**Graduate Program in Information Assurance Engineering**

# IA-500: Introduction to Information Assurance

Lab 5 – Vulnerability Scanning & Patching – NMAP

**Lab Objective:**

The objective of this lab is to introduce students to NMAP and ZenMap. The student will be able to use NMAP to scan a network and find computers. They will also be able to understand the ports that are open on a computer using NMAP.

**Laboratory Deliverable:**

1. Screenshot of using the basic NMAP command on the Kali VM.
2. Screenshot of using ZenMap to Ping scan the LAN on Kali VM.
3. Screenshot of using ZenMap’s Topology viewer on Kali VM.
4. Screenshot of using ZenMap to do an intense scan on the Kali4 VM.

**Materials:**

1. Kali Virtual Machine
2. Metasploitable Virtual Machine

**Instructions:**

1. Open your Kali VM
2. Open your Metasploitable VM and log in as “msfadmin” with the password “msfadmin”.
3. Make sure your VM settings on both VM’s have the network set as VMnet 1.
4. In your Kali VM edit the file “/etc/resolv.conf” to look like:

search localdomain

nameserver 8.8.8.8

nameserver 8.8.4.4

Edit the file “/etc/network/interfaces” to look like:

auto lo

iface lo inet loopback

auto eth0

iface eth0 inet dhcp

1. Repeat step 4 for your Metasploitable VM. To edit the files, use the following commands:

$ sudo nano /etc/resolv.conf

$ sudo nano /etc/network/interfaces

When you execute the commands, it will ask you for a password, use “msfadmin”.

1. In Kali, run:

$ /etc/init.d/networking restart

1. In Metasploitable, run:

$ sudo /etc/init.d/networking restart

If asked for a password, use “msfadmin”.

1. In Metasploitable, run:

$ ifconfig

Find your IP address on “eth0” where it says “inet addr:” and record it as the Metasploitable IP address. **Metasploitable IP address: (192.168.175.128), 192.168.65.1**

1. In Kali, open a terminal.

‘’’ OPTIONA

For ease of use, assign Metasploitable’s IP to the variable RHOST

$ RHOST= IP address

‘’’

1. Now let’s see if we can ping the Metasploitable box. You can either type out the IP address of the Metasploitable box or use the variable we created. If the variable doesn’t work, you may have left your terminal where you defined it. In that case, you’ll just have to redefine it.

$ ping $RHOST

#NOTE: RHOST = Metasploitable’s IP address

To stop pinging after we gotten a few responses back, interrupt the process. (CTRL + C)

If you are unable to ping the box, that means you have not successfully configured your boxes’ networking. Make sure you have followed all of the previous steps.

1. NMAP is a security scanner that is used to map networks. It is used to discover hosts and services on a network. Let’s try using NMAP now. In the Kali VM, run:

$ nmap $RHOST

Take a screenshot of the results.

1. NMAP will list the ports opened along with their state and what service they are associated with.
2. To get more information while the NMAP is running, we use the verbose switch. Try it out now:

$ nmap –v $RHOST

1. To get out more information about the host computer, we just add another switch:

$ nmap –O –v $RHOST

This will print out information about the host operating system. Or it will try to. Not always can NMAP guess what the system is.

You will see a device type, what OS the host is running, and how many hops away the host is.

1. To get even more operating system information from the host, we use:

$ nmap –sV –O –v $RHOST

This will print out information about system up time, TCP sequence prediction difficulty, IP ID sequence generation, and service info.

1. To do a ping scan, where we do not look up what services on running on a host but find out if there is a host up an address, we run:

$ nmap –sP $RHOST

1. To do a ping scan on a network to find all hosts up, we can use a wild card. Try using the first three octets of the Metasploitable IP address and then use a wildcard in place of the fourth octet. For example, if the Metasploitable’s IP is “192.168.1.14”, run:

$ nmap –sP 192.168.1.\*

1. To find out what hosts are running a web server, we can run a port scan on a network for just one port. To do this, try scanning the Metasploitable’s local network for hosts running web servers:

$ nmap –p80 192.168.1.\*

1. To scan for multiple certain ports, we can just add commas to the p switch.

$ nmap –p21,23,80 192.168.1.\*

1. On Kali, open up the terminal and enter

$ zenmap

1. In the Target field, type the Metasploitable IP address you recorded earlier. In the profile field, use the drop down menu and select “Regular scan”, then press “Scan”.

