja com ele para se propagar e causar danos.

Engenharia Social

Procedimento o qual os hackers manipulam o psicológico das vítimas para realizar transações, compartilhar dados e instalar aplicativos maliciosos.

Injection SQL

Até aqui compreendemos que a organização e proteção dos dados e informações são primordiais ao estabelecimento de estratégias e métricas que a organização segue de modo a atingir seus objetivos. Partindo do contexto digital, atualmente, nenhuma empresa vive sem pelo menos um Banco de Dados. É através deles que armazenamos os dados e informações estruturadas e os organizamos da melhor forma possível para consultá-los posteriormente.

Uma só empresa ou aplicação pode ter diversos bancos de dados. Cada um destinado a um ativo de informação específica e, em sua maioria, interligados. Um banco bem estruturado é aquele o qual a criação, leitura, atualização e exclusão dos dados são bem estipulados e controlados por profissionais capacitados. Lembre-se que todos os ativos de informação estão neles, e podem ser poucos, ou milhões. Portanto, exige-se muita cautela para controlá-lo e hierarquizar o seu acesso.

A linguagem mais comum na qual grande parte dos bancos de dados se baseia é a SQL (*Structured Query Language*, ou Linguagem de Consulta Estruturada), onde os comandos do banco de dados serão executados a partir dela. Com este recurso, podemos realizar o que chamamos de **CRUD (*Create, Read, Update, Delete*)**, ou seja, criar, ler, atualizar/modificar e deletar as informações contidas no banco de dados associados a alguma aplicação.

Dito isso, precisamos ter muita cautela ao manusear e passar o controle, seja parcial ou total a um banco de dados. Ademais, devemos garantir que a segurança dele perante ataques internos e externos seja preservada.

Por ser uma linguagem internacional e a mais popular, como consequência, é uma das que mais sofrem com ataques e falhas. E uma das mais conhecidas que, ainda podem ocorrer a um banco de dados, e ocasiona sérios problemas é o **SQL Injection (Injeção SQL)**, uma técnica na qual o indivíduo imputa um trecho código SQL (conhecido como Query) manipulado maliciosamente de algum campo vulnerável da aplicação que interage com o banco de dados a fim de realizar consultas para obter dados e informações sigilosas, ou até mesmo alterar ou apagar o que está armazenado no banco.

Como resultado deste ataque, diversos dados confidenciais como credenciais, senhas, e outras informações críticas e sigilosas são expostas e, muitas vezes violados, e ferem os princípios, principalmente dos pilares da Integridade e Confidencialidade da Segurança da informação, o que resulta em prejuízos e danos à imagem e reputação de uma empresa, muitas vezes irreparáveis.

Esta falha não tem relação com as ferramentas usadas para desenvolver a aplicação ou banco, mas sim com o próprio desenvolvedor que não adotou tratativas para impedir o SQL Injection.

Você aprenderá dois dos tipos de ataques mais comuns de SQL Injection. O por meio de formulários e de URL's.

SQL Injection em formulários

Para exemplificar o SQL Injection, neste primeiro momento, vamos imaginar um formulário de autenticação de usuário em um site qualquer.

josemoura
010203
CONTINUAR

Este formulário solicita duas variáveis para o cliente: o usuário e a senha. Assim que estes dados forem inseridos e o botão "CONTINUAR" for clicado, a aplicação fará uma consulta no banco de dados para procurar estes atributos e permitir o acesso caso encontre.

Vamos supor que inserimos o usuário **josemoura** e a senha **010203.**

A query(consulta) ficaria desta forma:

SELECT * FROM usuários WHERE usuário = josemoura' AND senha = “010203'

Aqui, o código solicita todos os resultados que estejam na tabela de usuários, em que o usuário for igual a **josemoura** e a senha seja **010203.** Agora, imagine que algum criminoso, na tentativa de obter acesso aos dados, colocasse esses comandos nos campos:

qualquercoisa' OR 1=1 #
*
CONTINUAR

Na consulta, ficou desta forma:

SELECT * FROM usuários WHERE usuário = 'qualquercoisa” * / OR 1=1; # AND senha = '010203'

No campo usuário, o atacante digitou um texto qualquer para indicar um usuário e colocou uma condicional “ou” de 1=1. O número 1 sempre será igual a 1, então, o sistema viu que havia nenhum usuário **“qualquercoisa”** dentro do banco e partiu para a segunda condicional **OR,** que simplesmente ignorou o campo usuário. O símbolo **“#”** transformou o restante da consulta, que está em verde em um comentário, ou seja, na hora da consulta, este campo será ignorado e ele conseguirá logar no sistema.

