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

Group #1: Sahil Bhirud, Sakshi Sakula, Sidney Henderson, Michael Bassimer

20th September 2019

I. Basic Networking Background

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: port 22, usually used to log into remote machines

(b) HTTP: port 80, communication between browsers and servers

(c) HTTPS: port 443, secure communication between browsers and servers.

(d) Telnet: port 23, connect to remote computers using TCP/IP

(e) DHCP:server uses port 67, client uses port 68. This service is used by Network Devices to assign automatic IP addresses to the devices in your network.

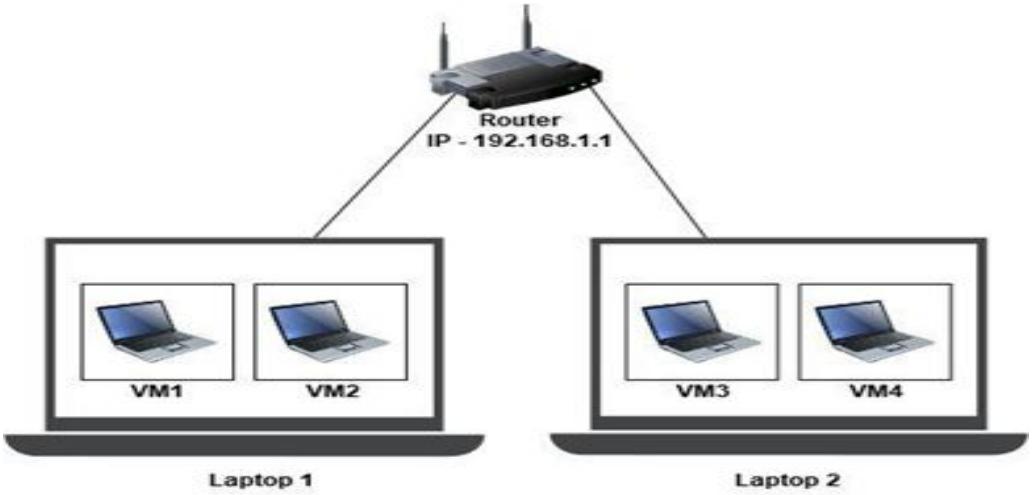
2. Assign IPs to the following devices if the VMs are connected in the following network settings. *You can modify the diagram to show the IPs OR list the IP addresses in text form. (For e.g.: VM1 - xx.xx.xx.xx, VM2 - xx.xx.xx.xx).* [2x4pts=8pts]

a. Bridge

Ans: Laptop 1 - 192.168.1.9, laptop 2 - 192.168.1.8

b. NAT *(You can assume any IP ranges for the Network that VMWare provides)*

Ans: Laptop 1 - 10.0.0.5, laptop 2 - 10.0.0.6



3. How many IPs and interfaces does the router use? Why? [1x2pts=2pts]

A router can have multiple interfaces but most of the routers have at least 2 network interface cards on them and each interface needs its own IP address. So that the router can easily move the packet from one IP network to different IP network.

Therefore, each IP in the network should be unique.

Reference:
https://www.youtube.com/watch?v=CVrYEPHexB4

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

1. What does a firewall do? [2pts]

A firewall acts as a defense system for a host system against viruses and other unauthorized access from entering a private network. It examines the incoming network traffic to make sure it doesn't contain blacklisted data and blocks unwanted traffic. It scans each packet of data and makes sure that these packets don't contain anything malicious.

2. What capabilities does iptables provide? Can it forward packets to other machines? [2pts]

A Userspace interface tool that allows Linux machines to function as routers or firewalls. Yes, the iptables can route packets to other machines.

3. What is the difference between iptables actions ACCEPT, DROP and REJECT? How is DROP and REJECT different? [3pts]

Accept is used to accept incoming traffic and connections.

Drop and Reject both prevent a packet from passing. However, REJECT sends an ICMP destination unreachable back to the host. DROP does not send a response.

4. State the purpose of each of the following iptable rules: [9x1pt=9pts]

a. iptables -S : Address source specification

b. iptables -P FORWARD ACCEPT : This is setting the policy to allowing the specific ip address to Forward and Accept packets.

c. iptables -t nat -P INPUT DROP : This command specifies the packet matching table and is consulted when a packet that creates a new connection is encountered. -P indecates to set the policy for the chain to the given target for packets. Drop implies to ignore the packet.

d. iptables -F :flush, flushes the selected chain

e. iptables -t mangle -F : table specifies which packet-matching table which the command should operate on. Mangle is a table used for specialized packet alteration.

f. iptables -L --line-numbers : lists all rules in the selected chain; when listing rules, add line numbers to the beginning of each rule.

g. iptables -D OUTPUT 4 : Delete chain-rule specification, OUTPUT refers to locally generate packets.

h. iptables -t mangle -D INPUT 12 : Calls a table used for specialized packet alteration, then runs chain rule-specification. “12” refers to the number of packets.

i. iptables -A INPUT -i eth0 -s 10.10.10.100 -p tcp --dport 25 -j ACCEPT :
This means to append the input rules at the bottom of the interface eth0 root shell from source 10.10.10.10.100 to accept TCP packets through port 25.

