O que você precisa saber sobre Iptables na certificação LPI nível 1

Introdução ao Firewall

O Firewall é um programa que como objetivo proteger a máquina contra acessos e tráfego indesejados em sua rede e proteger serviços que estejam rodando em seu servidor.

No kernel 2.4, foi introduzido o firewall iptables (também chamado de **netfilter**), que trabalha com o conceito de chains para tratar os pacotes de acordo com a situação dos mesmos, baseado na implementação de políticas.

Conceituamos as políticas em **básicas**, **exceções** e **controles**.

As **chains** a serem utilizadas serão: **INPUT** (tudo que entra no firewall), **OUTPUT** (tudo que sai do firewall) e **FORWARD** (tudo que passa pelo firewall), **PREROUTING**(tudo que entra no firewall para sofrer **NAT**), **POSTROUTING**(tudo que sai do firewall para sofrer **NAT**).

Teremos aqui uma pequena introdução em como implementar as regras no nosso firewall.

Tabelas do iptables:

filter	É a tabela padrão, ou seja, ela é usada quando na regra a tabela não é especificada. É utilizada quando há tráfego de dados normal.
nat	Quando é necessário fazer a passagem de dados de uma rede privada para a internet usamos a tabela nat.
mangle	É utilizada para fazer alterações em pacotes.

Adotaremos como política básica NEGAR (DROP) qualquer acesso ao firewall

```
# iptables -P INPUT DROP
# iptables -P OUTPUT DROP
# iptables -P FORWARD DROP
```

Neste momento, nossa máquina está totalmente protegida, porém está isolada na rede. Por isso é que agora nós adotaremos políticas de exceções para as situações em que deixaremos nosso firewall acessível.

PRIMEIRA EXCEÇÃO - "pingar" qualquer host, porém não responder ping para ninguém.

```
# iptables -A OUTPUT -p 1 --icmp-type 8 -s <meu ip> -d 0/0 -j ACCEPT
```

O que acontece nesta regra é o seguinte: todo pacote ICMP (protocolo de código 1 - vide **/etc/protocols**) do tipo 8 (echo request - solicitação de ping) que sair do meu firewall, tiver como origem o meu firewall (definido no parâmetro <meu ip>, onde coloco o IP do meu firewall) e como destino qualquer interface (definido por 0/0), ele irá aceitar (ACCEPT).

```
# iptables -A INPUT -p 1 --icmp-type 0 -s 0/0 -d <meu ip> -j ACCEPT
```

Ou seja, todo pacote ICMP, do tipo 0 (echo reply - resposta de ping) que entrar no meu firewall, tiver como origem qualquer interface e como destino o IP do meu firewall, ele irá aceitar.

OBS: até esse momento, nós ainda não conseguimos "pingar" nossa própria interface local (lo - loopback). Seria interessante então habilitarmos a entrada e saída de pacotes via interface lo.

iptables -A INPUT -d 127.0.0.1 -j ACCEPT

Tudo o que entrar no firewall com destino a interface local (loopback), ele irá aceitar. Agora sim eu consigo pingar a minha própria máquina!

SEGUNDA EXCEÇÃO - firewall como servidor ssh

Agora iremos fazer uma regra permitindo acesso ssh apenas de uma máquina para o nosso servidor. Por exemplo, poderíamos liberar conexão via ssh apenas para a máquina do administrador, para que ele possa fazer suporte remoto.

O cliente se conecta no servidor pela porta 22, sendo que o cliente recebe a resposta em uma porta alta (entre 1024 e 65535) aleatoriamente.

iptables -A INPUT -p 6 -s <ip do cliente> --sport 1024:65535 -d <ip do firewall> --dport 22 -j ACCEPT

Tudo o que entrar no firewall, sendo pacote TCP (código 6), tendo como origem o ip do cliente em uma porta alta (1024:65535), com destino ao ip do firewall na porta 22, ele irá aceitar.

iptables -A OUTPUT -p 6 -s <ip do firewall> --sport 22 -d <ip do cliente> --dport 1024:65535 -j ACCEPT

Aqui ele fará a regra inversa, ou seja, tudo o que sair do firewall, sendo pacote TCP, tendo como origem o ip do firewall na porta 22, com destino ao ip do cliente em uma porta alta, ele irá aceitar.