SQL Injection em URL

Por incrível que pareça, há a possibilidade de atacar sites apenas por meio da URL. A URL em si, ou *Uniform Resource Locator* (Localizador Uniforme de Recursos) é o endereço da aplicação disponível em uma rede, isto é, o endereço de um site que esteja na Web.
O método de invasão por SQL Injection via URL tem como objetivo atacar a aplicação a partir de uma vulnerabilidade encontrada em seu endereço.

Vamos usar como exemplo esta URL:

http://www.supercyberbrasil.com/noticias.php?cat=3

É possível identificar visualizando o final deste link que há um dado sendo transmitido de uma página para outra dentro da aplicação. Sabemos disso através do **“?”** e este dado pode ser tanto um número, igual o exemplo acima, como também letras ou palavras. Neste caso, o **“cat”** representa uma categoria de notícias e o link pede que seja a categoria de número **3**.

O código em SQL que podemos prever é:

SELECT * FROM noticias WHERE codigo='$cat”

Em outras palavras, ele busca uma notícia em que o código da categoria seja o mesmo do número que se encontra no endereço URL.

Para identificar se este site está vulnerável, podemos simplesmente remover o parâmetro de categoria. Caso o site apresente uma mensagem de erro de sintaxe de SQL, já é um sinal que há uma falha de segurança. Ficaria dessa forma:

http://www.supercyberbrasil.com/noticias.php?cat=

E retornaria no site algo parecido como:

You have an error in your SQL syntax ...

Um dos usos deste ataque é, por exemplo, reunir informações de várias tabelas do banco de dados através do comando **UNION**.

Pode ser inserido desta forma no navegador:

http://www.supercyberbrasil.com/noticias.php?cat=3 UNION ALL SELECT, 1,2,3,4.

Ou seja, solicita a consulta de todos as informações nas tabelas e colunas especificadas. Em posse destas informações, o criminoso conseguirá ir muito mais fundo e realizar outros procedimentos de invasão.
Apesar o SQL Injection não estar mais com tanta força como era há alguns anos, justamente pela evolução nos meios de proteção, não se deve baixar a guarda para manter o ambiente seguro.

NEGAÇÃO DE SERVIÇO – DoS e DDoS

Dentre os ataques web mais conhecidos, não podemos deixar de citar o DoS (*Denial of Service* – Negação de Serviço) e o DDoS (*Distributed Denial of Service* – Negação de Serviço Distribuída). De modo geral, não funcionam para roubar ou invadir dados e informações, mas para tirar do ar uma aplicação e/ou os servidores que a mantém ativa, e a sobrecarrega temporariamente por meio de várias métricas. São os ataques que exploram a **Disponibilidade**, um dos pilares da Segurança da Informação.

E são vários os motivos pelos quais esta abordagem é feita. Uma interrupção de alguma aplicação, ainda que rápida, pode causar prejuízos incalculáveis para a organização. Pode ser utilizada tanto para extorquir o proprietário da aplicação, pedir um resgate para a normalização do serviço, como também como estratégia para derrubar aplicações e outros serviços de concorrentes a fim de prejudicá-los em algum momento em específico.

Os ataques DoS e DDoS irão realizar diversas requisições a um servidor, aplicação ou até uma rede ou infra de maneira proposital com o intuito de exceder a capacidade de processamento a ponto de não conseguir realizar mais nenhum outro tipo de tarefa, o que derruba o serviço temporariamente.