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]

Establishing a NAT for a home environment would allow a household to have one public IP address to communicate between their private network and public networks through the internet. This would allow the household to establish IP addresses for their personal devices that are dissimilar than the public IP address to increase the amount of connectivity with limited resources.

2. Can you use NAT to translate addresses from one LAN (private IP) to another LAN (another private IP)? [1pt]

Yes, it is possible and likely that this would be implemented. Two different small companies could implement NAT routers in their organizations and in order to transmit data to each other the NAT routers would need to take the source private IP address and reformat it to be able to be routed through public networks.

3. Explain how SNAT, DNAT and PAT are different in 1-3 lines each. [3pts]

- SNAT- Static network address translation has one public IP address and one private IP address. These addresses never change.
- DNAT-DNAT changes private IP address packets from the internal network and assigns the first public IP address from the public Ip address pool to relay that packet to another public IP address.
- PAT--PAT is different because uses a private IP address along with ports to designate routing of packets.

4. What do these parts of the iptables syntax specify? What is their use? [2pts]

a. -m conntrack : -m is used for matching, which extends the packet matching module. “Conntrack” allows you to display the existing flows and their state, along with other information.

b. --ctstate ESTABLISHED,RELATED

Connection states of ESTABLISHED and RELATED.

5. What do the following iptables syntax do? **[6x1pt=6pts]**

a. iptables -A INPUT -m conntrack --ctstate NEW,ESTABLISHED --dport 4343 -j DROP

Append the INPUT chain verify the connection states of NEW, ESTABLISHED from destination port 4343 to DROP.

b. iptables -A INPUT -i lo -j ACCEPT

Append INPUT chain for input interface loop-back to ACCEPT

c. iptables -t nat -A PREROUTING -p tcp --dport 1000 -j DNAT --to-destination 10.0.3.100:80

Append the NAT table PREROUTING chain for TCP packets from destination port 1000 to send to destination NAT IP 10.0.3.100.80

d. iptables -A FORWARD -i eth1 -o eth2 -j DROP

Append the forward chain for input interface eth1, and output interface eth2 to DROP

e. iptables -P FORWARD DROP

Policy is set for the chain to the given target that are forwarded through the box, which become dropped.

f. iptables -A FORWARD -s 10.10.10.100 -o eth2 -j ACCEPT (checkthis)

Appending a forwarded source specification at ip 10.10.10.100, and the packet will be going to eth2 ports. If the packet matches, then the packet is let through.

III. Working with iptables

A. CONFIGURING THE NETWORK STRUCTURE

Download the required VMs below here:

1. DHCP Server :

   A Raspbian machine with a configured DHCP service to give out IPs in the 192.168.11.0/24 subnet. **Username:** pi **Password:** tplink

2. SSH Telnet and Web Server VM :

A Raspbian machine with SSH and Telnet servers enabled(You can connect via SSH and Telnet to these machines). It also has a working Apache Web server. **Username:** pi **Password:** tplink

3. Kali Machine VM :

   Generic Kali VM to be downloaded from Kali Official Website(64bit). **Username:** root **Password:** toor

We used Raspbian Operating System - a Debian Linux based OS for Raspberry Pi as the size of the OS is considerably smaller when compared to other Linux distros. Most of the Linux Terminal commands will work here.

Now, import the VMs to VMWare. *These are premade boxes saved in ".ovf" format. You can easily import these to VMWare by selecting the Import utility from VMWare or by double clicking on the ".ovf" files. If you cannot figure it out, then please Google for tutorial to do this.*

