Network Security - Assignment 5

Run the following commands in your virtual machine. Take screenshots of your output as you complete each task. Describe anything you find interesting or useful in each output. Answer the questions asked throughout. Add this to your GitHub repo and submit the repo link.

NOTE: If needed, to install a package in ubuntu, we can use Advanced Package Tools (APT). Use the following syntax to install a package: `sudo install apt packagename`

I. Enable UFW (Uncomplicated Firewall)

Default UFW Policies -

- Incoming: Denied (blocked) by default.
- Outgoing: Allowed by default.

1. Check the status of UFW. There is a good chance you don't have it installed or enabled yet: `sudo ufw status`
2. Before enabling UFW, you want to make sure your connection to ssh is allowed using the following command:
   - `sudo ufw allow 22/tcp`

- **Question**: If you are remotely accessing your server, why is it important to allow traffic through port 22 before enabling UFW?

3. Check the other ports that are open that you may need to allow specific connections (80, 443, etc). tuln below is for checking TCP, UDP, and Listening. n displays addresses in numeric form. Socket Statistics (ss) is a command line utility for checking network statistics.
   - `sudo ss -tuln`
   - If you see a port you are unsure of, you can check the specific service of that port using: `sudo lsof -i :portNumber`
4. Enable UFW: `sudo ufw enable`
5. Check the status now: sudo ufw status
6. Let's say your server is a web server. Which ports should be allowed through in UFW? Once you know, allow the port(s) access using the same command above.

7. Check the status using the verbose command. Any information that looks important or useful?

   - `sudo ufw status verbose`

8. Say you have a disgruntled ex employee who is known to wreck havoc. You want to block his ip address, 10.0.0.0, from your server using UFW. How would you do this? HINT: Check the UFW documentation: https://help.ubuntu.com/community/UFW

9. Say you want to allow 192.168.1.50 access to port 587. What is the command to allow this in UFW? What is port 587 typically used for? (Again, check documentaion).

10. Check that the rules were added by checking the status once more.

II. Enable UFW Logging

1. Before checking the logs, make sure that UFW logging is enabled. To enable logging, run: `sudo ufw logging on`

2. If you need more detailed or less verbose logs, you can change the logging level:

   - **low**: Minimal logging, mainly for blocked incoming packets.
   - **medium**: Includes blocked incoming packets with additional packet header details.
   - **high**: Includes all blocked packets and connection information.
   - **full**: Extensive logging of all UFW events.

   - Set the logging level to high: `sudo ufw logging high`

3. A typical UFW log entry might look like the following:

```
Oct  1 12:34:56 hostname kernel: [12345.67890] [UFW BLOCK] IN=eth0 OUT=
MAC=aa:bb:cc:dd:ee:ff SRC=192.168.1.100 DST=192.168.1.50 LEN=60 TOS=0x00
PREC=0x00 TTL=64 ID=54321 DF PROTO=TCP SPT=12345 DPT=80 WINDOW=14600 RES=0x00
SYN URGP=0
```

Let’s break this down:

- MAC: Source MAC address of the traffic - **MAC=aa:bb:cc:dd:ee:ff**
- SRC: Source IP address of the traffic - **SRC=192.168.1.100**
- DST: Destination IP address - **DST=192.168.1.50**

- SPT: Source port - **SPT=12345**
- DPT: Destination port - **DPT=80**
- PROTO: Protocol used (e.g., TCP, UDP) - **PROTO=TCP**
- [UFW BLOCK]: **Indicates that the packet was blocked by UFW.**
  - Why is this information useful to us?

4. The UFW logs are stored in `/var/log/ufw.log`. Use the following command to view your own logs in your VM: `sudo tail -f /var/log/ufw.log`
   - The `-f` options allows you to monitor the log in real time.
5. To filter specific entries, use the `grep` command:
   - For denied traffic: `sudo grep 'DENY' /var/log/ufw.log`
   - For allowed traffic: sudo grep 'ALLOW' /var/log/ufw.log
   - Is there any output for DENY? Why or why not?