Semana 27 - Aula 1

Tópico Principal da Aula: Medidas de Segurança: Firewall, WAF e DMZ

Subtítulo/Tema Específico: Conceitos de Implementação de Segurança

Código da aula: [SIS]ANO1C2B4S27A1

Objetivos da Aula:

- **Compreender** os conceitos fundamentais de **Firewall**, **WAF** e **DMZ** (Zona Desmilitarizada).
- **Reconhecer** a importância da segmentação de redes para a proteção de dados, conforme a **LGPD**.
- **Identificar** os diferentes tipos de *Firewall* e suas aplicações práticas no ambiente corporativo.

Recursos Adicionais (Sugestão, pode ser adaptado):

- Caderno para anotações;
- Acesso ao laboratório de informática e/ou internet;
- Software de virtualização (Ex: Oracle VirtualBox ou VMware Workstation).

Exposição do Conteúdo:

Referência do Slide: Slide 04 - O que é um Firewall

- **Definição:** O **Firewall** é um sistema de segurança, que pode ser baseado em *hardware* ou *software*, cuja função principal é monitorar e controlar o tráfego de rede (entrada e saída) com base em um conjunto predefinido de regras de segurança. Ele atua como uma barreira de proteção entre uma rede confiável (rede interna/LAN) e redes não confiáveis (Internet).
- **Aprofundamento/Complemento:** Essencial para a segurança dos dados pessoais sob a LGPD, o *Firewall* opera como um **filtro de tráfego**, decidindo quais pacotes de dados podem passar e quais devem ser bloqueados. É a primeira linha de defesa contra acessos não autorizados e ameaças externas.
- **Exemplo Prático:** Uma empresa configura o *Firewall* para bloquear todo o tráfego externo que tenta se conectar diretamente às portas de desktop dos funcionários (como RDP na porta 3389), permitindo apenas o tráfego destinado ao servidor web corporativo na porta 443 (HTTPS).
    - **Link de Vídeo 1:** O que é um firewall em redes?
    - **Link de Vídeo 2:** Tipos de firewall e como funcionam

Referência do Slide: Slide 06 - Tipos de Firewalls: Filtragem de Pacotes vs. Aplicação

- **Definição:**
    - **Firewall de Filtragem de Pacotes (Packet Filtering):** Verifica apenas as informações de **cabeçalho** do pacote (endereço IP de origem e destino, porta e protocolo), operando nas camadas 3 e 4 do modelo OSI. É rápido, mas não inspeciona o conteúdo real do pacote de dados.

    - **Firewall de Aplicação (Proxy/NGFW - Next-Generation Firewall):** Atua nas camadas superiores (até a **camada 7 - Aplicação**). Funciona como um **proxy**, intermediando a comunicação (não há conexão direta) e inspecionando o **conteúdo** dos dados (*payload*) para identificar ameaças avançadas, como malwares ou ataques específicos de protocolo.
- **Aprofundamento/Complemento:** O Firewall de Aplicação é considerado superior em segurança por realizar uma **inspeção profunda de pacotes (DPI)**. Um **NGFW** combina essa inspeção de aplicação com outras funções, como Prevenção de Intrusão (IPS) e filtragem de conteúdo, sendo crucial para proteger aplicações modernas.
- **Exemplo Prático:** Se um atacante tentar enviar código malicioso (*SQL Injection*) para um site, o Firewall de Pacotes veria apenas tráfego HTTP/HTTPS na porta 80/443 e permitiria. O **Firewall de Aplicação** reconheceria o padrão malicioso dentro do conteúdo do pacote e o bloquearia antes que chegasse ao servidor web.
    - **Link de Vídeo 1:** Conheça os Tipos de Firewall e suas diferenças
    - **Link de Vídeo 2:** O que é WAF e firewall? Firewall de rede e aplicativos web

Referência do Slide: Slide 08 - WAF (Web Application Firewall)

- **Definição:** O **WAF** (Web Application Firewall) é um tipo especializado de *Firewall de Aplicação* projetado especificamente para proteger **aplicações web** (tráfego HTTP/HTTPS) contra ataques direcionados. Ele protege contra vulnerabilidades comuns do OWASP Top 10, como *SQL Injection*, *Cross-Site Scripting (XSS)* e *Cross-Site Request Forgery (CSRF)*.
- **Aprofundamento/Complemento:** O WAF atua como um **proxy reverso** posicionado entre os usuários externos e o servidor web. Ele inspeciona cada requisição e resposta HTTP/HTTPS, aplicando regras de segurança para filtrar ou bloquear tráfego malicioso que visa explorar falhas de programação.
- **Exemplo Prático:** Ao lidar com a coleta e tratamento de dados pessoais (exigência da LGPD), um portal de e-commerce utiliza um WAF para garantir que nenhuma tentativa de injeção de código ou exploração de falhas em formulários de cadastro ou pagamento chegue ao servidor da aplicação.
    - **Link de Vídeo 1:** Cloudflare WAF (Referência da aula)
    - **Link de Vídeo 2:** O que é WAF?

