Escola de Educação Profissional Senai Porto Alegre

Técnico em Redes De Computadores

Módulo IV

Professor: Maurício Rodrigues Cerqueira.

Morfologia das Regras iptables

Iptables –t *tabela* –A *chain origem* –p *protocolo destino* –j *ação*

Tabela:

- Filter (INPUT, OUTPUT, FORWARD)
- Nat (PREROUTING, POSTROUTING)
- Mangle(usado em todas as chais para EMERGÊNCIAS)

CHAINs:

- INPUT – Pacotes com destino ao Firewall
- OUTPUT – Pacotes Originados no Firewall
- FORWARD – Passando pelo firewall
- PREROUTING – Antes do Roteamento (Redirecionar para a rede interna)
- POSTROUTING – Após o roteamento (Realizar NAT)

Origem:

- -s IP/REDE (EX.: -s 192.168.0.0/24 – Rede de origem ou –s 192.168.0.5 – Host de Origem)
- -i INTERFACE (EX.: -i eth0 – Pacotes vindos da eth0)

Protocolo:

- -p tcp --dport PORTA_DE_DESTINO_DO_SERVIÇO (EX.: -p tcp --dport 80 – Acesso ao serviço HTTP)
- -p udp --dport PORTA_ DE_DESTINO_DO_SERVIÇO (EX.: -p udp --dport 53 – Acesso ao serviço DNS)
- -p tcp --sport PORTA_DE_ORIGEM_DE_ORIGEM_DO_SERVIÇO (EX.: -p tcp --sport 80 – Resposta do Serviço HTTP)
- -p udp --sport PORTA_DE_ORIGEM _DO_SERVIÇO (EX.: -p udp --sport 53 – Resposta do Serviço DNS)

Destino:

- -d IP/REDE (EX.: -d 192.168.0.0/24 – Rede de destino ou –d 192.168.0.5 – Host de Destino)
- -o INTERFACE (EX.: -o eth0 – Pacotes saindo na eth0)

Ação:

- MASQUERADE (Realizar nat)
- ACCEPT (Permitir a trafego)
- DROP (Descartar o trafego)
- REJECT (Descartar o trafego e enviar resposta de negação)
- REDIRECT --to-port NOVA_PORTA (EX.: *REDIRECT --to-port 3128* – Redirecionar para o proxy local)
- DNAT --to-destination IP:PORTA (EX.: *DNAT --to-destination 192.168.0.10:80* – Redireciona o trafego para o host 192.168.0.10 na porta 80)