Isso faz com que até **os usuários legítimos não consigam acessar os dados**.

Os atacantes realizam toda uma investigação e planejamento nesta investida. Eles conseguem avaliar qual é o melhor alvo e o momento certo para atacar. Desde um hardware e sua capacidade, como até mesmo uma vulnerabilidade na aplicação ainda não resolvida e que, forçando-o para acontecer, trará instabilidades e interrupções comprometedoras. Como fazê-lo consumir todo o processamento ou memória RAM de um servidor Web, e interromper e derrubar totalmente a aplicação.

DoS

Nos ataques DoS, as requisições realizadas irão partir apenas do computador do criminoso direto para o servidor de aplicação. São comumente utilizados em dispositivos mais simples e fracos.

Do DDoS, o cibercriminoso estará munido de **mais máquinas para realizar o ataque**. Ele conseguirá, através de ataques de malwares, se apossar de computadores que controlam outros, e produzir

uma ação de “escravidão” a outros computadores para fazer o “serviço sujo”. Normalmente, chamamos **estas máquinas controladoras de Mestre, enquanto as escravas chamamos de Zumbis**.

A diferença do Dos para o DDoS é, sem sombra de dúvidas, o poder de fogo. Com mais máquinas trabalhando para ele, o atacante consegue realizar ataques de larga escala a serviços mais parrudos.

Há três métodos de ataque de negação de serviço mais comuns.

São eles:

- *Negação de serviço por excesso ou volume* - Ataques que envolvem, exclusivamente, o **excesso de requisições, o que resulta em um congestionamento no serviço**.
- *Negação de serviço por amplificação* - Ataques que compreendem a falsificação do endereço IP do atacante para realizar requisições a inúmeros servidores simultaneamente.
- *Negação de serviço por protocolos* – Ataques feitos através de inúmeras solicitações de **conexão simultâneas por meio de algum protocolo ou falha na infraestrutura**.

Com a popularidade destes tipos de ataques, fica cada vez mais difícil estabelecer métricas fixas e padronizadas para DoS e DDoS. Como já aprendemos, a educação e a prevenção são fundamentais para combater os crimes cibernéticos.

Para as organizações, de modo geral, uma boa política de segurança baseada na prevenção de anomalias e controle de tráfego de dados e firewall, além dos contínuos testes de penetração, juntamente com a identificação e correção rápida de bugs irão reduzir drasticamente a probabilidade de novos ataques. No entanto, se o ataque for iminente e, realmente, sobrecarregar o serviço a ponto de interrompê-lo, que existam estratégias predefinidas no escopo da política para corrigir e ter o controle da disponibilidade de volta e evitar que isso ocorra novamente.

Varredura e Análise

Para manter uma infraestrutura e um ambiente seguros, além da implantação das políticas de segurança, é necessário o uso de ferramentas de varredura e análise da rede, sistemas operacionais e aplicações. Elas são capazes de auxiliar no encontro de vulnerabilidades, detecção e eliminação de ameaças, e realizar o vasculhamento aprofundado de diversas áreas e é responsável pela emissão de relatórios úteis para a gestão de T.I.

Todas essas devem ser adquiridas e utilizadas de acordo com a real necessidade de cada um, ou seja, ferramentas de varredura e análise são necessárias para realizar um levantamento de todos os requisitos necessários para estabelecer a segurança no ambiente.

Firewall

Firewall é uma das principais ferramentas de proteção a redes de computadores e sistemas.

Traduzindo do inglês, “paredes corta-fogo”, é um dispositivo físico (hardware), software ou híbrido (hardware + software) capaz de filtrar e barrar agentes nocivos dentro de redes domésticas e corporativas computadores/servidores, e evitar que estes agentes se propaguem no ambiente e causem danos e prejuízos.

Estes agentes nocivos podem ser tanto dados mal-intencionados, como também malwares, capazes de se espalharem como verdadeiras pragas.

Quando falamos em **firewall por hardware**, são dispositivos físicos conectados juntamente com a

rede para gerir uma quantidade maior de computadores. Ele é mais recomendado nesses ambientes devido a grande quantidade de tráfego de dados e informações.