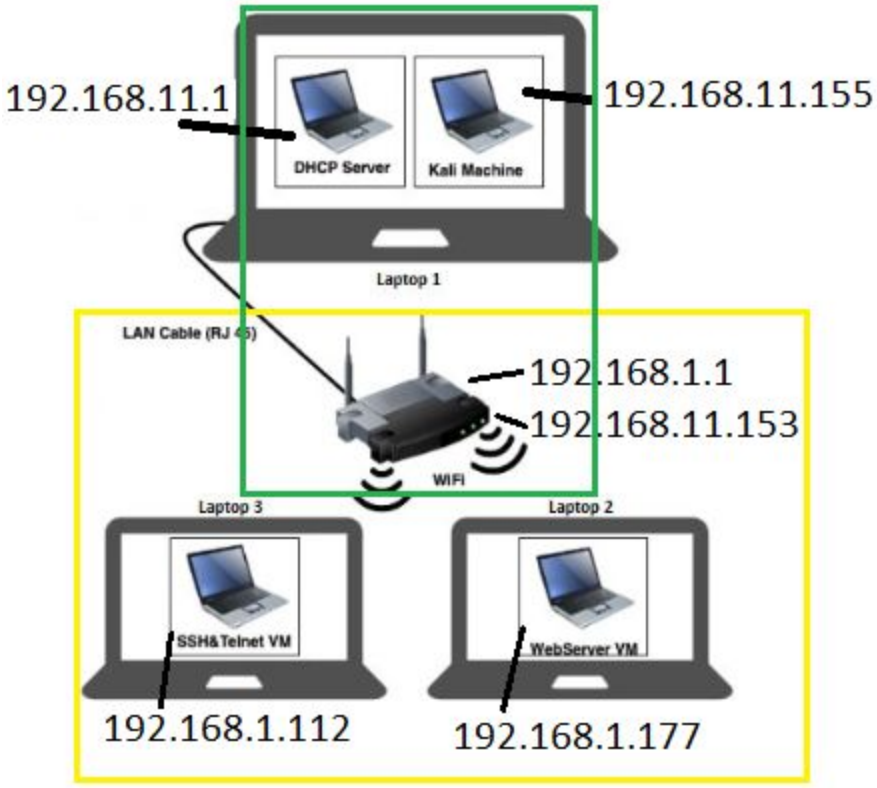
Next, connect the VMs and the devices as shown in the diagram below. Make sure that all the VMs have to be connected in Bridge mode so that they all resemble separate devices on the network. **Note:** *Use the "SSH Telnet and Web Server VM" for "SSH&Telnet VM" and "WebServer VM".* External Network: The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



Without the NAT, the laptops, router, and VM's can still communicate with one another over their own subnet. No communication can happen across the router if it is not forwarding between the two interfaces.

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”.

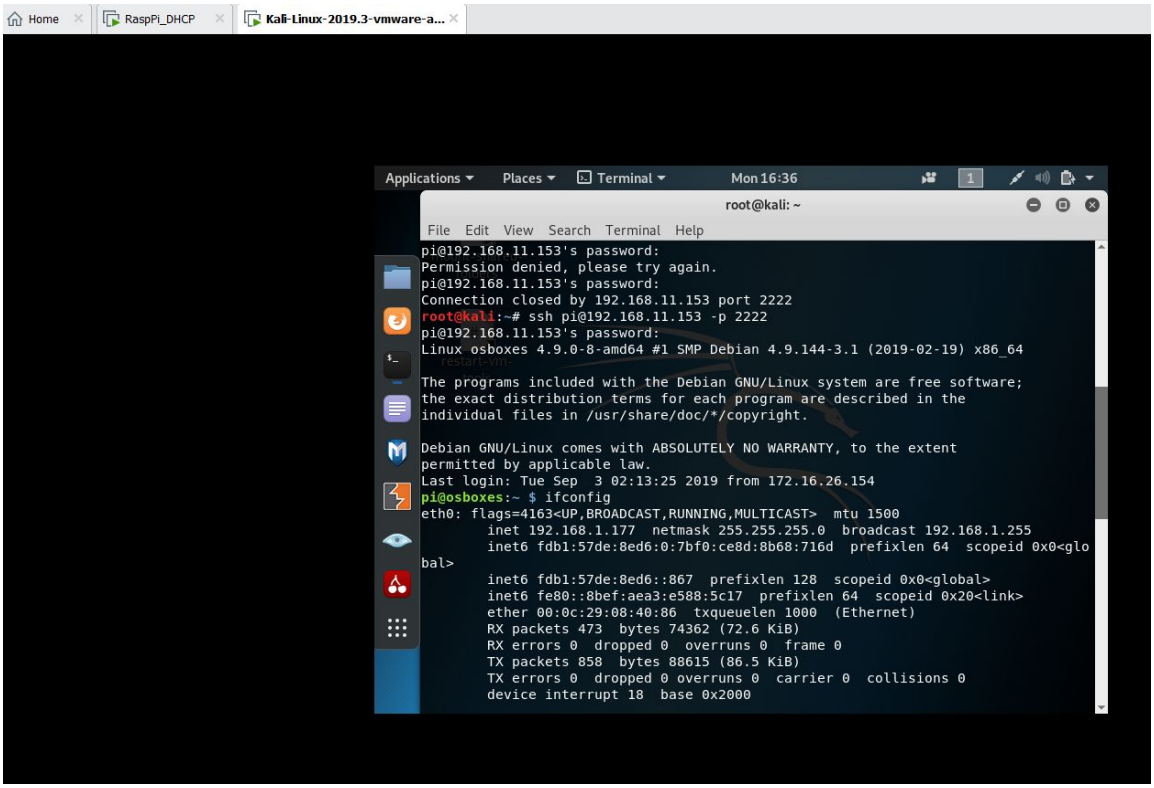
4. Allow access to the router's Web UI from WAN on port 8080.

