ITIS 6200/8200 Principles of Information Security and Privacy

Fall 2019 Semester Project: *Exploiting & Defending a SmartHome Router*

Phase 1: Network Security

Group Project

Deadline: Wednesday, October 9, 2019

Phase 1 Total Points Possible: 100

Submission instructions at the end of this document

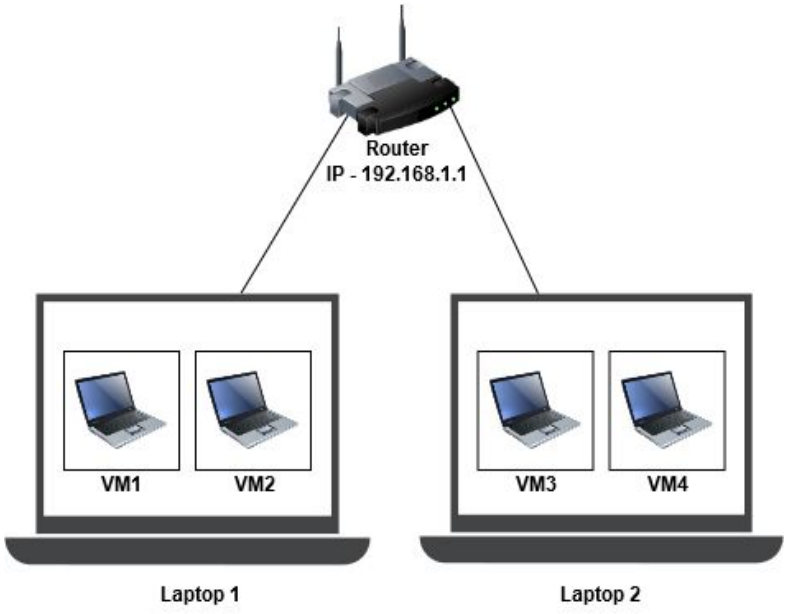
I. Basic Networking Background

This task will test your basic networking knowledge that is required to complete Phase 1 successfully. If you do not have this background, please refer to the Appendix "Networking Background References" at the end of this project document.

Task I: Answer the following questions [Total 20pts]

1. List the port numbers used for the following services and specify what the services are used for in **1-3** lines. **[5x2pts=10pts]**
   (a) SSH, (b) HTTP, (c) HTTPS, (d) Telnet, (e) DHCP

2. Assign IPs to the following devices if the VMs are connected in the following network settings. *You can modify the diagram to show the IPs OR list the IP addresses in text form. (For e.g.: VM1 - xx.xx.xx.xx, VM2 - xx.xx.xx.xx).* **[2x4pts=8pts]**
   a. Bridge
   b. NAT *(You can assume any IP ranges for the Network that VMWare provides)*



3. How many IPs and interfaces does the router use? Why? **[1x2pts=2pts]**
   Reference: https://www.youtube.com/watch?v=CVrYEPHexB4

II. Learning iptables—The Linux Firewall

"iptables" is a firewall and networking tool available to all Linux distros and operates by analyzing packets and can be configured to provide a high level of control over which packets are allowed in the network. In this part you will read and understand the functioning and configuration of iptables.

A. BASIC "IPTABLES" REQUIRED READING

1. Firewall: https://www.youtube.com/watch?v=x1YLj06c3hM
2. iptables by Mike Murphy: https://www.youtube.com/watch?v=iP8YWcvKDr0 (Watch 2:15-6:10)
3. How to write iptables rules:
    a. https://www.youtube.com/watch?v=eC8scXX1_1M
    b. https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-using-iptables-on-ubuntu-14-04
    c. https://www.cybrary.it/0p3n/introduction-iptables-command/

Task II.A: Answer the following questions in 1-3 sentences ONLY [Total 16pts]

1. What does a firewall do? **[2pts]**
2. What capabilities does iptables provide? Can it forward packets to other machines? **[2pts]**
3. What is the difference between iptables actions ACCEPT, DROP and REJECT? How is DROP and REJECT different? **[3pts]**
4. State the purpose of each of the following iptable rules: **[9x1pt=9pts]**

