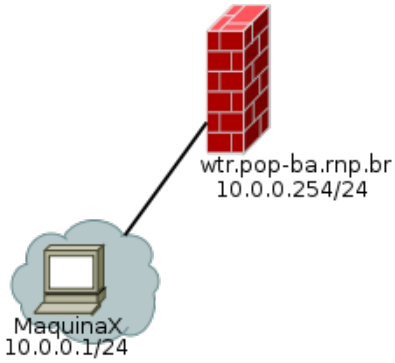
I WTR do POP-BA

I Workshop de Tecnologias de Rede
Ponto de Presença da RNP na Bahia
Instrutor: Italo Valcy
Monitor: Ibirisol Fontes

Prática 02: Construindo firewalls no Linux com IPTables



Este laboratório visa apresentar aos alunos os passos para configuração de um Firewall filtro de pacotes em uma rede local usando o IPTables/Netfilter. A figura acima ilustra a topologia lógica para configuração do ambiente. Nessa figura, a máquina ***MaquinaX*** representa a estação de trabalho do aluno, enquanto que ***wtr.pop-ba.rnp.br*** representa uma máquina virtual que funcionará como o firewall da rede local.
Obs.: Substitua o ***X*** abaixo por um identificador único fornecido pelo instrutor (valor natural de 0 à 255).

Objetivo da Prática

O objetivo da configuração de nosso firewall é atender aos seguintes requisitos:
- Deve ser permitido executar testes de conectividade da rede interna (10.X.0.0/24) para o firewall via ferramenta ping (Protocolo ICMP tipos echo-request e echo-reply).
- Deve ser permitido acessar o firewall via HTTP (porta 80/TCP) e HTTPS (porta 443/TCP) a partir da rede interna (10.X.0.0/24)
- Deve-se fazer logging das tentativas de IP Spoofing na rede interna
- Nada mais deve ser permitido

Parte 01: Configurações iniciais de rede

Obs.: Caso já tenha realizado esta etapa, pule para a etapa seguinte.

Para configurar a rede na máquina ***MaquinaX***, inicie o gerenciador de configurações de rede do Windows e edite a interface de rede física da máquina, seção do *Protocolo TCP/IP versão 4 (TCP/IPv4)*, e adicione as seguintes configurações:
- Usar o seguinte endereço IP:

- Endereço IP: ***10.X.0.1***
- Máscara de sub-rede: ***255.255.255.0***
- Gateway padrão: ***10.X.0.254***
- Servidor DNS preferencial: ***8.8.8.8***

Adicionalmente, edite o arquivo `c:\WINDOWS\system32\drivers\etc\hosts` e acrescente o seguinte (substitua o X pelo valor apropriado):
10.X.0.254 www.exemplo.pop-ba.rnp.br

Inicie a máquina virtual ***wtr.pop-ba.rnp.br*** e edite as configurações de rede do sistema:

sed -i 's/10.0.0./10.X.0./g' /etc/network/interfaces
/etc/init.d/networking restart

Parte 02: Configuração do firewall

Passos para configuração (os comandos a seguir devem ser executados na máquina ***wtr.pop-ba.rnp.br*** a menos que diga-se explicitamente o contrário):
- Habilitando o encaminhamento entre interfaces:

sysctl net.ipv4.ip_forward=1

- Definindo a política padrão. Com exceção das regras listas acima, todos as outras tentativas de conexão devem ser bloqueadas pelo firewall. Para tal definiremos a política padrão como sendo DROP.

iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

Na máquina ***MaquinaX***, tente acessar o firewall (10.X.0.254) via HTTP/HTTPS e verificar a conectividade com o ***ping***. Qual o resultado?

- Liberando testes de conectividade das máquinas da rede interna para o o firewall (substitua o valor de X pelo fornecido pelo instrutor):

iptables -A INPUT -i eth1 -p icmp --icmp-type echo-request -s 10.X.0.0/24 -j ACCEPT
iptables -A OUTPUT -o eth1 -p icmp --icmp-type echo-reply -d 10.X.0.0/24 -j ACCEPT

Na máquina ***MaquinaX***, verifique novamente a conectividade com o firewall (10.X.0.254) via ***ping***.

- Liberando acesso via HTTP (80/TCP) e HTTPS (443/TCP) das máquinas da rede interna para o o firewall (substitua o valor de X pelo fornecido pelo instrutor):

iptables -A INPUT -i eth1 -p tcp --dport 80 -s 10.X.0.0/24 -j ACCEPT
iptables -A OUTPUT -o eth1 -p tcp --sport 80 -d 10.X.0.0/24 -j ACCEPT
iptables -A INPUT -i eth1 -p tcp --dport 443 -s 10.X.0.0/24 -j ACCEPT
iptables -A OUTPUT -o eth1 -p tcp --sport 443 -d 10.X.0.0/24 -j ACCEPT

Na máquina ***MaquinaX***, tente acessar novamente o firewall (www.exemplo.pop-ba.rnp.br) via HTTP/HTTPS.