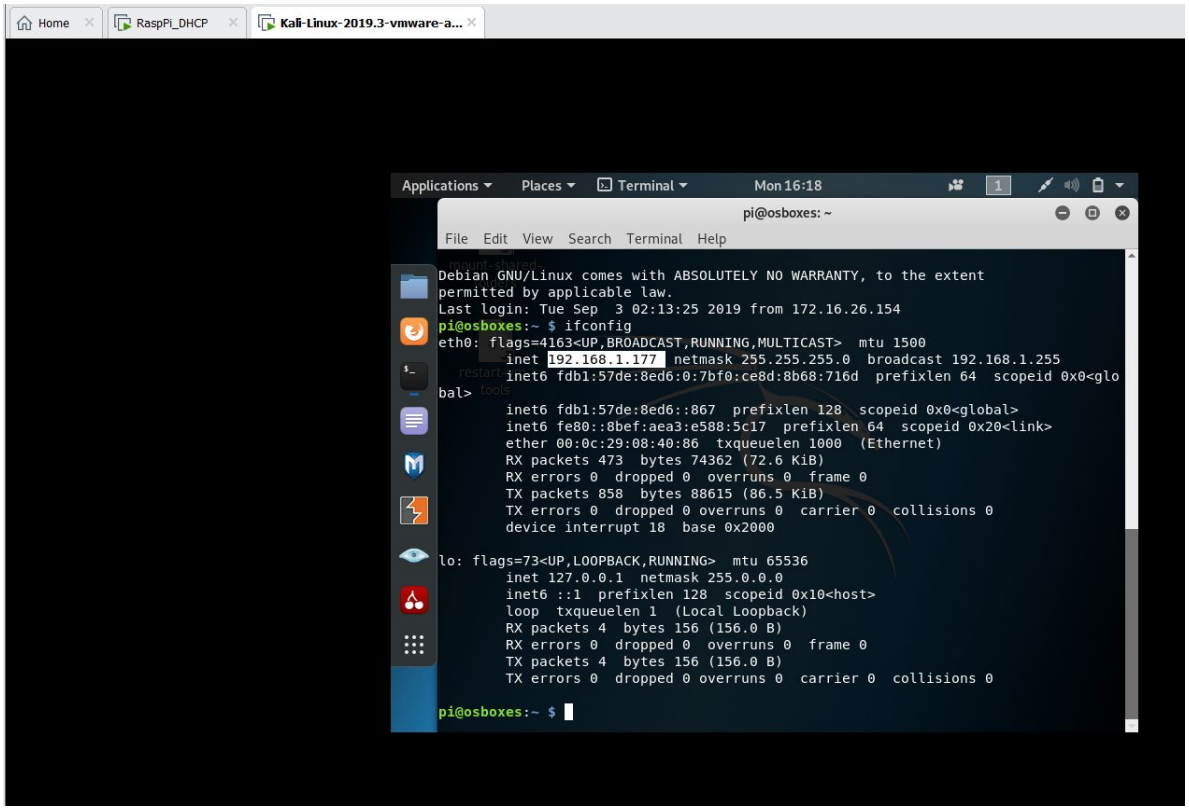
Task III.B: Provide screenshots for the following [5x8pts=40pts]