O firewall físico tende a ser mais caro do que o software. Isso porque soma-se o custo do equipamento, instalação e implementação e também o controle/manutenção, porém é bem mais otimizado e entrega maior segurança no ambiente.

Normalmente, estes dispositivos vêm de fábrica pré-configurados com algumas políticas genéricas de segurança, mesmo assim, há a personalização de entrada e saída de pacotes ou portas da rede da organização, podendo assim ter um controle maior do que é trafegado e as requisições.

Vale ressaltar que fica sob responsabilidade da equipe de T.I./S.I. manter este dispositivo devidamente atualizado e conforme as políticas de segurança do local.

Já o **firewall via software** é o mais popular. Visam o custo mais baixo e oferecem proteção regular às máquinas pessoais de usuários comuns ou organizações pequenas. Geralmente, são renovados através de licenças anuais e recebem atualizações frequentes do desenvolvedor.

Entretanto, este método é bem mais limitado comparado ao firewall por hardware, pois, de um modo geral, possui menos ferramentas de controle e dependem de o usuário querer atualizá-la, além de consumir o hardware do próprio computador, juntamente com os demais programas utilizados.

Vale ressaltar que nenhum método de segurança é 100% seguro e de nada adianta adquirir qualquer tipo de firewall ou outra ferramenta, se não houver a conscientização do real motivo deste recurso ser implantado. Por isso, em caso de ambientes organizacionais, os colaboradores devem ser devidamente instruídos a utilizar a rede e sistemas operacionais de maneira segura e de acordo com as políticas de segurança, assim como o usuário comum deve se atentar ao que acessa. Quanto mais ferramentas tivermos e com a devida orientação, aprimoramos a segurança dos ativos de informação em qualquer ambiente.

Tipos de Firewall

Os firewalls são componentes essenciais da segurança de rede, pois atuam como barreiras entre a rede interna de uma organização e a Internet externa, permitindo o controle do tráfego de rede e bloqueando o acesso indesejado. A escolha de um firewall dependerá de uma variedade de fatores, incluindo a configuração da rede, os usuários, as necessidades específicas, os hardwares e sistemas operacionais envolvidos, além das políticas de segurança em vigor. Vejamos alguns dos tipos mais populares e utilizados de firewalls:

Firewall de Filtro de Pacotes (Packet-Filtering Firewalls)

Este é o tipo mais básico de firewall. Ele atua no nível de rede do modelo OSI e decide se os pacotes de dados podem passar com base em endereços IP, portas e direção (entrada ou saída).
Embora sejam eficazes, não possuem a capacidade de filtragem de conteúdo.

Firewalls de Inspeção de Estado (Stateful Inspection Firewalls)

Esses firewalls mantêm um registro de todas as conexões ativas. Ao receber um pacote, o firewall verifica se o pacote pertence a uma conexão existente e, em caso afirmativo, permite que o pacote passe sem qualquer inspeção adicional.

Firewalls de Proxy (Proxy Firewalls)

Também conhecidos como gateways de aplicação, esses firewalls atuam como intermediários para o tráfego de rede. Eles filtram pacotes em **nível de aplicação do modelo OSI** e oferecem mais

recursos de segurança, como registro de conteúdo e verificação de autenticidade do usuário.

Firewalls de Próxima Geração (Next-Generation Firewalls - NGFWs)

Os NGFWs são uma combinação de vários tipos de firewalls que incluem funções como filtragem de pacotes, inspeção de estado, inspeção profunda de pacotes, IPS (sistema de prevenção de intrusões) e identificação de usuário. Eles são mais complexos, mas oferecem segurança avançada.

Firewalls Unificados de Ameaças (Unified Threat Management - UTM)

Os **UTMs são dispositivos de segurança multifuncionais**. Eles combinam as funções de um firewall com outros recursos de segurança, como antivírus, prevenção de intrusões e controle de aplicativos.

