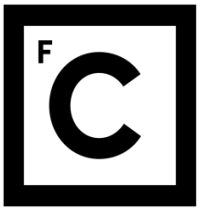

Ciências ULisboa

Faculdade de Ciências da Universidade de Lisboa

Segurança e Confiabilidade

2017/2018

Relatório de Iptables da Fase 3

Grupo 09

Diogo Pereira, n.º 47888

José Águas, n.º 47804

Simão Ferreira, n.º 47827

Disclamer: Utilizamos como máquina de testes uma máquina do DI do laboratório 1.3.12 com IP 10.101.149.5.

Regras Iptables

$ sudo /sbin/iptables -A OUTPUT -j ACCEPT -d 10.121.52.14,10.121.52.15,10.101.52.16,10.121.72.23,10.101.85.6,10.101.85.138,10.101.85.18,10.101.148.1,10.101.85.137
$ sudo /sbin/iptables -A INPUT -j ACCEPT -s 10.121.52.14,10.121.52.15,10.101.52.16,10.121.72.23,10.101.85.6,10.101.85.138,10.101.85.18,10.101.148.1,10.101.85.137

Estas duas regras são executadas para impedir o bloqueio do PC uma vez que os computadores do DI dependem destes servidores para o seu funcionamento. Enunciamos a seguir os endereços:

Os IP's 10.121.52.14, 10.121.52.15, 10.101.52.16 são para permitir ligação ao DCs.

O IP 10.121.72.23 é para o storage.

Os IP's 10.101.85.6 e 10.101.85.138 são para permitir a ligação ao Iate/Falua.

O IP 10.101.85.18 serve para a ligação do Nemo.

O IP 10.101.148.1 serve para a ligação do Gateway.

E por fim o IP 10.101.85.137 serve para a ligação à proxy.

Utilizamos as flags INPUT e OUTPUT para permitir a receção e o envio da máquina servidora até estes IP's que são necessários ao funcionamento de um computador do DI. Utilizamos a opção -A para fazer append a lista de regras e fazemos -j ACCEPT para aceitar estas ligações.

$ sudo /sbin/iptables -A INPUT -i lo -j ACCEPT
$ sudo /sbin/iptables -A OUTPUT -o lo -j ACCEPT

Estas duas regras foram executados para permitir o tráfego com ele próprio, de novo OUTPUT e INPUT para envio e receção, ACCEPT para aceitar, e as flags necessárias antes de cada argumento. O -i significa Input Interface e o -o Output Interface, o lo é a interface Local Loopback. Com isto permitimos a conexão com a própria máquina.

$ sudo /sbin/iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$ sudo /sbin/iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

Regras que aceitam tráfego relacionado com uma ligação já estabelecida (já constavam do enunciado). "-m state" é para aplicar a regra a um determinado estado o "--state ESTABLISHED,RELATED" é para dizer que o estado é de uma já estabelecida. O resto dos parâmetros já foram explicados em cima.

$ sudo /sbin/iptables -A INPUT -s 10.101.151.5 -p icmp --icmp-type 8 -j ACCEPT
$ sudo /sbin/iptables -A OUTPUT -d 10.101.151.5 -p icmp --icmp-type 0 -j ACCEPT

Estas regras servem para permitir tráfego de e para o servidor GCC com IP 10.101.151.5 utilizando para esse efeito o INPUT e OUTPUT. Como usamos o protocolo de Internet Control Message Protocol especificamos também o type com 0 que significa reply ou seja estamos a responder (OUTPUT) com respostas. Do lado contrário utilizamos o type a 8 para requests.

$ sudo /sbin/iptables -A INPUT -p tcp --dport 23232 -j ACCEPT

Esta regra permite receber pedidos de ligações TCP para o porto do servidor (23232), pedidos esses que são dos clientes. O -p é a flag para identificar o protocolo, neste caso TCP, o "--dport" é o porto destino, neste caso o 23232.

$ sudo /sbin/iptables -A INPUT -p tcp -s 10.101.149.52/255.255.254.0 --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
$ sudo /sbin/iptables -A OUTPUT -p tcp --sport 22 -m conntrack --ctstate ESTABLISHED -j ACCEPT

Estas regras servem para aceitar pedidos TCP da sub-rede do computador em que foram feitos os testes, aceitamos o estado de novas ligações e ligações estabelecidas. Para a resposta da máquina servidora utilizamos a mesma o porto 22 do TCP e aceitamos ligações estabelecidas também.

$ sudo /sbin/iptables -A INPUT -s 10.101.149.52/255.255.254.0 -p icmp --icmp-type 0 -j ACCEPT
$ sudo /sbin/iptables -A OUTPUT -d 10.101.149.52/255.255.254.0 -p icmp --icmp-type 8 -j ACCEPT

Estas últimas regras foram executadas com o intuito de permitir à máquina servidora fazer ping às máquinas da mesma mascara (255.2555.254.0) para isto utilizamos o IP source e destination como o IP da máquina servidora com a máscara pretendida. O protocolo utilizado é o ICMP em que na regra do Input (receber) permitimos receber replys, no Output(enviar) permitimos enviar requests.

$ sudo /sbin/iptables -P INPUT DROP
$ sudo /sbin/iptables -P OUTPUT DROP

Com estas regras rejeitamos todas as outras ligações, que não aceitamos em cima, sem enviar um aviso de rejeição. O parâmetro -P serve para definir a policy, neste caso usamos o INPUT(receber) e OUTPUT(enviar) e usamos o DROP para rejeitar sem avisar.

Métodos de Teste e Observações

Criámos um bash script onde estão todas as regras e quando corremos este script as regras são colocadas na tabela de regras.

Nesta parte dos teste executamos um script com todas as regras do iptables mencionadas acima e utilizamos também o comando ping com IP's ou da máquina servidora ou dos computadores do mesmo laboratório. Utilizamos um PC pessoal para realizarmos testes com o servidor gcc.

Também executamos a nossa aplicação para observar se esta continua a funcionar de outras máquinas para a máquina servidora.