**LAB 3: NMAP and IPTABLES**

**1. NMAP:**

Nmap (Network Mapper) is a security scanner used to discover hosts and services on a computer network, thus creating a map of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyzes the responses.

Extensive information about nmap can be found at:

<https://nmap.org/>

Using nmap gather information about the 10.10.111.0/24 network and 10.20.111.0/24 network.

First be sure that all of your virtual machines are powered up, starting with the external router (rtr), then the internal router (int-rtr), then the other VMs. Your primary virtual machine for this lab will be Backtrack 5 (bt5). The username is “root” with a password of “toor”.

After you login, start the gui using the command “startx”.

You should have a DHCP address assigned to your Backtrack machine. You can verify this by opening a terminal session and typing: ifconfig.

Open up a terminal window and execute the nmap scan of 10.10.111.0/24 and 10.20.111.0/24 from the command line.

**Part 1:**

Follow the instructions and document the commands and results using screenshots in your report. Explain what is going on in each screenshot.

1. Using nmap, find all the open ports and OS on each host in the 10.10.111.0/24 network. List the command which is used. [10 points]

2. Using nmap, find all the open ports and OS on each host in the 10.20.111.0/24 network. List the command which is used. [10 points]

**2. IPTABLES:**

iptables is a user-space application program that allows a system administrator to configure the tables provided by the Linux kernel firewall (implemented as different Netfilter modules) and the chains and rules it stores.

Extensive information on iptables can be found in the following links:

[https://wiki.archlinux.org/index.php/Iptables](https://wiki.archlinux.org/index.php/Iptables" \t "_blank)

[https://wiki.archlinux.org/index.php/Simple\_stateful\_firewall](https://wiki.archlinux.org/index.php/Simple_stateful_firewall" \t "_blank)

**All Firewall and NAT operations for this lab must be performed on 10.20.111.1 (internal router/firewall).**

**Part 2:**

Configure the iptables firewall on the internal network firewall machine to implement the following firewall policies and list the commands that is used.

A) For outgoing traffic (from 10.20.111.0/24 to 10.10.111.0/24) - your internal machine should be able to communicate with the external network and the external machines without restrictions. [10 pts]

B) For incoming traffic (from the 10.10.111.0/24 to the 10.20.111.0/24) - all incoming connection requests should be rejected with the following exceptions:

1) The internal machine (10.20.111.2) should respond to a ping from 10.10.111.0/24 [5 pts]

2) The internal machine (10.20.111.2) should block all incoming SSH and http requests from 10.10.111.0/24 [5 pts]

3) The internal machine (10.20.111.2) should accept telnet connections from the BT Machine only. [5 pts]

Verify that your rules are installed correctly by generating appropriate traffic.

**Note:** if required you can flush all the firewalls rules on the internal firewall at the beginning before installing any rules. This can be done using the command:

**Iptables -F**

**3. NMAP & IPTABLES:**

**Part 3:**

1. Following are the options you will find yourself often needing when using nmap. Use each of these options to perform a scan on student\_linux VM (10.10.111.106) using BT5 as an attacker machine. Submit a quick one-liner beside each to explain what each does and screenshots of each scan that you performed. (10 points)
2. -n
3. -P0
4. -O
5. -v
6. -oN
7. Using the BT5 machine as the scanning machine, perform a nmap scan on DVL VM. Include screenshots of the scan results in your report.
8. Did DVL VM respond to nmap’s probes? If yes, write a firewall rule that blocks all incoming ICMP packets and connection to TCP ports 80 (HTPP) and 443 (HTTPS) on your DVL VM.(5 points)
9. Now that you have blocked incoming ICMP messages and the other nmap probes to the DVL VM, execute nmap. Submit screenshots of your nmap command and results of your scan. (5 points)
10. There is a method of forcing nmap to scan hosts even if the initial nmap probes are blocked. Leaving the iptables in place that block nmap’s initial probe requests and run nmap with a set of options that scans 10.10.111.110 even when it doesn't reply to nmap’s initial probe requests. Include the nmap options you used and a screenshot of the scan. (5 points)
11. Using BT5 machine as an attacker machine, perform a nmap TCP SYN scan on DVL VM (10.10.111.110). Then construct an iptable rule to block all incoming TCP SYN packets only from the BT5 scanning server’s IP address. Explain what are the trades off of blocking all TCP SYN packets from an IP address. Submit screenshots of your TCP SYN scans before and after applying the iptable rule. (5 points)