TDDD17 lab 2

Gustav Ahlberg gusah849
Claire Vacherot clava401

February 18, 2013

Exercise 6

6-1

```
iptables -A INPUT -p tcp –dport 22 -i eth0 -j ACCEPT
```

6-2

```
iptables -A OUTPUT -p udp –dport 53 -d 10.0.0.0/24
```

6-3

```
iptables -A INPUT -m iprange –src-range 10.0.0.1-10.0.0.6
```

6-4

```
iptables -N TEST
iptables -A TEST -m iprange –src-range 10.0.0.1-10.0.0.6
iptables -A TEST -j RETURN
```

Exercise 7

7-1

If we have for example an IDS or IPS we want to forward all incoming network traffic to that process before it is sent to the destination process.

7-2

```
iptables -P INPUT DROP
iptables -A INPUT -j LOG
```

Exercise 8

8-1

When using stateful matching the firewall needs to save the state of each connection and save packets to be able to figure out which packets are related. If we only inspect the header flags we only need to examine one packet.

8-2

If for example we establish a FTP connection to a FTP-server. If we then try to download a file a new connection between my computer and the server is established. That new data connection will have the state RELATED because it is related to my existing connection to the server.

If a server responds to a UDP packet with a ICMP packet that response is considered to be RELATED to the initial UDP packet.

8-3

In UDP a connection is never established in the same sense as in TCP. So it is impossible to determine if a packet that is being sent is part of a previous request by just examining just one packet. But if we use connection tracking we can figure out if the incoming request is part of a previous ESTABLISHED connection.

8-4

If we use a idlescan we can scan the target in the perspective of the zombie host. So if we find a zombie host that is trusted by the target we can still scan the target for open ports.

Exercise 9

9-1

```
iptables -t nat -A POSTROUTING -s 10.0.0.0/8 ! -d 10.0.0.0/8 -j SNAT –to-source 192.0.2.1
```

9-2

IP addresses are carried in FTP packet are readable and of variable length. As NAT requires to rewrite them, it can change the length of the TCP packet, and SEQ and ACK numbers have to be changed.

Exercise 11

General policy

1

```
iptables -P FORWARD DROP
iptables -I FORWARD -i eth0 -o eth1 -m state –state ESTABLISHED,RELATED -j ACCEPT
iptables -I FORWARD -i eth0 -o eth2 -m state –state ESTABLISHED,RELATED -j ACCEPT
```

2

```
iptables -I FORWARD -i eth1 -o eth0 -m state –state ESTABLISHED,RELATED -j ACCEPT
iptables -I FORWARD -i eth1 -o eth2 -m state –state ESTABLISHED,RELATED -j ACCEPT
```

3

```
iptables -I FORWARD -i eth2 -o eth0 -j ACCEPT
iptables -I FORWARD -i eth2 -o eth1 -j ACCEPT
```

DNS

4

```
iptables -I FORWARD -i eth0 -p tcp -d 10.19.11.12 –dport 53 -j ACCEPT
iptables -I FORWARD -i eth0 -p udp -d 10.19.11.12 –dport 53 -j ACCEPT
```

5

```
iptables -I FORWARD -i eth1 -p udp –dport 53 -d 10.19.11.142 -j ACCEPT
iptables -I FORWARD -i eth1 -p tcp –dport 53 -d 10.19.11.142 -j ACCEPT
```

6

This is taken care of by rule 2.

7

```
iptables -I FORWARD -i eth1 -p udp -s 10.19.11.12 –dport 53 -j ACCEPT
```

Mail

8

```
iptables -I FORWARD -i eth0 -p tcp -d 10.19.11.11 –dport 25 -j ACCEPT
```

9

```
iptables -I FORWARD -i eth1 -p tcp -s 10.19.11.11 -d 10.19.11.141 –dport 25 -j ACCEPT
```

10

Is taken care of by rule 3

11

```
iptables -I FORWARD -i eth2 -p tcp ! -s 10.19.11.141 –dport 25 -j DROP
iptables -I FORWARD -i eth2 -p tcp -d 10.19.11.141 –dport 25 -j ACCEPT
```

Web

12

```
iptables -I FORWARD -i eth0 -p tcp -d 10.19.11.10 –dport 443 -j ACCEPT
iptables -I FORWARD -i eth0 -p tcp -d 10.19.11.10 –dport 80 -j ACCEPT
```

Firewall

13

```
iptables -I INPUT -i lo -j ACCEPT
```

14

```
iptables -I INPUT -p udp -d 224.0.0.9 –dport 520 -j ACCEPT
```

15

```
iptables -A INPUT -i eth2 -p tcp –dport 22 -j ACCEPT
```

16

```
iptables -P INPUT DROP
```

Other

17

```
iptables -t nat -A POSTROUTING -o eth2 -d 10.19.11.0/24 -j SNAT –to-source 192.168.12.0-192.168.12.255
```

18

```
iptables -I FORWARD -i eth0 -o eth2 –match policy –pol ipsec –dir in -j ACCEPT
```

19

```
iptables -N ICMP_CHAIN
iptables -I FORWARD -p icmp -j ICMP_CHAIN
iptables -I ICMP_CHAIN -j DROP
iptables -I ICMP_CHAIN -p icmp –icmp-type 3 -j ACCEPT
iptables -I ICMP_CHAIN -p icmp –icmp-type 4 -j ACCEPT
iptables -I ICMP_CHAIN -p icmp –icmp-type 5 -j ACCEPT
iptables -I ICMP_CHAIN -p icmp –icmp-type 9 -j ACCEPT
```

20

```
iptables -N AS_LOG
iptables -I AS_LOG -j DROP
iptables -I AS_LOG -j LOG –log-level info –log-prefix "ADDRESS SPOOFING DETECTED"
iptables -I FORWARD -i eth2 -m iprange ! –src-range 10.19.11.129-10.19.11.255 -j AS_LOG
iptables -I FORWARD -i eth2 ! -s 192.168.12.0/24 -j AS_LOG
```

21

```
iptables -I FORWARD -i eth1 -m iprange ! –src-range 10.19.11.0-10.19.11.128 -j AS_LOG
```

22

```
iptables -I FORWARD -i eth0 -s 192.168.12.0/24 -j AS_LOG
iptables -I FORWARD -i eth0 -s 10.19.11.0/24 -j AS_LOG
```

23

Answered in question 20