> **For example:**
> ***iptables -L*** **-** displays the rules for the default "filter" table
> ***iptables -t nat -L*** **-** displays the rules for the NAT table
> ***iptables -A INPUT -s 192.168.0.1 -p tcp --dport 25 -j DROP*** **-** Adds a rule to the INPUT chain in the default table "filter" stating to allow all traffic from source 192.168.0.1 with the protocol tcp on the destination port 25.

    a. *iptables -S*
    b. *iptables -P FORWARD ACCEPT*
    c. *iptables -t nat -P INPUT DROP*
    d. *iptables -F*
    e. *iptables -t mangle -F*
    f. *iptables -L --line-numbers*
    g. *iptables -D OUTPUT 4*
    h. *iptables -t mangle -D INPUT 12*
    i. *iptables -A INPUT -i eth0 -s 10.10.10.100 -p tcp --dport 25 -j ACCEPT*

After doing the answering the above, you SHOULD BE ABLE to do the following on the router: *(This is just for reference. Don't add these rules to the router just yet)*

1. Allow SSH connections on port number 2222 from the WAN.
2. Allow telnet connections on port 2233 from the WAN.
3. Allow HTTP and HTTPS connections from the WAN.
4. Drop all other incoming connections.

Note: *WAN is the interface of the router that is connected to the outside world. It is the "Blue" port.*

B. ADVANCED "IPTABLES" REQUIRED READING

Use the following resources to learn more about what other functionality iptables offers than to just allow/deny connections. For example: NAT and forward.

1. NAT - SNAT, DNAT, PAT: https://www.youtube.com/watch?v=wg8Hosr20yw
2. NAT in practical use by Dr. Mike Murphy: https://www.youtube.com/watch?v=3mTQ8MS4Nr0
3. Deep dive into iptables and netfilter
   Read up on the following topics in the link below:
   a. *What Are IPTables and Netfilter?*
   b. *IPTables Tables and Chains*
   c. *The Filter table*
   d. *The NAT table*
   e. *Checkout the chains in the "Filter" and "NAT" tables*
   f. *Chain Traversal Order*
   g. *IPTables and Connection Tracking*
   h. *Available States*
   https://www.digitalocean.com/community/tutorials/a-deep-dive-into-iptables-and-netfilter-architecture
4. *Do not read the whole writeup. Quick read and keep referring to this link as and when needed.* https://www.booleanworld.com/depth-guide-iptables-linux-firewall/

Task II.B: Answer the following questions in 1-3 sentences ONLY [Total 14pts]

1. With the help of an example describe the working of NAT in a home environment. **[2pts]**
2. Can you use NAT to translate addresses from one LAN (private IP) to another LAN (another private IP)? **[1pt]**
3. Explain how SNAT, DNAT and PAT are different in 1-3 lines each. **[3pts]**
4. What do these parts of the iptables syntax specify? What is their use? **[2pts]**
   a. *-m conntrack*
   b. *--ctstate ESTABLISHED,RELATED*
5. What do the following iptables syntax do? **[6x1pt=6pts]**
   a. *iptables -A INPUT -m conntrack --ctstate NEW,ESTABLISHED --dport 4343 -j DROP*
   b. *iptables -A INPUT -i lo -j ACCEPT*
   c. *iptables -t nat -A PREROUTING -p tcp --dport 1000 -j DNAT --to-destination 10.0.3.100:80*
   d. *iptables -A FORWARD -i eth1 -o eth2 -j DROP*
   e. *iptables -P FORWARD DROP*
   f. *iptables -A FORWARD -s 10.10.10.100 -o eth2 -j ACCEPT (checkthis)*

