Trabalho 3 - Implementação de um Firewall

H. de M. O. Lima – 211055281, L. P. Torres – 222011623, and M. N. Miyata – 180126890

I. Introdução

O presente trabalho tem como objetivo a implementação de um firewall utilizando o `iptables` em um ambiente Linux. O firewall será configurado para controlar o tráfego de rede, permitindo ou bloqueando conexões com base em regras específicas.

No ambiente experimental, utilizaremos três máquinas virtuais: uma atuando como roteador/firewall, outra como cliente interno e a terceira como servidor interno. Em seguida, detalharemos as regras implementadas no firewall, a metodologia utilizada para testar sua eficácia e a análise dos resultados obtidos.

II. Fundamentação Téorica

Um firewall é um sistema de segurança de rede que monitora e controla o tráfego de entrada e saída com base em regras de segurança predefinidas. Ele atua como uma barreira entre redes confiáveis e não confiáveis, protegendo os sistemas internos contra acessos não autorizados e ameaças externas.

No Linux, o `iptables` é uma ferramenta amplamente utilizada para configurar firewalls. Ele permite a criação de regras que definem como o tráfego deve ser tratado, seja permitindo, bloqueando ou redirecionando pacotes de dados.

III. Ambiente Experimental

Como mencionado anteriormente, o ambiente experimental consiste em três máquinas virtuais: Roteador/Firewall, Cliente Interno e Servidor Interno. A máquina Roteador/Firewall está configurada para atuar como o ponto central de controle do tráfego de rede entre o Cliente Interno e o Servidor Interno. Além disso, todos foram configurados com endereços IP estáticos para garantir a comunicação adequada entre eles.

IV. Roteador/Firewall

Os scripts de configuração do firewall estão contidos em três arquivos principais: `00_enable_routing.sh`, `01_setup_firewall.sh` e `02_cleanup_firewall.sh`. A máquina virtual é um Debian sem interface gráfica, configurada com dois adaptadores de rede: um em modo “Rede Interna” (conectado ao Cliente e Servidor Internos) e outro em modo “NAT” (conectado à Internet). Os detalhes de configuração do firewall são apresentados nas próximas subseções.

A. Roteamento e NAT

O script `00_enable_routing.sh` ativa o encaminhamento de pacotes IP no sistema. Três variáveis principais são definidas: `WAN_IF` (interface de rede conectada à Internet), `LAN_IF` (interface de rede conectada à rede interna) e `LAN_IP` (endereço IP da interface LAN). A seguir, o script configura o endereço IP da interface LAN, ativa o encaminhamento de pacotes e configura o NAT (Network Address Translation) para permitir que os dispositivos na rede interna acessem a Internet através do roteador/firewall.

```bash
#!/bin/bash
# Habilita roteamento e NAT de forma persistente.

# Interface de saída para a internet, conectada ao provedor
WAN_IF="${WAN_IF:-enp0s3}"
# Interface de rede interna, utilizada pelos clientes para se conectar ao roteador
LAN_IF="${LAN_IF:-enp0s8}"
# Endereço IP da rede interna (LAN)
LAN_IP="${LAN_IP:-192.168.50.1/24}"

echo "[+] Ativando roteamento IPv4..."
sysctl -w net.ipv4.ip_forward=1
sed -i 's/^#\?net.ipv4.ip_forward.*/net.ipv4.ip_forward=1/' /etc/sysctl.conf

echo "[+] Configurando IP da LAN..."
ip addr add $LAN_IP dev $LAN_IF
ip link set $LAN_IF up

echo "[+] Limpando regras antigas..."
iptables -t nat -F

echo "[+] Ativando NAT (masquerade) na interface $WAN_IF..."
iptables -t nat -A POSTROUTING -o $WAN_IF -j MASQUERADE

echo "✓[] Roteamento e NAT configurados."
```

B. Regras do Firewall

O script `01_setup_firewall.sh` é responsável por configurar as regras do firewall utilizando o `iptables`. As cadeias de entrada (INPUT), encaminhamento (FORWARD) e saída (OUTPUT) são configuradas com políticas padrão seguras, bloqueando todo o tráfego por padrão. Em seguida, regras específicas são adicionadas para permitir o tráfego necessário e bloquear conexões indesejadas:

INPUT: Permite o tráfego de loopback, conexões estabelecidas e acesso ao servidor web na porta 8000.

No entanto, o tráfego ICMP (ping) é permitido apenas para a rede interna.

```
echo "[+] INPUT: Permitir tráfego de loopback"
iptables -A INPUT -i lo -j ACCEPT

echo "[+] INPUT: Permitir conexões estabelecidas"
iptables -A INPUT -m conntrack --ctstate ESTABLISHED,
    RELATED -j ACCEPT

echo "[+] INPUT: Permitir acesso ao servidor web (
    porta 8000)"
iptables -A INPUT -s $REDE_INTERNA -p tcp --dport
    8000 -m state --state NEW -j ACCEPT

echo "[+] INPUT: Permitir Ping (ICMP) da rede interna
    "
iptables -A INPUT -s $REDE_INTERNA -p icmp --icmp-
    type echo-request -j ACCEPT
```

FORWARD: Permite conexões estabelecidas, bloqueia DNS para redes sociais específicas (Facebook e TikTok) utilizando correspondência de strings, permite DNS de saída (UDP e TCP), permite HTTP e HTTPS de saída, e gerencia o tráfego ICMP (ping) de forma controlada.

```
echo "[+] FORWARD: Permitir conexões estabelecidas"
iptables -A FORWARD -m conntrack --ctstate
    ESTABLISHED,RELATED -j ACCEPT

echo "[+] FORWARD: Bloqueando DNS para redes sociais
    (String Match)"
iptables -A FORWARD -s $REDE_INTERNA -p udp --dport
    53 -m string --string "facebook" --algo bm -j
    REJECT
iptables -A FORWARD -s $REDE_INTERNA -p udp --dport
    53 -m string --string "tiktok" --algo bm -j
    REJECT

echo "[+] FORWARD: Permitir DNS (UDP e TCP) de saída
    (Geral)"
iptables -A FORWARD -s $REDE_INTERNA -p udp --dport
    53 -m state --state NEW -j ACCEPT
iptables -A FORWARD -s $REDE_INTERNA -p tcp --dport
    53 -m state --state NEW -j ACCEPT

echo "[+] FORWARD: Permitir HTTP e HTTPS de saída"
iptables -A FORWARD -s $REDE_INTERNA -p tcp --dport
    80 -m state --state NEW -j ACCEPT
iptables -A FORWARD -s $REDE_INTERNA -p tcp --dport
    443 -m state --state NEW -j ACCEPT

echo "[+] FORWARD: ICMP (Ping) gerenciado"
iptables -A FORWARD -s $REDE_INTERNA -d
    $SERVIDOR_INTERNO -p icmp --icmp-type echo-
    request -j ACCEPT
iptables -A FORWARD -s $REDE_INTERNA -p icmp --icmp-
    type echo-request -j REJECT --reject-with icmp-
    host-prohibited
```

OUTPUT: Aceita todo o tráfego de saída sem restrições. Essa escolha visa garantir que o firewall não interfira nas conexões iniciadas pela própria máquina roteadora/firewall, permitindo que ela se comunique livremente com outros dispositivos na rede ou na Internet.