

Ramiro Henrique - RA: 1747444

Atividade Prática I

2) iptables -A INPUT -j DROP
iptables -A FORWARD -j DROP
iptables -A OUTPUT -j DROP

3) iptables -A INPUT -p ALL -j LOG --log-prefix "INPUT"
iptables -A OUTPUT -p ALL -j LOG --log-prefix "OUTPUT"
iptables -A FORWARD -p ALL -j LOG --log-prefix "FORWARD"

4) O comando possibilita que pacotes sejam recebidos pelo protocolo ssh.
iptables -A INPUT -p tcp --dport 22 -j ACCEPT

5) Todos os protocolos TCP/IP estão autorizados a receber pacotes de qualquer endereço e coloca a regra como a primeira da lista INPUT.
iptables -I INPUT 1 -p tcp -j ACCEPT

6) iptables -D INPUT 2

1) O comando cria uma regra no começo da lista INPUT, que permite pacotes serem recebidos caso eles tenham iniciado uma nova conexão.
iptables -I INPUT 1 -m state --state NEW -j ACCEPT

2) iptables -A INPUT -j DROP
Pelo fato do comando estar abaixo na lista INPUT, o primeiro comando nega seus efeitos.

3) Permite que pacotes sejam recebidos pelo protocolo ssh que não tenham criado um nova conexão.
iptables -I INPUT 2 -p tcp --dport 22 -m state --state RELATED, ESTABLISHED -j ACCEPT