# Homework 4 – Linux Firewall

Daniel Hutchins – CIS 480-76

## Task 1. Find IP addresses

1. Find the IP address of the client and the firewall.
2. Show the addresses in screenshots.

Text

Description automatically generated

## Task 2. Nmap scan

1. Perform a nmap scan on the client for open ports on the server. Show the output in a screenshot.

Text

Description automatically generated

1. Run *wget* and report captured packets on wireshark in a screenshot. To capture packets for a new command, you need to stop/start capturing without exiting wireshark.

Graphical user interface, text, application

Description automatically generated

1. Run *ssh* and report captured packets on wireshark in a screenshot.

Graphical user interface, application

Description automatically generated

1. Run *telnet* and report captured packets on wireshark in a screenshot.

Table

Description automatically generated with medium confidence

## Task 3. Use iptables to limit traffic to the server

1. Show that ssh traffic is allowed. On the client, run ssh while capturing traffic on the firewall. Report these two activities in two screenshots. Explain how you know ssh traffic is allowed.

Graphical user interface, text, application

Description automatically generated



SSH is allowed as the capture showed the handshake that occurred in the first three packets.

1. Show that HTTP traffic is allowed. Report the same as you did for ssh traffic.

Text

Description automatically generated

Graphical user interface, application

Description automatically generated

HTTP traffic is going through on port 80 as the handshake occurs in the first three packets & the relevant HTTP packets are allowed (packets 4 and 14).

1. Show that telnet traffic is blocked. Report the same as you did for ssh traffic.

Text

Description automatically generatedGraphical user interface, text, application, email

Description automatically generated

When the client tries to access port 23 for Telnet, the incoming packets are blocked (as shown with the black/red packets in Wireshark.)

1. At the end, perform a nmap scan on the client for open ports on the server. Show the output in a screenshot.

Text

Description automatically generated

## Task 4. Open a new service port

1. Show that wizbang traffic is allowed. On the client, run wizbang while capturing traffic on the firewall. Report these two activities in two screenshots. Explain how you know wizbang traffic is allowed.

Text

Description automatically generated with medium confidence

Graphical user interface, text, application

Description automatically generated

Within the first few packets, the handshake for the Wizbang program is successful.

(SYN, SYN ACK, ACK)

1. At the end, perform a nmap scan on the client for open ports on the server. Show the output in a screenshot.

Text

Description automatically generated

**My rules used for this assignment. (Added lines 32-39)**

Text

Description automatically generated