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 Kali. The username is "student" with a password of "student".

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

Turn in for 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 that 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 that 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/Simple_stateful_firewall

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

Turn in for part 2:

Configure the iptables firewall on the internal network firewall machine to implement the following firewall policies and list the commands 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 [10 pts]
2) The internal machine (10.20.111.2) should block all incoming SSH and http requests from 10.10.111.0/24 [10 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:

“sudo iptables -F”

3. NMAP & IPTABLES:

Turn in for 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 the Ubuntu VM using Kali as an attacker machine (see Lab 0 for the login information for the Ubuntu machine). Submit a quick one-liner beside each to explain what each does and screenshots of each scan that you performed. (10 points)
   a) -n
   b) -P0
   c) -O
   d) -v
   e) -oN

2) Using Kali as the scanning machine, perform an nmap scan on the Int-Linux VM (see Lab 0 for the login information for the Int-Linux machine). Include screenshots of the scan results in your report.

   a) Did the Int-Linux VM respond to nmap's probes? If yes, write firewall rules to stop it. This involves blocking incoming ICMP packets, and ports 443 and 80. If you write firewall rules, make sure to verify that they are installed correctly. (10 points)
   b) Now that you have implemented the appropriate rules on the Int-Linux VM, execute nmap from Kali. Submit screenshots of your nmap command and results of your scan. (10 points)
   c) 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, run nmap with a set of options that scans Int-Linux even when it doesn't reply to nmap's initial probe requests. Include the nmap options you used and a screenshot of the scan. (10 points)

3) Using the Kali machine as an attacker machine, perform a nmap TCP SYN scan on the Metasploitable VM (see Lab 0 for the login information for the Metasploitable machine). Then construct an iptable rule to block all

incoming TCP SYN packets only from the Kali scanning server’s IP address. Explain the trade offs of blocking all TCP SYN packets from an IP address. Submit screenshots of your TCP SYN scans before and after applying the iptable rule. (10 points)