TERCEIRA EXCEÇÃO - Firewall como cliente http (para acesso em um source do APT, por exemplo).

A próxima exceção será permitir com que o firewall possa se conectar a um source APT, para poder baixar pacotes via apt-get. Tomaremos aqui como exemplo um source que se utiliza do protocolo http.

iptables -A OUTPUT -p 6 -s <ip do firewall> --sport 1024:65535 -d <ip do servidor APT> --dport 80 -j ACCEPT

Tudo o que sair do firewall, sendo pacote TCP, tendo como origem o ip do nosso firewall por uma porta alta, com destino ao ip do servidor APT na porta 80, ele irá aceitar.

iptables -A INPUT -p 6 -s <ip do servidor APT> --sport 80 -d <ip do firewall> --dport 1024:65535 -j ACCEPT

Agora tudo o que entrar no firewall, sendo pacote TCP, tendo como origem o ip do servidor APT na porta 80, com destino ao nosso firewall em uma porta alta, ele irá aceitar.

OBS: se eu possuir um source via ftp, eu só devo mudar na regra do firewall a porta no servidor de 80 para 21.

Podemos ter várias exceções configuradas no nosso firewall, para diversos protocolos, sendo que a diferença são os serviços disponíveis a serem acessados. A lógica de aplicação das chains de INPUT e OUTPUT vão, portanto, seguir a mesma lógica, por exemplo, para um acesso telnet, smtp, https, etc.

Para saber a(s) porta(s) e os respectivos protocolos que os serviços utilizam, basta consultar os arquivos **/etc/services** e **/etc/protocols**, respectivamente.

Depois de vistas as exceções, precisamos implementar controle sobre alguns eventos indesejados em nossa rede, pois mesmo o firewall barrando tais eventos eu posso geral logs para posterior auditoria no que ocorrer.

Eu quero logar informações sobre tentativas de acesso na porta 23 do meu firewall (conexões através do telnet):

iptables -A INPUT -p 6 -s 0/0 --sport 1024:65535 -d <ip do firewall> --dport 23 -j LOG –log-prefix "intruso"

Tudo que entrar no firewall, sendo pacote TCP, tendo como origem qualquer IP em uma porta alta, com destino a interface do meu firewall na porta 23, ele irá logar essa informação, acrescentando ao final da linha do log um prefixo específico (a palavra "intruso) para identificar o log de tentativa de acesso nesta porta.

Da mesma maneira, eu posso implementar controles, adequados e necessários ao meu ambiente, em portas que eu queira controlar tais eventos para posterior auditoria do administrador.

Visualizando as regras configuradas em nosso firewall:
iptables -nL | more

Todas as regras configuradas até o momento estão em memória, ou seja, quando eu reiniciar minha máquina elas serão perdidas. Então vamos salvá-las para um arquivo:

iptables-save > /root/regras

Se eu precisar restaurá-las em memória:
iptables-restore < /root/regras

Limpando as regras da memória
iptables -F
iptables -n -L

Dicas:

Compartilhando a Internet com Iptables:

modprobe iptable_nat
echo "1" >**/proc/sys/net/ipv4/ip_forward**

Atenção!

Procedimento equivalente ao #echo "1" >/proc/sys/net/ipv4/ip_forward:
Editar o arquivo **/etc/sysctl.conf**

De:
net.ipv4.ip_forward=0
Para:
net.ipv4.ip_forward=1

Isso ativa o roteamento na inicialização do Linux.

iptables -t nat -A POSTROUTING -s <ip/mascara da sua rede> -o ppp0 -j MASQUERADE

Exemplo:
iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -o ppp0 -j MASQUERADE

Para listar suas regras de nat:
iptables -t nat -L

Para limpar as regras de firewall (flush):
iptables -F