A escolha do tipo de firewall a ser usado em uma organização depende de uma variedade de fatores, como a natureza do negócio, o tamanho e a configuração da rede, e o nível de segurança necessário. A decisão deve ser tomada levando em consideração a necessidade de equilíbrio entre segurança, desempenho e custo.

RESUMO

A segurança em redes de computadores é o estudo das ameaças em potencial para computadores conectados na internet e quais são as ferramentas e atenções necessárias para termos mais segurança no meio digital. Todo cuidado é pouco na hora de configurar e utilizar qualquer dispositivo conectado à internet.
Com boas práticas de políticas de segurança e ferramentas adequadas ao local de aplicação, diminui-se consideravelmente o risco de ocorrerem novas ameaças e possibilitará a mitigação e correção mais certeira.

Atividades com base no texto:

1. Explique o que é um firewall e qual é o seu papel na segurança de redes de computadores. Cite dois tipos de firewalls e discuta suas diferenças.

Firewall é uma ferramenta essencial na segurança de redes de computadores, atuando como uma barreira que protege a rede interna de uma organização contra ameaças externas. Ele controla o tráfego de dados, decidindo quais pacotes podem entrar ou sair da rede com base em regras de segurança predefinidas.

Dois tipos de firewalls são:
- Firewall de Filtro de Pacotes (Packet-Filtering Firewall): Este é o tipo mais básico de firewall que opera no nível de rede do modelo OSI. Ele permite ou bloqueia pacotes com base em critérios como endereços IP, portas e protocolos. Não tem a capacidade de inspecionar o conteúdo dos pacotes.
- Firewall de Inspeção de Estado (Stateful Inspection Firewall): Este tipo de firewall mantém um registro das conexões ativas e verifica se um pacote pertence a uma conexão existente. Se o pacote fizer parte de uma conexão válida, ele é permitido sem inspeção adicional. Esse tipo de firewall oferece uma segurança mais robusta comparado ao firewall de filtro de pacotes, pois pode rastrear o estado das conexões e filtrar pacotes com base nesse contexto.

2. Discuta a importância da autenticação em redes de computadores. Explique como a autenticação em dois fatores pode fortalecer a segurança dos sistemas.

Autenticação é crucial em redes de computadores porque verifica a identidade dos usuários antes de permitir o acesso a sistemas e dados. Ela impede que pessoas não autorizadas acessem informações confidenciais, ajudando a manter a integridade e a confidencialidade dos dados.

Autenticação em dois fatores (2FA) aumenta significativamente a segurança dos sistemas ao exigir dois tipos de credenciais de verificação: algo que o usuário sabe (como uma senha) e algo que o usuário tem (como um dispositivo móvel). Mesmo que um atacante obtenha a senha, sem o segundo fator, ele não conseguirá acessar o sistema.

3. Descreva o que é criptografia e qual é o seu papel na segurança das comunicações em redes de computadores. Cite dois algoritmos de criptografia amplamente utilizados e explique suas características principais.

Criptografia é o processo de codificação de informações para impedir que pessoas não autorizadas possam lê-las. Na segurança de redes, a criptografia é usada para proteger os dados durante a transmissão, garantindo que apenas as partes autorizadas possam acessar o conteúdo.

Dois algoritmos de criptografia amplamente utilizados são:
- AES (Advanced Encryption Standard): É um algoritmo de criptografia simétrica amplamente utilizado por sua eficiência e segurança. Ele usa chaves de 128, 192 ou 256 bits para criptografar e descriptografar dados, sendo considerado extremamente seguro e rápido.
- RSA (Rivest–Shamir–Adleman): É um algoritmo de criptografia assimétrica que utiliza um par de chaves (uma pública e uma privada) para criptografar e descriptografar dados. Ele é amplamente usado para criptografia de dados e para estabelecer canais seguros de comunicação.

4. Discuta as diferenças entre uma rede local (LAN) e uma rede virtual privada (VPN). Explique como uma VPN pode fornecer segurança adicional para as comunicações em uma rede.