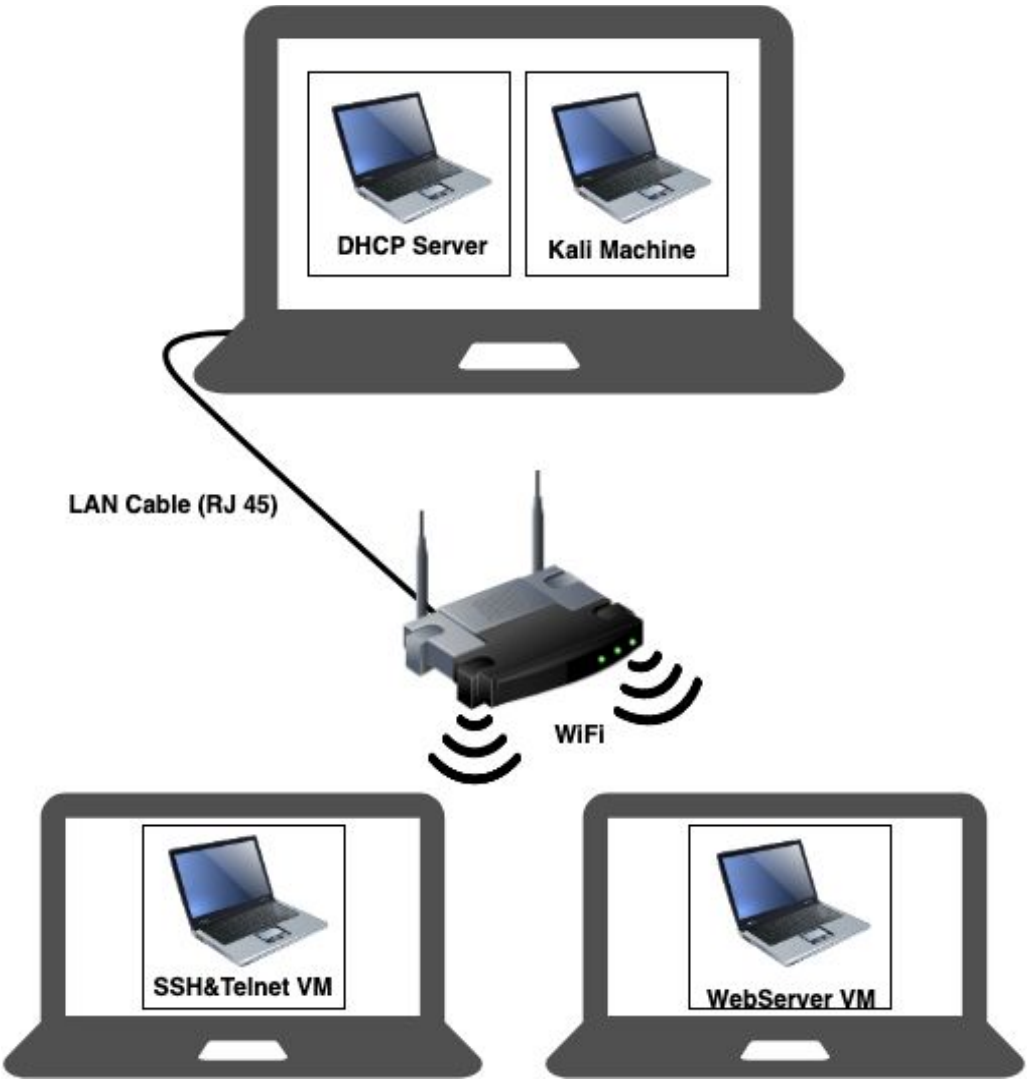
III. Working with iptables

A. CONFIGURING THE NETWORK STRUCTURE

Download the required VMs below here:

1. DHCP Server
2. SSH Telnet and Web Server VM
3. Kali Machine VM

Now, import the VMs to VMWare.
Next, connect the VMs and the devices as shown in the diagram below. Make sure that all the VMs have to be connected in Bridge mode so that they all resemble separate devices on the network.
Note: *Use the "SSH Telnet and Web Server VM" for "SSH&Telnet VM" and "WebServer VM".*



External Network: The DHCP server VM and the Kali VM is supposed to be running on a laptop that is connected to the WAN(Blue) port of the Router with a RJ45(LAN) cable. The DHCP server will create a network and give IPs to 4 machines - the DHCP server, Kali Machine, the Host Laptop(Host for the DHCP VM) and the Router.