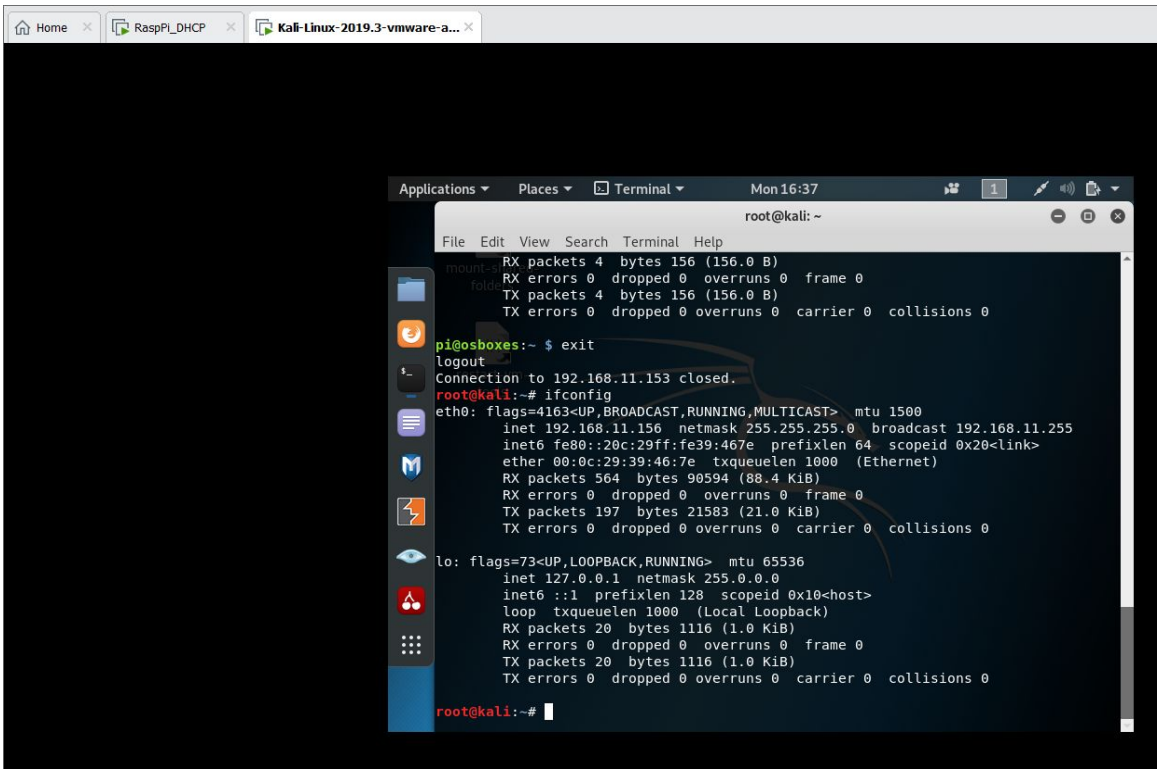
1. Run “ifconfig” on the “Kali Machine VM”. Then SSH into the “SSH&Telnet VM” from the “Kali Machine VM” and run “ifconfig”. Submit screenshot of the terminal showing both the ifconfigs.

Ans: ssh pi@192.168.11.153 -p 2222

(Images below)