Apoio:
RNP UFBA CENTRO DE PROCESSAMENTO DE DADOS UFBA extreme networks D-Link Building Networks for People

- Habilitando logging das tentativas de IP Spoofing na interface da rede interna (substitua o valor de X pelo fornecido pelo instrutor):

iptables -A INPUT -i eth1 ! -s 10.X.0.0/24 -j LOG --log-prefix 'IP-Spoofing '
iptables -A FORWARD -i eth1 ! -s 10.X.0.0/24 -j LOG --log-prefix 'IP-Spoofing '

Experimente modificar o endereço IP da máquina ***MaquinaX*** (por exemplo, para 172.16.X.1) e executar um ***ping*** para outro endereço da mesma rede (por exemplo, 172.16.X.254). Observe no arquivo de log do IPTables as mensagens que são exibidas (veja em */var/log/kern.log*). Devem ser exibidas mensagens como:

Sep 17 19:31:42 wtr kernel: [31090.837791] ***IP-Spoofing IN=eth0*** *OUT=eth0* ***SRC=172.16.X.1 DST=172.16.X.254*** *LEN=60 TOS=0x00 PREC=0x00 TTL=127 ID=1030 PROTO=ICMP TYPE=8 CODE=0 ID=1 SEQ=130*

Parte 03: Usando o módulo state do IPTables para armazenar o estado da conexão

Na configuração acima (*Parte 01*) foi possível observar que para cada regra adicionada era necessário adicionar uma outra regra para o pacote de resposta. Nessa parte veremos como usar módulo *state* do IPTables para tratar esse estado das conexões. Para tal usaremos os mesmos objetivos da *Parte 01*.

Passos para configuração (os comandos a seguir devem ser executados na máquina ***wtr.pop-ba.rnp.br*** a menos que diga-se explicitamente o contrário):

- Refaça a *Parte 01* para voltar a configuração de rede da máquina ***wtr.pop-ba.rnp.br*** ao original.

- Removendo as regras anteriores:

iptables -F

- Definindo o tratamento de estados das conexões. O objetivo é permitir os pacotes de conexões já estabelecidas ou outras conexões relacionadas à conexões já existentes e barrar pacotes cujo estado seja desconhecido. Para tal execute os seguintes comandos:

iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -m state --state INVALID -j DROP
iptables -A OUTPUT -m state --state INVALID -j DROP
iptables -A FORWARD -m state --state INVALID -j DROP

- Liberando testes de conectividade das máquinas da rede interna para o firewall (substitua o valor de X pelo fornecido pelo instrutor):

iptables -A INPUT -i eth1 -p icmp --icmp-type echo-request -s 10.X.0.0/24 -j ACCEPT

Na máquina ***MaquinaX***, verifique novamente a conectividade com o firewall (10.X.0.254) via ***ping***.

- Liberando acesso via HTTP (80/TCP) e HTTPS (443/TCP) das máquinas da rede interna para o o firewall (substitua o valor de X pelo fornecido pelo instrutor):

iptables -A INPUT -i eth1 -p tcp -m multiport --dports 80,443 -s 10.X.0.0/24 -j ACCEPT

Na máquina ***MaquinaX***, tente acessar novamente o firewall (10.X.0.254) via HTTP/HTTPS.

Apoio:


Parte 04: Aplicando as regras de firewall na inicialização do sistema

O leitor deve observar que toda a configuração do IPTables foi realizada via comandos do shell. Isso sugere que podemos construir um script com tais comandos e configurar o sistema para executá-lo na inicialização. Utilizaremos essa tática para ativar nosso firewall na inicialização.

- Para tal, crie o arquivo ***/etc/init.d/firewall*** com o seguinte conteúdo (para evitar o trabalho de digitar o conteúdo abaixo, foi disponibilizado um arquivo similar ao abaixo em `/root/arquivos/firewall`. Copie-o para o /etc/init.d – ***cp /root/arquivos/firewall /etc/init.d/*** - e substitua o X pelo valor apropriado):

```
#!/bin/bash

iptables -F

case $1 in
start|restart)
   sysctl net.ipv4.ip_forward=1

   iptables -P INPUT   DROP
   iptables -P OUTPUT  DROP
   iptables -P FORWARD DROP

   iptables -A INPUT   -m state --state RELATED,ESTABLISHED -j ACCEPT
   iptables -A OUTPUT  -m state --state RELATED,ESTABLISHED -j ACCEPT
   iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
   iptables -A INPUT   -m state --state INVALID -j DROP
   iptables -A OUTPUT  -m state --state INVALID -j DROP
   iptables -A FORWARD -m state --state INVALID -j DROP

   iptables -A INPUT -i eth1 -p icmp --icmp-type echo-request -s 10.X.0.0/24 -j ACCEPT
   iptables -A INPUT -i eth1 -p tcp -m multiport --dports 80,443 -s 10.X.0.0/24 -j ACCEPT
   ;;

stop)
   rmmod iptable_filter
   rmmod ip_tables
   ;;

*)
   echo "Invalid option $1"
   echo "Usage: $0 start|stop|restart"
   ;;

esac
```

- Adicione permissão de execução ao arquivo e adicione-o à inicialização

chmod +x /etc/init.d/firewall

update-rc.d firewall defaults

- Reinicie a máquina virtual e verifique se as regras de firewall foram carregadas com sucesso.

Boa prática! Em caso de dúvidas, não hesite em consultar o instrutor.

Apoio:

RNP UFBA