In the right window, the command output you would see in the console is printed. In the “Command:” field, you will see the command you would run if you were in the console. In the left window, there is a list of hosts that have been scanned.

1. In the right window, select the tab that reads “Topology”.

This is a map of the network you have scanned. Your computer is the black dot located in the center of the map. The big red dot is the Metasploitable VM that you just scanned. The reason it is a big red ball is because the host has a lot of services open. The less the services, the littler the circle will be. If there are only closed ports, then the circle will be green. If the host is a router, then there will be a square instead of a circle.

1. Let’s do a simple “Ping scan” on your local network. This is the most we will do because we are not allowed to do a service scan on a network that we do not own. This will demonstrate a larger network since we can’t setup one in a virtual environment as it would take too many system resources.

Open up your host computer.

If you are using a Windows computer, press the Windows key and “R” (WINDOWS + R) and then type “cmd” and press ENTER. This will open the Windows command prompt. Run:

$ ipconfig

Find and record your IP address of VMnet1, this is your host address.

If you are using a Mac computer, open up the applications menu, select utilities, and then terminal. Type:

$ ifconfig

Find and record your IP address of VMnet1, this is your host address.

1. Open up your Kali VM and inside the the target field, type the first three octets of the IP address and then replace the last with a wildcard or “\*”. So if your IP address is “192.168.100.42”, then enter “192.168.100.\*”. Next, select from the drop down menu of the profile field, “Ping scan”. Make sure you have the “Nmap Output” tab selected. Next, press “Scan”. This will scan the entire LAN for computers.

Take a screenshot of your VM.

1. Press the “Topology” tab and look at the network map. Note the number of hosts in the left window. See how there are more hosts now?

Take a screenshot of the network topology.

1. Let’s go back to the “Nmap Output” tab and try out an “Intense scan”. In the target field, type the IP address of the Metasploitable VM. In the drop down of the “Profile” field, select “Intense scan” and then run the scan.

Take a screenshot of the results.

1. Select the “Ports/Hosts” tab. In this view, we can see the port/protocol/state/service/version of the services that are running on a host. Make sure the Metasploitable host is selected from the list of hosts in the left window.
2. Select the “Host Details” tab. In this view, we can see the list of operating system details about the host. Select the different dropdown values and examine the Metasploitable VM’s details.

==END==

**Questions:**

1. What is NMAP? **a tool that hackers use to view information about a host computer like IP information, what the system’s OS is, general system info, and it can ping the system**
2. What is ZenMap? **A tool that hackers use to gather information about a target computer like what ports are open, host details, different scanning options to detail more about the host while remaining discreet**
3. Are you allowed to scan any IP address on the internet or your school/business’s intranet? Why or why not? **No, only doing a simple NMAP ping, but more than that is illegal (mainly the system cannot allocate enough resources in the VM to complete the scan)**
4. How do you perform a regular scan on the host at 192.168.100.2 via NMAP? **nmap 192.168.100.2**
5. How do you perform a ping scan on the host at 192.168.100.10 via NMAP? **nmap -sP 192.168.100.10**
6. How do you perform a ping scan on the LAN at 192.168.50.0 via NMAP? **nmap –sP 192.168.50.0**
7. How do you perform a regular scan on the LANs at 192.168.0.0 via NMAP? **nmap -sP 192.168.0.\***
8. Using the Kali VM and ZenMap, what is the command used to complete an “Intense scan” with NMAP? nmap –T4 –A –v
9. What does the Topology view of ZenMap do? **It shows you the network you scanned with a visual representation that displays if a system has open or closed ports, and how big the dot is shows how many services it has open**
10. What does the Host Details view of ZenMap do? **It shows the status of the host, including the IP, the number of closed, scanned ports, up time, last boot, etc.**
11. Why is ZenMap so useful? **It is helpful in finding vulnerabilities of a host discreetly**

|  |  |  |  |
| --- | --- | --- | --- |
| Requirement | **Points Allowed** | **Points Actual** | **Comments** |
|  |  |  |  |
| **Title page** | **5** |  |  |
| **Screen shots** | **5** |  |  |
| **Questions** | **10** |  |  |
| **Conclusion** | **5** |  |  |
|  |  |  |  |
| **Extra Credit** |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **Total Points** | **25** |  |  |