CAN304 Lab 8

Firewall – ufw

In this lab, students will learn firewall, in particular, the Ubuntu built-in firewall application terms ufw. With the experiment, students will learn how to use ufw to filter traffic.

Prerequisite

1. You have followed the previous lab for creating Ubuntu VM, and this lab needs 2 VMs
2. Install ufw on the Ubuntu VM by using this command-line: **apt-get install ufw**

1. Installing dependencies

1.1. Install ufw

1) sudo apt-get update
2) sudo apt-get install ufw

2. Firewall

2.1. A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules [1]. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet [2].

2.2. Firewall tools available on Ubuntu:

- iptables [3]
- ufw/gufw (we focus on using this firewall application)
- firewall builder
- etc.

3. Conduct the experiment

3.1. Step 1

Start two VMs, i.e., A and B, and they locate on the same network (e.g., both A and B use "NAT network" of Virtualbox). In my case, VM A uses IP address 10.0.2.9, and VM B uses IP address 10.0.2.4

3.2. Step 2

On VM A, open a terminal and create a simple http server by typing the command "**python3 -m http.server --bind 10.0.2.9 80**"

```
root@bitcoinattacker:/home/wfan# python3 -m http.server --bind 10.0.2.9 80
Serving HTTP on 10.0.2.9 port 80 (http://10.0.2.9:80/) ...
```

3.3. Step 3

On VM A, open a new terminal, and let's deny http traffic by using the ufw: "**ufw deny from 10.0.2.4 to 10.0.2.9 port 80**" and "**ufw enable**".

```
root@bitcoinattacker:/home/wfan# ufw deny from 10.0.2.4 to 10.0.2.9 port 80
Rules updated
root@bitcoinattacker:/home/wfan# ufw enable
Firewall is active and enabled on system startup
```

3.4. Step 4

On VM B, try this command again "**wget -o - 10.0.2.9**", what will you see?

```
root@controller1:/home/wfan# wget -o - 10.0.2.9
--2021-12-09 14:51:20--  http://10.0.2.9/
Connecting to 10.0.2.9:80...
```

3.5. Step 5

Go back to VM A, type the command "**ufw disable**" to stop the firewall.

```
root@bitcoinattacker:/home/wfan# ufw disable
Firewall stopped and disabled on system startup
```

Homework:

Follow the aforementioned lab steps, enable ufw on VM B, and then use nmap on VM A to scan VM B's http service to see if you can get any result.

Reference

[1] Boudriga, Noureddine (2010). Security of mobile communications. Boca Raton: CRC Press. pp. 32–33. ISBN 978-0849379420.

[2] Oppliger, Rolf (May 1997). "Internet Security: FIREWALLS and BEYOND". *Communications of the ACM*. 40 (5): 94. doi:10.1145/253769.253802. S2CID 15271915.

[3] https://www.netfilter.org/

[4] https://wiki.ubuntu.com/UncomplicatedFirewall

[5] http://fwbuilder.sourceforge.net/