Referência do Slide: Slide 10 - DMZ (Zona Desmilitarizada)

- **Definição:** A **DMZ** (Demilitarized Zone) é uma sub-rede física ou lógica que funciona como uma **zona de amortecimento** ou perímetro de segurança entre a rede local (LAN) interna e a Internet. É o local de hospedagem dos servidores que precisam ser acessados publicamente (ex: Servidores Web, FTP, E-mail).
- **Aprofundamento/Complemento:** A DMZ deve ser protegida por uma arquitetura de **dois Firewalls** (ou um *Firewall* com múltiplas interfaces) para criar isolamento máximo. O tráfego de entrada da Internet só pode ir para a DMZ; o tráfego da DMZ para a LAN interna deve ser rigorosamente inspecionado e restrito. Se um atacante comprometer um servidor na DMZ, a rede interna permanece protegida por uma camada adicional.

- **Exemplo Prático:** Uma instituição financeira coloca seu *site* público e seu servidor de e-mail na DMZ. Seu banco de dados de clientes, que contém dados pessoais sensíveis, está na rede interna (LAN). Se o *site* for invadido, o atacante precisará de uma segunda exploração para penetrar o *Firewall* interno e acessar o banco de dados.
    - **Link de Vídeo 1:** [DMZ] O que é uma DMZ? Zona DESMILITARIZADA em redes informáticas
    - **Link de Vídeo 2:** DMZ Explained in 3 minutes

Semana 27 - Aula 2

Tópico Principal da Aula: Implementação Prática de Segurança

Subtítulo/Tema Específico: Preparando o Ambiente de Virtualização

Código da aula: [SIS]ANO1C2B4S27A2

Objetivos da Aula:

- **Configurar** um ambiente de **Máquinas Virtuais (VMs)** que simule uma arquitetura de rede WAN, LAN e DMZ.
- **Conectar** corretamente as interfaces de rede das VMs aos ambientes de rede virtual para garantir o isolamento.

Recursos Adicionais (Sugestão, pode ser adaptado):

- Software de virtualização (VirtualBox ou VMware);
- Imagens de sistemas operacionais para servidor *Firewall* (Ex: pfSense) e hosts (Ex: Windows/Linux).

Exposição do Conteúdo:

Referência do Slide: Slide 06 - Preparação do Ambiente com VMs

- **Definição:** A preparação consiste na instalação e configuração de VMs que irão simular os papéis de *Firewall* (o sistema de segurança, ex: pfSense), a rede externa (*Internet/WAN*), a rede interna (*LAN*) e a **Zona Desmilitarizada (*DMZ*)**. Isso permite testar a segurança em um ambiente controlado.
- **Aprofundamento/Complemento:** A virtualização é uma ferramenta didática e profissional fundamental, pois permite a criação de ambientes complexos e replicáveis. No contexto de segurança, evita-se a exposição da rede real a riscos durante a configuração e teste das regras de tráfego.
- **Exemplo Prático:** Para o laboratório, cria-se uma VM com pfSense, uma VM Cliente (na LAN) e uma VM Servidor Web (na DMZ), sendo o pfSense o ponto central de controle do tráfego entre todas as redes virtuais.
    - **Link de Vídeo 1:** ALURA. Segurança de rede firewall... 01 Preparando o ambiente (Referência da aula)
    - **Link de Vídeo 2:** Laboratório com DMZ e Rede Interna no VirtualBox

Referência do Slide: Slide 08 - Configuração de Adaptadores de Rede (WAN, LAN, DMZ)