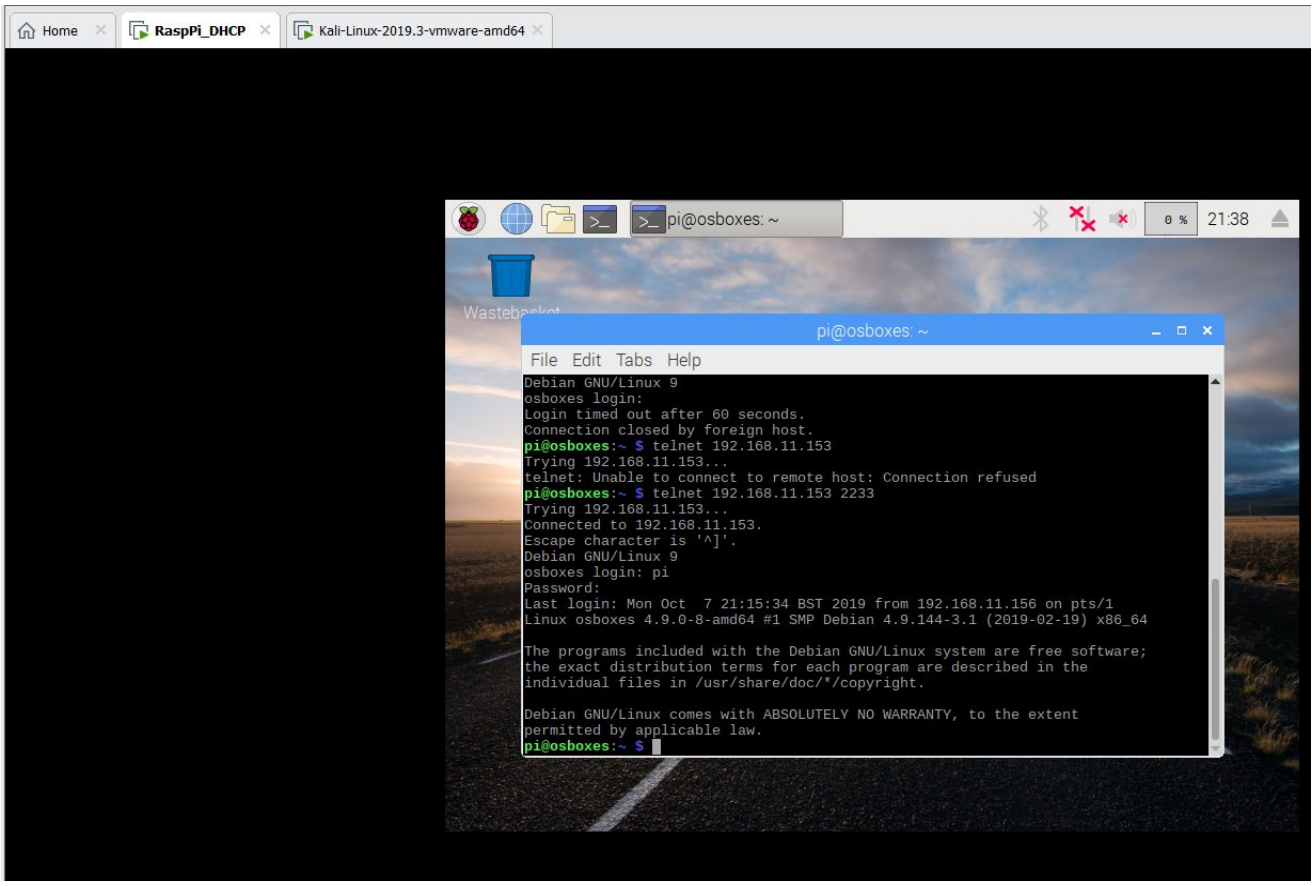


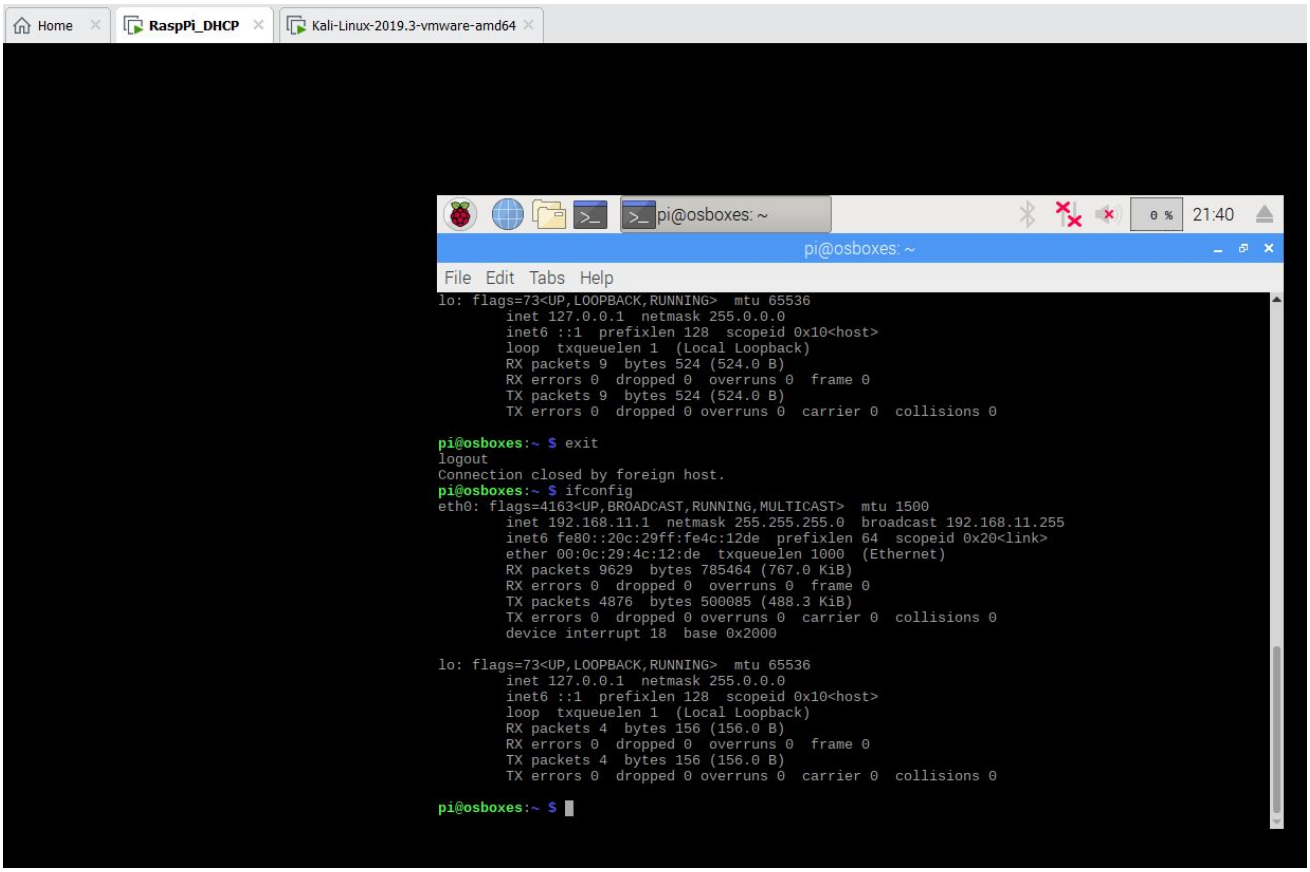


2. Run “ifconfig” on the “Kali Machine VM”. Then TELNET into the “SSH&Telnet VM” from

