Firewall

Robin Bruynseels
R0658408

Bachelor in Toegepaste Informatica

Academiejaar 2019-2020
Campus Geel, Kleinhoefstraat 4, BE-2440 Geel

LID VAN ASSOCIATIE KU LEUVEN

THOMAS MORE

1) Ruleset opzetten firewall

1.1) Opdracht

As a system engineer your expertise is asked to create a firewall ruleset for a hosting server.

The server is provided with the following services: Apache, ProFTPd and bind9. Please, do not allow zonetransfers. Also protect the server against ping flooding. The server is not allowed to make outgoing connections, except for the installation of security updates.

Present your result through a git commit on Gitlab or Github

1.2) Ruleset

We gaan beginnen met commando's op te geven die gaan zorgen dat alle updates en upgrades gedaan zijn.

- Sudo apt-get update
- Sudo apt-get upgrade

hierna gaan we de volgende services installeren. Apache, ProFTPd en bind9. Dit doen we door volgende commando's uit te voeren.

- *Sudo apt install proftpd*
- *Sudo apt install apache2*
- *Sudo apt install bind9*

Je kan altijd checken dat deze versie kloppen door de parameter '-v' mee te geven. Vb. Apache2 -v

Als we de opdracht lezen wordt het duidelijk wat ze juist vragen. Zo vragen ze dat om geen zone transfers toe te laten. We gaan dus de tcp op poort 53 niet door laten en udp wel doorlaten. Dit kunnen we doen met volgende commando's:

- Iptables -A INPUT -p udp –dport 53 -j ACCEPT
- Iptables -A INPUT -p tcp –dport 53 -J DROP

We gaan de server protecten tegen ping flooding (ICMP). Hiervoor gaan we volgende commando's gebruiken :

- Iptables -t filter -A INPUT -p icmp –icmp-type echo-request -m limit –limit 5/minute -j ACCEPT
- Iptables -t filter -A INPUT -p icmp -J DROP
- Iptables -t filter -A OUTPUT -p icmp –icmp-type echo-reply -j ACCEPT

Deze gaan ervoor zorgen dat we enkel 5 echo requests per minuut gaan ontvangen. Daarna worden deze gedropped.

Ten slotte moesten we wel security updates toelaten. Hier heb ik gerbuik gemaakt van een established of related:

Iptables -A INPUT -m state –state ESTABISHED,RELATED -p tcp –dport http -j ACCEPT

Dit wordt dan het resultaat:

```
robin@robin-VirtualBox:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
DROP       tcp  --  anywhere             anywhere             tcp dpt:domain
ACCEPT     icmp --  anywhere             anywhere             icmp echo-reques
 limit: avg 5/min burst 5
DROP       icmp --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             state RELATED,ES
ABLISHED tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere             icmp echo-reply
robin@robin-VirtualBox:~$
```

```
robin@robin-VirtualBox:~$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A INPUT -p udp -m udp --dport 53 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 53 -j DROP
-A INPUT -p icmp -m icmp --icmp-type 8 -m limit --limit 5/min -j ACCEPT
-A INPUT -p icmp -j DROP
-A INPUT -p tcp -m state --state RELATED,ESTABLISHED -m tcp --dport 80 -j ACCEP
T
-A OUTPUT -p icmp -m icmp --icmp-type 0 -j ACCEPT
robin@robin-VirtualBox:~$
```