INSTITUTO FEDERAL DO NORTE DE MINAS GERAIS - CAMPUS JANUÁRIA

IPTables

O que é e para que serve?

- Iptables é uma ferramenta de firewall para sistemas Linux que permite controlar o tráfego de rede, decidindo quais conexões são permitidas e quais são bloqueadas.

- Essas regras podem ser configuradas para permitir certos tipos de tráfego enquanto bloqueiam outras atividades maliciosas.

Sintaxe Básica

1. Para verificar as regras já existentes no IPTables:

```
sudo iptables -L
```

2. Limpando todas as regras de todas as cadeias nas tabelas:

```
sudo iptables -F
```

Sintaxe Básica

3. Para excluir uma todas as regras de uma cadeia:

```
sudo iptables -F <chain>
```

-F: Indica que queremos limpar todas as regras da cadeia especificada.

Chains IPTables

- Chains ou “Cadeias” são grupos dentro das tabelas e formam um conjunto de regras para avaliar um pacote, de maneira sequencial (de cima para baixo, listadas no terminal).

- O pacote passa por todas as regras e para na primeira regra segundo suas especificações.

- Se não houver correspondência do pacote para nenhuma regra dentro da cadeia, a política padrão será consultada.

```
iptables -P <chain> <ação>
```

Chains IPTables

- INPUT – A regra será executada em pacotes de entrada
- OUTPUT – A regra será executada para pacotes gerados por um processo local
- FORWARD – A regra será executada aos pacotes de rede roteados através do servidor (inclusive entre interfaces de rede do próprio servidor)
- PREROUTING – A regra será executada aos pacotes quando eles chegam e antes do roteamento. Usado para DNAT (Destination NAT)
- POSTROUTING – A regra será executada no pacotes após o roteamento. Usado para SNAT (Source NAT)

Tables

O IPTables trabalha com diferentes tabelas, cada uma com finalidades distintas:

- Filter: padrão, usada para filtrar pacotes (INPUT, OUTPUT, FORWARD).
- Nat: usada para tradução de endereços (DNAT, SNAT – PREROUTING, POSTROUTING).
- Mangle: modifica pacotes (TTL, marcações).
- Raw: permite manipulação antes do rastreamento de conexões.

Sintaxe Básica

4. Adicionar uma regra para bloquear tráfego de saída:

```
sudo iptables -A <chain> -o eth0 -p <protocolo> --dport <porta destino> -j <ação>
```

- **-A**: Adiciona a regra à cadeia especificada.
- **-o**: Especifica a interface de rede de saída para onde o tráfego está sendo enviado.
- **-p**: Especifica o protocolo do pacote (neste caso, UDP).
- **--dport**: Especifica a porta de destino do pacote.
- **-j**: Indica a ação a ser tomada se a regra for correspondida (neste caso, DROP).

Sintaxe Básica

Ações definidas com o -j ou -jump na escrita da regra, são as ações a serem tomadas pelo iptables caso o match aconteça: As principais são:

- REJECT - Rejeita o pacote
- ACCEPT - Aceita o pacote
- DROP - Descarta o pacote (não informa a origem da ação tomada sobre a conexão)
- LOG - Gera log referente ao pacote

Sintaxe Básica

5. Remover uma regra específica:

```
sudo iptables -D INPUT 3
```

- **-D**: Indica que estamos excluindo uma regra.
- **INPUT**: Especifica a cadeia da qual a regra será removida.
- **3**: É o número da regra que será excluída. Você pode ver os números das regras usando o comando iptables -L numerado.

INSTITUTO FEDERAL DO NORTE DE MINAS GERAIS - CAMPUS JANUÁRIA

Obrigada!

ADMINISTRAÇÃO DE REDES