Homework 4 – Linux Firewall

- This is an individual assignment and worth 20 points.
- The due date is Saturday, October 22, midnight.
- Please zoom in on the outputs.
- Use the accompanying output document to report your results.
- Follow the naming convention.
- YOU ARE NOT ALLOWED TO DO THIS DURING THE CLASS.

Overview

- The objective of this assignment is to create firewall rules on the firewall in Labtainer. The firewall rules are used to accept/reject traffic to the server.
- This learning objective is evaluated by examining the outputs captured in screenshots after performing the tasks.

Background on IPTABLES

- Overview of IPTABLES
  - https://www.booleanworld.com/depth-guide-iptables-linux-firewall/
- IPTABLES manual
  - https://linux.die.net/man/8/iptables

Tutorials on IPTABLES

- Tutorial 1
  - https://www.youtube.com/watch?v=vbhr4csDeI4&t=83s&ab_channel=XPSTECH
  - https://www.youtube.com/watch?v=H1WPwAjMXRo&t=474s&ab_channel=XPSTECH
- Tutorial 2
  - https://www.youtube.com/watch?v=eC8scXX1_1M

Tasks

- This assignment is based on the **Labtainer iptables2** lab manual.
- You need to execute commands with a superuser permission. For this, use *sudo <command>*. Alternatively, switch into a super user by tying *sudo su*.

Task 1. Find IP addresses

a) Find the IP address of the client and the firewall.
b) Show the addresses in screenshots.

Task 2. Nmap scan

a) Follow the instructions in sec 3.1.

b) Launch Wireshark on the firewall. After you launch it, do not exit. When you need to capture different traffic, just stop and start capturing. When you exit and relaunch, Wireshark may not be launched successfully. Reinstalling Wireshark does not work. In this case, you need to dump the labtainer VM and recreate.
c) Perform a nmap scan on the client for open ports on the server. Show the output in a screenshot.
d) 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.
e) Run *ssh* and report captured packets on wireshark in a screenshot.
f) Run *telnet* and report captured packets on wireshark in a screenshot.

Task 3. Use iptables to limit traffic to the server

a) Follow the instructions in sec 3.2 to prevent the firewall from forwarding any traffic to the server other than SSH and HTTP.
b) On the firewall, you will find an example script (example_fw.sh) to apply to answering questions for the tasks. Create a copy of the file and rename it as *cis-<last name>.sh*. For example, mine is *cis-im.sh*. Use the copied one to answer the questions.
c) To edit the script, use nano editor. If you are familiar with a different editor, feel free to use it. Type: *nano <filename>*.
d) 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.
e) Show that HTTP traffic is allowed. Report the same as you did for ssh traffic.
f) Show that telnet traffic is blocked. Report the same as you did for ssh traffic.
g) At the end, perform a nmap scan on the client for open ports on the server. Show the output in a screenshot.

Task 4. Open a new service port

a) Follow the instructions in sec 3.3. When you run wizbang, you need to add a few words. For example, type: *./wizbang Good Morning*.
b) Update the script to allow the new service.
c) 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.
d) At the end, perform a nmap scan on the client for open ports on the server. Show the output in a screenshot.