LAN (Local Area Network) é uma rede que conecta dispositivos dentro de uma área limitada, como um escritório ou residência. Ela é geralmente de alta velocidade e opera dentro de um ambiente controlado.

VPN (Virtual Private Network) é uma tecnologia que permite criar uma conexão segura e criptografada sobre uma rede pública, como a internet. Ela permite que usuários remotos acessem uma rede privada como se estivessem fisicamente presentes, garantindo a segurança dos dados transmitidos.

Segurança adicional: Uma VPN fornece segurança adicional ao criptografar todas as comunicações que passam por ela, protegendo os dados contra interceptações e garantindo que apenas usuários autorizados possam acessar a rede privada.

5. Explique o conceito de detecção de intrusões em redes de computadores. Descreva dois métodos comuns de detecção de intrusões e discuta suas vantagens e desvantagens....

Conceito de Detecção de Intrusões em Redes de Computadores

A detecção de intrusões em redes de computadores refere-se ao processo de monitorar e analisar o tráfego de rede e sistemas para identificar atividades suspeitas ou anômalas que possam indicar tentativas de acesso não autorizado, ataques cibernéticos ou violações de políticas de segurança. O objetivo principal dos sistemas de detecção de intrusões (IDS, do inglês *Intrusion Detection Systems*) é identificar possíveis ameaças em tempo real ou quase em tempo real, permitindo que medidas corretivas sejam tomadas para mitigar o impacto dos ataques.

Dois Métodos Comuns de Detecção de Intrusões

5.1. Detecção Baseada em Assinaturas (Signature-based Detection)

- Descrição: Esse método compara o tráfego de rede ou atividades do sistema com um banco de dados de assinaturas conhecidas de ataques e ameaças. Cada assinatura é um padrão ou uma sequência de dados que representa um ataque específico. Se uma correspondência entre o tráfego atual e uma assinatura conhecida for encontrada, o sistema gera um alerta.

- Vantagens:

- Precisão: Como o sistema está comparando diretamente com assinaturas conhecidas, a taxa de falsos positivos tende a ser baixa.
- Facilidade de Implementação: Esse tipo de detecção é mais fácil de implementar e configurar, pois depende de um banco de dados de ameaças já conhecidas.

- Desvantagens:

- Limitação para Novas Ameaças: Esse método é eficaz apenas para ameaças conhecidas. Ataques novos ou variantes de ataques que ainda não foram catalogados podem não ser detectados.
- Atualizações Constantes: O banco de dados de assinaturas precisa ser constantemente atualizado para incluir novas ameaças, o que pode ser um desafio de manutenção.

5.2. Detecção Baseada em Anomalias (Anomaly-based Detection)

- Descrição: Esse método monitora o comportamento normal do sistema ou da rede, criando um perfil padrão. Qualquer desvio significativo desse comportamento padrão é considerado uma anomalia e pode ser sinalizado como uma possível intrusão.

- Vantagens:

- Capacidade de Detectar Ameaças Desconhecidas: Como se baseia no comportamento anômalo, este método pode detectar ataques novos ou inéditos que não possuam assinaturas definidas.
- Adaptabilidade: Pode se ajustar dinamicamente a novos padrões de comportamento conforme a rede ou o sistema evoluem.

- Desvantagens:

- Altos Falsos Positivos: Como qualquer comportamento fora do padrão é considerado uma possível ameaça, há uma maior probabilidade de falsos positivos, onde atividades legítimas são erroneamente classificadas como ameaças.
- Complexidade: A configuração e o ajuste deste tipo de sistema podem ser complexos, exigindo monitoramento constante e, muitas vezes, uma análise mais profunda para interpretar os resultados.

Conclusão

Ambos os métodos de detecção de intrusões têm suas aplicações, e muitas vezes são utilizados em conjunto para cobrir as deficiências um do outro. Enquanto a detecção baseada em assinaturas oferece precisão contra ameaças conhecidas, a detecção baseada em anomalias fornece uma camada adicional de segurança contra ataques novos ou modificados. A escolha entre um ou outro, ou a combinação dos dois, depende das necessidades e recursos específicos da organização.