

# TDDD17 lab 2

Gustav Ahlberg gusah849

Claire Vacherot clava401

February 5, 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.