Introdução ao IP Tables

1) Introdução:

O **netfilter** é um conjunto de mecanismos para filtragem e manipulação de pacotes implementados diretamente no kernel do linux a partir da versão 2.4.x. Os mecanismos do netfilter são selecionados através de três tabelas:

FILTER: utilizada para filtrar pacotes
MANGLE: utilizada para ações de marcação e manipulação de pacotes
NAT: utilizada para as ações de tradução de endereços **(NAT e NAPT)**

O iptables corresponde aos mecanismos utilizados para organizar as regras utilizadas pelo netfilter. O iptables utiliza o conceito de chains para indicar para quais pacotes uma determinada regra deve ser aplicada. As chains utilizadas pelo mecanismo de filtragem de pacotes são:

INPUT: a regras se referem aos pacotes que entram por uma interface
OUTPUT: as regras se referem ao que sai por uma interface
FORWARD: as regras se aplicam aos pacotes que serão roteados, isto é, ao pacotes que não são destinados ao próprio computador.

A sintaxe para manipulação das regras do iptables segue a estrutura. Se a tabela não for especificada, assume-se a tabela FILTER:

iptables -AID CHAIN N -t TABLE MATCH -j TARGET

A opção –A é usada para acrescentar uma regra ao fim da chain. A opção –I N é utilizada para inserir uma regra na posição N. E a opção –D N para apagar a regra da posição N. As seguintes opções complementam uma regra:

opção (short)	opção (long)	parâmetro	significado
-s	--src	X.X.X.X/Y	endereço de origem do pacote
-d	--dst	X.X.X.X/Y	endereço de destino do pacote
-i	--in-interface	interface	interface pela qual o pacote chegou
-o	--out-interface	interface	interface pela qual o pacote vai sair
-p	--protocol	tcp, udp, icmp	protocolo do pacote
--sport	--source-port	porta[:porta]	porta ou intervalo de portas de origem
--dport	--destination-port	porta[:porta]	porta ou intervalo de portas de destino

-	--icmp-type	tipo/código	pacote icmp (iptables -p icmp -h para info
-	--match	-	habilita o modo de opções extendido

Com a opção --p PROTOCOL ou --match, pode-se usar adicionalmente as seguintes opções:

opção	parâmetro	significado
--limit	X/time	limita a média de matchs. Time pode ser /second, /minute, /hour ou /day
--limit-burst	X	Número máximo inicial de matchs. Esse valor é "recarregado" em 1 a cada intervalo de tempo em que o limite não foi alcançado, até o valor especificado. Utilize essa opção para permitir rajadas.
--mask	X	casa com um pacote "marcado" com o valor X.
--state	NEW,ESTABLISHED, RELATED, INVALID	casa com o estado de uma conexão.
--tcp-flags	MASK FLAGS	Examina as flags "MASK" e casa com FLAGS. Exemplo: SYN,ACK ACK = examina SYN e ACK e casa com pacotes com SYN desligado e ACK ligado.
--tos	name	casa com o campo Type of Service. User iptables -m tos -h para ver os nomes/valores
--ttl	valor	casa com o valor do campo ttl do pacote

Para negar uma opção, utiliza-se !. Por exemplo: -s !192.168.0.1/32

As seguintes ações podem ser executadas na tabela FILTER:

Alvo	opções	significado
ACCEPT	-	Aceita um pacote
REJECT	-	Rejeita um pacote
REJECT	--reject-with type	Rejeita um pacote e envia um pacote ICMP type para a origem
DROP	-	Descarta silencionsamente o pacote
LOG	-	Loga os headers do pacote
LOG	--log-level X	Loga utilizando o nível X (veja o arquivo syslog.conf)

LOG	--log-prefix	permite acrescentar um prefixo de 29 letras. É útil para identificar o tipo pacote/regra

Exercício 1: Crie regras bloqueando o envio de mensagem ICMP Echo (ping) para o seu Servidor (VM)

a)Verifique as regras instaladas no iptables

b) Se houver alguma regra, remova (flush).

c) Caso não estejam, mude a política default de todas as chain para ACCEPT

d) Crie uma regra bloqueando o recebimento de ICMP, e em seguida efetue um ping do ambiente windows para o endereço IP da máquina virtual. Identifique o endereço IP da máquina virtual digitando ifconfig.

e) Limpe a regra anterior, e crie uma nova regra de bloqueio, mas agora usando ao ação REJECT ao invés de DROP. Repita o ping o windows para máquina virtual e observe o resultado.

f) Verfique se a máquina virtual consegue pingar o ambiente Windows. Em seguida, altere a regra do iptables da máquina virtual, e verifique a possibilidade de enviar ping nos dois sentidos.