**IT 5434 Network Security Fundamentals**

**Lab Assignment 7 (L7)**

**60 points**

**Due: 11:59 pm, Wednesday, October 19, 2018**

**Student name:**

**Last 4 of Eagle ID:**

**Read the following introduction about Ubuntu Linux firewalls. Complete the following tasks on Ubuntu Linux using Uncomplicated Firewall (ufw) and attach screenshot(s) for each task.**

The Linux kernel includes the **Netfilter** subsystem, which is used to manipulate or decide the fate of network traffic headed into or through your Linux. **All modern Linux firewall solutions** use this system for packet filtering.

The kernel’s packet filtering system would be of little use to administrators without a user space interface to manage it. This is the purpose of **iptables**. When a packet reaches your server, it will be handed off to the Netfilter subsystem for **acceptance**, **manipulation**, or **rejection** based on the **rules** supplied to it from user space via iptables. Thus, iptables is all you need to manage your firewall if you're familiar with it, but many frontends are available to simplify the task.

The default firewall configuration tool for **Ubuntu** is **ufw**. Developed to ease iptables firewall configuration, ufw provides a user friendly way to create an **IPv4** or **IPv6** host-based firewall. **ufw by default is initially disabled**. From the ufw man page: “ufw is not intended to provide complete firewall functionality via its command interface, but instead **provides an easy way to add or remove simple rules**.”

1. **ufw needs to be enabled before used. From a terminal (Shell) enter:** **“*sudo ufw enable”***

**Q: What did the terminal show after you entered this command? (provide screenshot, 4 points)**

**A:**

1. **Open port number 22: “*sudo ufw allow 22”***

**Q: What did the terminal show after you entered this command? (provide screenshot, 4 points)**

**A:**

**Q: What default protocol/service will this command allow? (5 points)**

**A:**

1. **Create a rule using a numbered format: “*sudo ufw insert 1 allow 80”, then answer the following question.***

**Q: What did the terminal show after you checked the firewall status using “*sudo ufw status*”? (show screenshot, 4 points)**

**A:**

1. **Close port 22 that was opened in step 2.**

**Q: Show the status of your firewall. (show screenshot and commands used, 5 points)**

**A:**

1. **Remove the rule that was created in step 4.**

**Q: Show the status of your firewall. (show screenshot and commands, 4 points)**

**A:**

1. **It is also possible to allow access from specific hosts or networks to a certain port.** **This command allows ssh (tcp traffic on port 22) access from host 192.168.0.2 to any IP address on this host: “*sudo ufw allow proto tcp from 192.168.0.2 to any port 22”***

**Q: Show the status of your firewall. (show screenshot, 5 points)**

**A:**

1. **Run the command: “sudo ufw allow proto tcp from 192.168.0.0/24 to any port 22”.**

**Q: What does the command try to do? (your answer must address the CIDR /24 and the corresponding range of IP addresses; check the command manual page and use Google if needed) (5 points)**

**A:**

**Q: Show firewall status using “sudo ufw status”? (show screenshot, 4 points)**

**A:**

1. **To view more details of the firewall status, use command “sudo ufw status verbose”**

**Q: Attach screenshot. (4 points)**

**A:**

1. **To view the numbered format: “*sudo ufw status numbered”***

**Q: Attach screenshot. (4 points)**

**A:**

1. **Q: If you want to run FTPS Service (e.g. FileZilla Server, which allows secure file transfers over open networks), what is/are the command(s) to set the ufw firewall rule that will allow FTPS requests coming from any IP address? Run your command(s) on terminal and show status of firewall. Note that FTPS may need more than one port to run properly [2]. (show screenshots and commands, 8 points)**

**A:**

1. **ufw can be disabled by running commend “*sudo ufw disable”*.**

**Q: Show firewall status? (show screenshot, 4 points)**

**A:**

**References**:

[1] Official Documentation for Ubuntu Linux Firewall <https://help.ubuntu.com/lts/serverguide/firewall.html>

[2] List of TCP and UDP port numbers: <http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers>