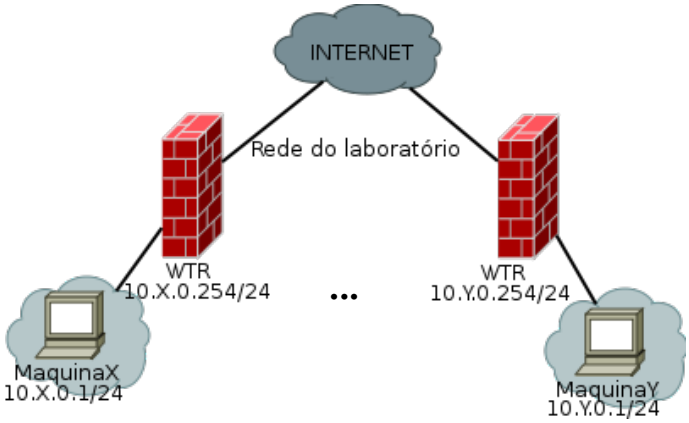
Prática 03: Configurando NAT Masquerade



Este laboratório visa apresentar aos alunos os passos para configuração de um Firewall para traduções NAT 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*** 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 a partir de qualquer rede 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 de qualquer rede
- Deve-se permitir que as máquinas da rede interna (10.X.0.0/24) acessem a Internet (DNS (53/UDP) e HTTP/HTTPS (80 e 443/TCP).
- Na máquina ***MaquinaX***, temos uma aplicação executando na porta 135/TCP que deve ser acessível da Internet (DNAT) (de fato, a porta 135/TCP foi escolhida pois já está aberta na maioria das máquinas Windows, porém poderia ser qualquer outra aplicação).
- 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*** a menos que diga-se explicitamente o contrário):

- Habilitando o encaminhamento entre interfaces:

```
sysctl net.ipv4.ip_forward=1
```

- Primeiramente vamos limpar as tabelas Filter e NAT do IPTables para evitar que regras anteriores influenciem na configuração:

```
iptables -F
iptables -t nat -F
rmmod iptable_filter
rmmod iptable_nat
rmmod ip_tables
```

- Definindo a política padrão da tabela Filter. 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
```

Apoio:

- 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 para o o firewall:

iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

- Liberando acesso via HTTP (80/TCP) e HTTPS (443/TCP) para o firewall:

iptables -A INPUT -p tcp -m multiport --dports 80,443 -j ACCEPT

Na máquina ***MaquinaX***, tente acessar novamente o firewall (10.X.0.254) via HTTP/HTTPS. Peça para que algum colega tente acessar seu firewall via HTTP/HTTPS, forneceça o endereço IP global da interface eth0 do firewall para ele (para saber esse endereço execute: ***ifconfig eth0***)

- Liberando acesso à Internet para as máquinas da rede interna (10.X.0.0/24) via HTTP/HTTPS (80 e 443/TCP) e DNS (53/UDP):

sysctl net.ipv4.ip_forward=1
iptables -A FORWARD -i eth1 -o eth0 -s 10.X.0.0/24 -p tcp -m multiport --dports 80,443 -j ACCEPT
iptables -A FORWARD -i eth1 -o eth0 -s 10.X.0.0/24 -p udp --dport 53 -j ACCEPT

Na máquina ***MaquinaX***, tente acessar o site http://www.wtr.pop-ba.rnp.br. Qual foi o resultado? Qual a justificativa para esse comportamento?

- Habilite o mascaramento dos endereços da rede interna no firewall:

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

Na máquina ***MaquinaX***, tente novamente acessar o site http://www.wtr.pop-ba.rnp.br.

- Devemos configurar um NAT do tipo DNAT para encaminhar as requisições que chegam ao firewall na porta 135/TCP para a máquina ***MaquinaX*** e permitir tais conexões na tabela de filtros (substitua *IPDOFW* pelo endereço global da interface eth0 no firewall. Para saber esse endereço execute: ***ifconfig eth0***).

iptables -t nat -A PREROUTING -d IPDOFW -p tcp --dport 135 -j DNAT --to 10.X.0.1
iptables -A FORWARD -d 10.X.0.1 -p tcp --dport 135 -j ACCEPT

- Aguarde um outro colega finalizar essa etapa e tente conectar-se no servidor dele. Para isso inicie o prompt de comandos do Windows e digite o seguinte comando (substitua *IPREMOTO* pelo endereço IP do firewall do colega na interface *eth0*). Para finalizar o comando tecle CTRL+]

telnet IPREMOTO 135

Apoio:

Para verificar se a conexão foi efetivada com sucesso, verifique na máquina remota as conexões estabelecidas (no prompt do Windows, digite: ***netstat -an -p tcp***)

- Verifique se os objetivos previstos na seção *Objetivos da Prática* foram cumpridos com sucesso.

- OPCIONAL: altere o script de firewall da prática anterior (`/etc/init.d/firewall`) para acrescentar as traduções de NAT especificadas acima.

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

Apoio: