CSIS 3230 Computer Networking Principles

Group Lab Report 10 – IP Packet filtering and firewalls

Names: Michael Chillemi | Harry Zhu | John Raven | Benigno Ledesma I

1. Kernel packet filtering defaults

List the name and policy of each rule chain

Chain INPUT,FOWARD,and OUTPUT. Each one has an ACCEPT policy

What do the policies indicate about restrictions placed on traffic to/from your PC?

There are currently no restrictions.

2. Filter by IP address and protocol

a) Describe the table entry for the new filtering rule.

There's is now a restriction on the IP address that we've provided and it rejects on icmp-port-unreachable

b) What message is displayed on the host attempting to `ping` when the `REJECT` action is used?

destination port unreachable

c) What are the **Type** and **Code** values for the `icmp` packets returned to the host being blocked (include the code numbers and explanatory text)?

Type 3, destination unreachable

☒ Hosts not being blocked are able to ping your host.

d) What message is displayed on the host attempting to `ping` when the `DROP` action is used?

```
5 packets transmitted, 0 received, 100% packet loss
```

e) What is different about the Wireshark traces when you `DROP` ping packets compared to when you `REJECT` them?

```
Instead of UNREACHABLE, it shows NO RESPONSE FOUND
```

f) Write the rule used to disable `ping` from all other computers on your LAN.

```
sudo iptables -A INPUT -s 192.168.4.1 -p icmp -j REJECT
```

What happens when a computer on another LAN pings you?

```
destination port unreachable
```

g) What message does the *sender* get when *outgoing* ping's are being blocked?

```
Operation not permitted
```

3. Filtering and logging

Log entries include information extracted from the packet headers.

a) What data was recorded in the log entries that identify them as an attempt to access a ***web server***?

```
MAC address, source IP, destination IP
```

b) ☒ Blocked host is not able to access web server

☒ Other hosts can still access web server

c) Does the current filtering rule also block `https` requests? Explain your answer.

```
Yes.
```

4. Filter by protocol and flags

a) The tcp flags info lists:
FLAGS BEING OBSERVED/FLAGS THAT SHOULD BE SET (=1)
Briefly describe how this rule prevents incoming TCP connections but allows outgoing TCP connections

Incoming connection are rejected using a TCP protocol, outgoing connections are dropped using an icmp protocol

b) Why is it still possible to ping the computer that is blocking incoming TCP connections?

It is not possible to ping the computer that is blocking the incoming TCP connections

c) Describe the response packets (ICMP) generated when another PC tries to connect from a web browser.

Retransmission packets are generated

d) Is the server able to connect to other hosts with `ftp` (or `www`)? Why?

Yes, because outgoing traffic is not blocked

e) Write the rule used to block all incoming connections except to your web server.

```
sudo iptables -A INPUT -p tcp --syn ! --dport 80 -j REJECT
```

f) What happens when a host tries to connect to the web server?

Able to connect

What happens when a host tries to connect with `ftp`?

Connection timed out

5. Switching policy

a) What happens when pinging *to* a host with INPUT policy set to DROP?

5 packets transmitted, 0 received, 100% packet loss

b) What happens when pinging *from* a host with INPUT policy set to DROP? Does this result seem to contradict what the packet capture shows? Explain what is happening.

Operation not permitted, no packets showing in packet capture

c) Write the rule that allows pings from hosts on your LAN.

```
sudo iptables -A INPUT -s 192.168.88.0/24 -p icmp -j ACCEPT
```

d) Explain why the current rule set prevents you from accessing a web site on another computer.

Because it is not accepting the "reply" (ACK)

6. Stateful firewalls

a) ☒ The stateful rule allows you to access the other web site

b) You can access a web page on another computer now, but why does the current rule set not allow another computer to access your web site?

Becasue the chain OUTPUT is set to DROP.

7. Experiment

Write the rules for the practice exercises. Note that each scenario can be accomplished with a single rule.

a)

```
sudo iptables -A INPUT -s 192.168.4.0/24 -p icmp -j ACCEPT
supo iptables -A INPUT 0s 192.168.4.0/24 -p tcp --dport 80 -j DROP
```

b)

```
sudo iptables -A OUTPUT -s 10.20.18.10 -j DROP
```