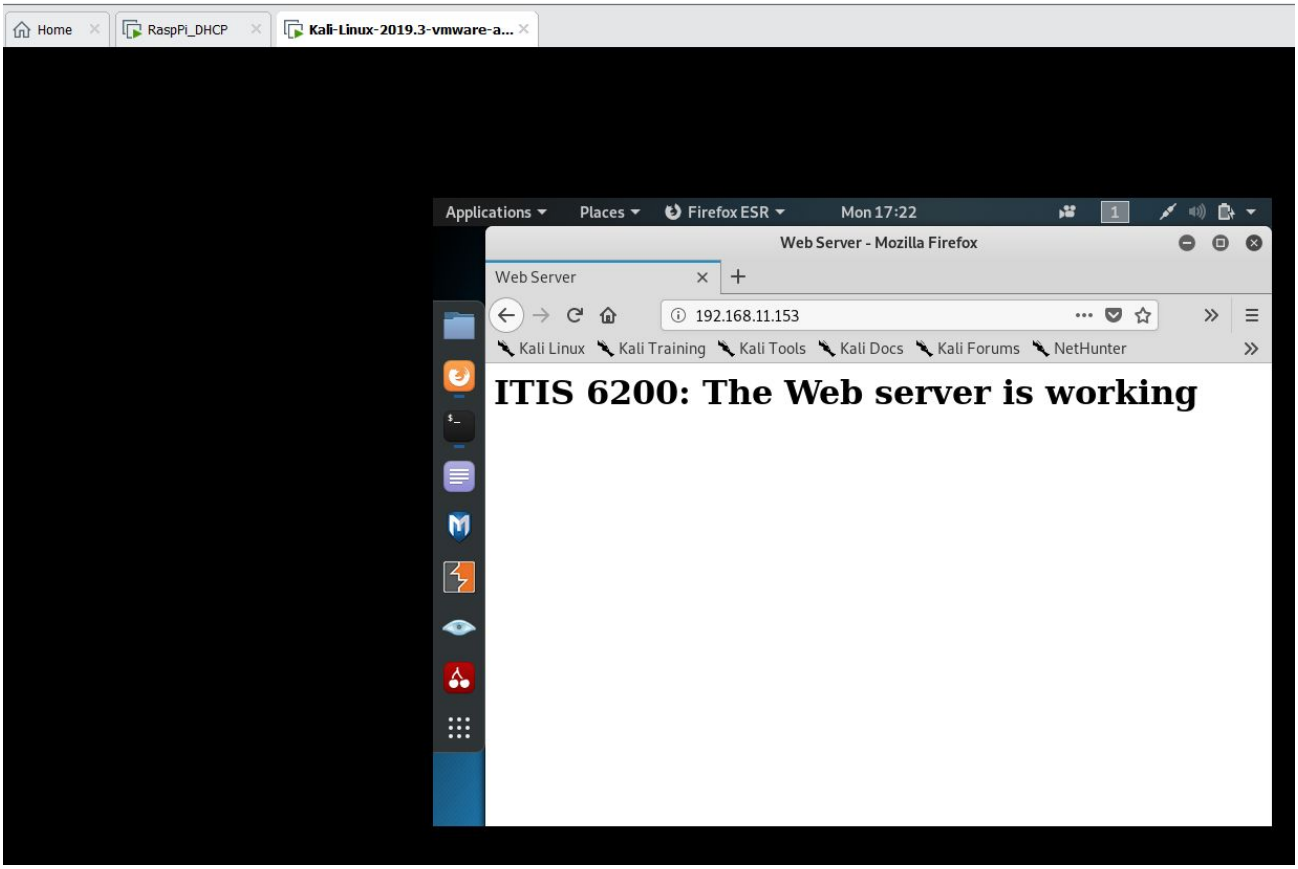
the “Kali Machine VM” and run “ifconfig”. Submit screenshot of the terminal showing both the ifconfigs.