Internal Network: These devices can be connected via Wireless(WiFi) or Wireline(RJ45 cable). These devices will be on a seperate network (internal network) of the router and the router will act as a DHCP for these devices. It will assign IPs for the 2 host Laptops and the 2 VMs.

Task III.A: Answer the following questions [2x5pts=10pts]

1. Create a network diagram and list out the IPs that each of the machines (Host and VM) gets assigned (You can use the above diagram or create your own).
   Note: The Router will have 2 interfaces, i.e. 2 IP addresses.

2. Draw boxes to show the group of devices that can communicate without any kind of NAT.

B. CONFIGURING IPTABLES

Notes:

a. *Since, you are doing this on a router, there would be a lot of pre-defined rules on the router. Don't worry about those rules and add the rules to enable the following functionality.*
b. *If you think that you misconfigured something, you can either delete the rule by identifying the line number of that rule and deleting it or just restart the router to reset the configuration.*

Add iptables rules for the following:

1. Allow SSH connections from WAN(Outside network) on port 2222 and forward them to port 22 of the "SSH&Telnet VM".
2. Allow telnet connections from WAN on port 2233 and forward them to port 23 of the "SSH&Telnet VM".
3. Allow connections on HTTP and HTTPS port from WAN and forward them to the same ports on "WebServer VM".
4. Allow access to the router's Web UI from WAN on port 8080.

Task III.B: Provide screenshots for the following [5x8pts=40pts]

1. Run "ifconfig" on the "Kali Machine VM". Then SSH into the "SSH&Telnet VM" from the "Kali Machine VM" and run "ifconfig". Submit screenshot of the terminal showing both the ifconfigs.
2. Run "ifconfig" on the "Kali Machine VM". Then TELNET into the "SSH&Telnet VM" from the "Kali Machine VM" and run "ifconfig". Submit screenshot of the terminal showing both the ifconfigs.
3. Access the website at "<Router's External(WAN) IP address>". Submit a Screenshot of the browser showing the address bar and the opened web page.
4. Access the router's Web UI at <Router's External IP address> at port 8080. Submit a screenshot of the browser showing the address bar and the opened web page.
5. Submit 2 text files rules in your "filter" and "nat" tables by writing the output to a text file.

   Print the rules to the text file in the following way:

   ```
   cd /
   iptables -S > filter_group#.config (Replace # with your group number)
   iptables -t nat -S > nat_group#.config
   ```

   Pull the files from the router to your local machine using scp or pscp in the following way after spawning a shell on your Desktop.

   For MAC - `scp root@192.168.1.1:/<filename> .`

   For Windows - Use this link at *6:50*

   https://www.youtube.com/watch?v=Sc0f-sxDJy0

SUBMISSION

Please TYPE (handwritten answers not accepted) your answers to questions in **Task I**, **Task II.A, Task II.B**, and **Task III.A** merge with screenshots in **Task III.B** into a .pdf document. Then compress (zip) this pdf with the file extracted from **Task III.B.5**. Submit the .zip file on Canvas by the due date. **Each group should submit ONE .zip file.**

Note: *Follow the instructions closely, and organize your answers neatly. Please label your answers with the appropriate Task and question labeling. For example "Answer Task II.A". Illegible, unclear answers or answers that do not adhere to instructions will be penalized.*

IV. Appendix: Networking Background References

1. Basic Networking Concepts: https://www.digitalocean.com/community/tutorials/an-introduction-to-networking-terminology-interfaces-and-protocols
2. Network Ports: https://www.youtube.com/watch?v=qsZ8Qcm6_8k
3. Hub, Switch, & Router: https://www.youtube.com/watch?v=1z0ULvg_pW8
4. Functionality of Routers: https://www.youtube.com/watch?v=CVrYEPHexB4v
5. NAT: https://www.youtube.com/watch?v=FTUV0t6JaDA
6. VMWare Networking Configurations (NAT, Bridge): https://pubs.vmware.com/workstation-9/index.jsp?topic=%2Fcom.vmware.ws.using.doc%2FGUID-D9B0A52D-38A2-45D7-A9EB-987ACE77F93C.html