Parte I:
Relatório iptables

Segurança e Confiabilidade
2021/2022
Trabalho 2

Henrique Barata fc54387

Hugo Marques fc54400

João Vidal fc54467

Todos os comandos (a negrito) foram executados no terminal do servidor MServer, pela ordem que são mostrados

Começamos por fazer os primeiros dois comandos:

- **sudo iptables -P OUTPUT DROP**
- **sudo iptables -P INPUT DROP**

Assim conseguimos ignorar qualquer pedido feito a esta máquina.

O tráfego do dispositivo de loopback não deve ser filtrado e relacionado com uma ligação já estabelecida também deve ser aceite, acrescentando assim estes comandos indicados no enunciado:

- **sudo iptables –A INPUT –i lo –j ACCEPT**
- **sudo iptables –A OUTPUT –o lo –j ACCEPT**
- **sudo iptables –A INPUT –m state –-state ESTABLISHED,RELATED –j ACCEPT**
- **sudo iptables –A OUTPUT –m state –-state ESTABLISHED,RELATED –j ACCEPT**

Criamos agora as diferentes regras para cada um das maquinas pedidas para estas conseguirem estabelecer ligação com a maquina MServer.

Temos de aceitar tanto o output com o input para os diferentes ips das maquinas desejadas(DC1, DC2 , DC3, Storage, Falua, Gateway, Proxy, Luna):

- **sudo iptables -A INPUT -s 10.121.52.14 -j ACCEPT**
- **sudo iptables -A OUTPUT -d 10.121.52.14 -j ACCEPT**
- **sudo iptables -A INPUT -s 10.121.52.15 -j ACCEPT**
- **sudo iptables -A OUTPUT -d 10.121.52.15 -j ACCEPT**
- **sudo iptables -A INPUT -s 10.121.52.16 -j ACCEPT**
- **sudo iptables -A OUTPUT -d 10.121.52.16 -j ACCEPT**
- **sudo iptables -A INPUT -s 10.121.72.23 -j ACCEPT**
- **sudo iptables -A OUTPUT -d 10.121.72.23 -j ACCEPT**
- **sudo iptables -A INPUT -s 10.101.85.138 -j ACCEPT**
- **sudo iptables -A OUTPUT -d 10.101.85.138 -j ACCEPT**
- **sudo iptables -A INPUT -s 10.101.204.1 -j ACCEPT**
- **sudo iptables -A OUTPUT -d 10.101.204.1 -j ACCEPT**
- **sudo iptables -A INPUT -s 10.101.85.137 -j ACCEPT**
- **sudo iptables -A OUTPUT -d 10.101.85.137 -j ACCEPT**
- **sudo iptables -A INPUT -s 10.101.85.24 -j ACCEPT**
- **sudo iptables -A OUTPUT -d 10.101.85.24 -j ACCEPT**

Foram adicionadas as seguintes regras para cada uma das restrições:

(i) a máquina responde a pings apenas com origem na máquina gcc (10.101.151.5)

- **sudo iptables -A INPUT -p icmp -s 10.101.151.5 -j ACCEPT**
- **sudo iptables -A OUTPUT -p icmp -d 10.101.151.5 -j ACCEPT**

(ii) aceita ligações de clientes de qualquer origem para o servidor Trokos

- **sudo iptables -A INPUT -p tcp -- dport 45678 -m state –state NEW -j ACCEPT**
- **sudo iptables -A INPUT -p tcp -- dport 45678 -m state --state ESTABLISHED,RELATED -j ACCEPT**

(iii) aceita ligações ssh para o servidor Trokos, apenas de máquinas da sua sub-rede local(com máscara 255.255.254.0)

- **sudo iptables -A INPUT -p tcp -- dport 22 -s 10.101.204.0/23 -m state –state NEW -j ACCEPT**
- **sudo iptables -A INPUT -p tcp -- dport 22 -s 10.101.204.0/23 -m state --state ESTABLISHED,RELATED -j ACCEPT**

Criar um limite de 3 pings por segundo as maquinas da sub-rede

- **sudo iptables -A OUTPUT -p icmp -d 10.101.204.0/23 -m limit --limit 3/s -j ACCEPT**

O MServer apenas responde a pings com origem na maquina gcc, deixando as outras maquinas sem resposta.

O MClient acede ao server, conseguindo conectar o TrokosClient

O Outsider, não tem operações permitidas