Ans: telnet 192.168.11.153 2233

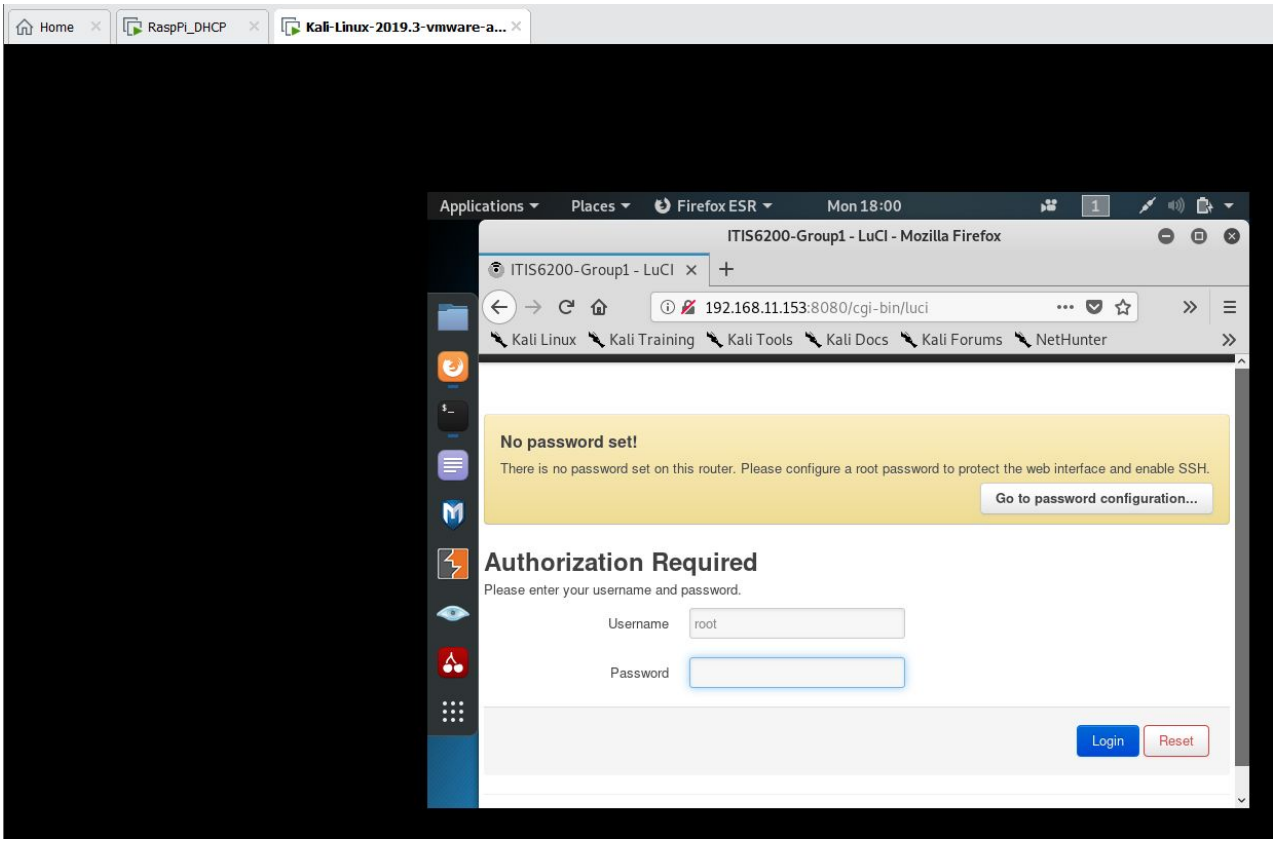



Home
RaspPi_DHCP
Kali-Linux-2019.3-vmware-amd64
pi@osboxes: ~
0 %
21:40
pi@osboxes: ~
File Edit Tabs Help
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1 (Local Loopback)
RX packets 9 bytes 524 (524.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 9 bytes 524 (524.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
pi@osboxes:~ $ exit
logout
Connection closed by foreign host.
pi@osboxes:~ $ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.11.1 netmask 255.255.255.0 broadcast 192.168.11.255
inet6 fe80::20c:29ff:fe4c:12de prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:4c:12:de txqueuelen 1000 (Ethernet)
RX packets 9629 bytes 785464 (767.0 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 4876 bytes 500085 (488.3 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device interrupt 18 base 0x2000
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1 (Local Loopback)
RX packets 4 bytes 156 (156.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 4 bytes 156 (156.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
pi@osboxes:~ $

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.



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