- **Definição:** A arquitetura de DMZ exige que o *Firewall* possua **múltiplas interfaces de rede** virtuais, cada uma conectada a uma sub-rede lógica diferente.
    - **WAN:** Interface conectada à Internet (simulada por *NAT* ou *Bridge*).
    - **LAN:** Interface conectada à rede interna confiável.
    - **DMZ:** Interface conectada à zona desmilitarizada, isolada das outras duas.
- **Aprofundamento/Complemento:** No VirtualBox, as interfaces LAN e DMZ devem ser configuradas como **Rede Interna**, usando nomes diferentes para criar os segmentos isolados (ex: `Rede_LAN` e `Rede_DMZ`). Essa separação lógica é o que garante que as regras de *Firewall* possam ser aplicadas para isolar o tráfego.
- **Exemplo Prático:** O técnico associa o **Adaptador 1** da VM pfSense à WAN, o **Adaptador 2** à Rede Interna `Rede_LAN` (que terá a VM Cliente) e o **Adaptador 3** à Rede Interna `Rede_DMZ` (que terá a VM Servidor Web).
    - **Link de Vídeo 1:** COMO CONFIGURAR a Interface DMZ (Demilitarized Zone) no pfSENSE PLUS+ 23.01
    - **Link de Vídeo 2:** PfSense: Criando uma DMZ / Para que serve uma DMZ?

Semana 27 - Aula 3

Tópico Principal da Aula: Configuração de Regras de Segurança no pfSense

Subtítulo/Tema Específico: Gerenciando o Firewall e Políticas de Acesso

Código da aula: [SIS]ANO1C2B4S27A3

Objetivos da Aula:

- **Acessar** a interface administrativa do pfSense e **mapear** as interfaces de rede.
- **Implementar** regras de **bloqueio geral** e **políticas de permissão** em diferentes interfaces.

Recursos Adicionais (Sugestão, pode ser adaptado):

- Máquina Virtual pfSense configurada (Aula 2);
- VMs Cliente e Servidor para teste de conectividade.

Exposição do Conteúdo:

Referência do Slide: Slide 06 - Acesso ao pfSense e Mapeamento de Interfaces

- **Definição:** O **pfSense** é um *Firewall* e roteador de código aberto baseado no sistema FreeBSD, popular por sua robustez e interface web de fácil gerenciamento. O acesso inicial é feito por meio da interface de linha de comando (*console*) e a configuração avançada é feita pela **interface web (GUI)** de uma máquina cliente na mesma rede LAN.
- **Aprofundamento/Complemento:** Após o *boot* e a configuração inicial no console, a interface web é acessada pelo IP da interface LAN do pfSense (ex: `https://192.168.1.1`). É fundamental, ao iniciar, verificar se as interfaces WAN, LAN e DMZ (se criada) foram corretamente identificadas e mapeadas pelo sistema

operacional para que as regras de segurança possam ser aplicadas de forma precisa.

- **Exemplo Prático:** De uma VM Cliente na rede LAN, o aluno digita o IP de LAN do pfSense no navegador para acessar o painel, onde irá confirmar se os adaptadores de rede configurados na Aula 2 (WAN, LAN, DMZ) estão operacionais e com os endereços IP corretos.
    - **Link de Vídeo 1:** ALURA. Segurança de rede firewall... 03 Acessando pfSense (Referência da aula)
    - **Link de Vídeo 2:** Como instalar e configurar o pfSense - Curso Completo

Referência do Slide: Slide 08 - Criação de Regras de Segurança (Block e Pass)

- **Definição:** As regras de *Firewall* no pfSense são as instruções que definem o fluxo de tráfego. Elas são aplicadas por interface e processadas de **cima para baixo (Top-Down)**. A primeira regra que coincide com o tráfego é aplicada, e o processamento é interrompido (**First Match**). Ao final da lista, existe uma regra implícita de **"negar tudo" (Implicit Deny)**.
- **Aprofundamento/Complemento:** Para a segurança máxima exigida pela LGPD, a estratégia deve ser **"o que não é explicitamente permitido é bloqueado"**. As regras de *Block* específicas (negação) devem ser colocadas no topo da lista, antes de regras mais amplas de *Pass* (permissão), para garantir que as negações tenham prioridade.
- **Exemplo Prático:** Para proteger a rede interna, o técnico cria a seguinte regra na interface DMZ:
    - **Ação:** Block
    - **Protocolo:** Any
    - **Origem:** DMZ Subnet
    - **Destino:** LAN Subnet
    - Essa regra impede que um invasor na DMZ consiga fazer qualquer tipo de varredura ou conexão direta com a rede LAN.
    - **Link de Vídeo 1:** Curso gratuito - pfSenseCORE - Aula 13 - Regras de Firewall no pfSense
    - **Link de Vídeo 2:** Firewall PfSense - Aprendendo Rules- Jeito Fácil