**Lab 6: Vulnerability Scanning**

**Objective**

The objective of this lab is to create a report of potential vulnerabilities for a virtual machine. The VM is an Ubuntu-based Linux distribution called MetaSploitable2, which is specifically designed to teach penetration testing skills such as vulnerability scanning.

**Setup VMs**

**Set Up the “infoset-net” Network for VirtualBox**

## **infosec-net Network Map**

The network map is as follows:

| **IP Address** | **Machine** |
| --- | --- |
| 192.168.55.100192.168.55.101192.168.55.102 | Windows 10 VMKali Linux VMMetasploitable2 |

1. Download the Metasploitable2 VM that has been configured with the IP address 192.168.55.102 from this link:

<https://www.dropbox.com/s/uxow5s4bb0osyr8/metasploitable2.ova?dl=0>

**Note:** Skip this entire section if you're using the VMs I distributed in class.

2. Import Metasploitable2 into VirtualBox. After booting up the VM, log in with username “msfadmin” and password “msfadmin.”

3. Boot up the Kali VM.

4. **Important**: Ensure that you can ping each VM from each VM before continuing the lab. If using the VMs provided for the class, Kali has the IP address 192.168.55.101 and Metasploitable2 has the IP address 182.168.55.102. Ping each VM as follows:

From Kali VM, pinging Metasploitable VM:

ping 192.168.102

From Metasploitable VM, pinging Kali VM:

Ping 192.168.55.101

You should see a response like the following:



**Note:** Stop the ping command with the keys **control + c**.

**Part 1. Host Discovery and Scanning using NMAP**

NMAP is the de facto standard of host discovery and port scanning and has a host of features that make the q tool very robust. In this section of the lab, you’ll try a few of NMAP’s features.

1. Open a terminal window in Kali by selecting the Applications menu in the top left of the screen, and selecting Accessories —> Terminal.
2. Type nmap. Take a quick look at the available options.
3. Use nmap to determine whether the your Metasploitable2 VM is live using a ping scan:

nmap -sn [IP of Metasploitable]

The ping scan not only sends an ICMP request, but also an ARP ping, TCP pinging, and other techniques to determine if a host is live on the network.

1. You can also scan a range of IPs using [CIDR block notation](https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing#CIDR_notation). My “Host-Only Network” range is 192.168.55.0/24, meaning all of my addresses for that network are between 192.168.55.1 – 192.168.55.255. So I would type:

nmap -sn 192.168.56.0/24

You can know your network by typing ifconfig on either Kali or Metasploitable, and looking for the inet address plus the mask value on the same line. A maskof 255.255.255.0 applied to an inet address of something like 192.168.56.17 translates to a network of 192.168.56.0/24. (Get it? 24 is the number of bits to mask and it takes 8 bits to make 255, 8x3=24, so mask three of the ‘.’ blocks.)

**Question:** What information is shown for your Metasploitable VM, besides its IP address?

1. Once you determine that a host is live, you can use NMAP to scan for open ports. Use a TCP scan to determine which ports are open on Metasploitable2:

nmap -sS [IP of Metasploitable]

This scans approximately 1,800 of the most common TCP ports on the target machine.

**Question:** Which ports are open on the Metasploitable2 VM?

1. You can also specify additional ports to scan. Scan the first 10,000 ports of the Metasploitable2 VM:

nmap -sS -p1-10000 [IP of Metasploitable]

**Question:** Did you find any additional ports?

1. Nmap can provide additional information about open ports by interrogating the ports it finds using the “sV” flag:

nmap -sV [IP of Metasploitable]

**Note:** Press the “enter” key to see a status of the NMAP scan.

1. You can get further information still by using the advanced flag (“-A”).

nmap -sV -A [IP of Metasploitable]

**Question:** What additional information about the open ports on Metasploitable2 were you able to obtain by using the -sV and -A flags?

1. A useful feature of nmap is operating system fingerprinting which it accomplishes by profiling how a system responds to its scans.

nmap -O [IP of Metasploitable]

**Note:** That’s a capital “oh” not a “zero.”

**Question:** What operating system does nmap report Metasploitable2 to be?

1. Now scan for web applications on Metasploitable2. Increasingly, applications run off of a different URL, all using port 80.

nmap -sV --script=http-enum [IP of Metasploitable]

**Question:** What web applications are available on Metasploitable2?

**Part 2. Nessus**

If you are **not** using my prepared VM, then [install Nessus onto your Kali VM](https://daveeargle.com/security-assignments/virtual-machines#install-nessus). If you **are** using my prepared Kali VM, then proceed with the steps below.

1. In the Kali VM, open a terminal and type service nessusd start
2. On the Firefox web browser, navigate to https://kali:8834 to open the Nessus web interface (note the “s”). (Click ‘Advanced’ > ‘Add Security Exception’ > ‘Confirm Security Exception’ to get past the SSL warning.)
3. Login with username “root” and password “toor”. Click the “reload” if the page fails to load.
4. Click the “Policies” tab and press the “New Policy” button.
	1. Choose “Basic Network Scan”
	2. Name the policy “Custom.”
	3. Under the category “Discovery,” change the “Scan Type” to “All ports.”
	4. Under “Assessment”, change the dropdown to “Scan for known web vulnerabilities.”
	5. Under “Advanced”, select Scan Type “Custom”. Then select “General” on the left. Uncheck “Enable safe checks.”
	6. Under the target field, enter the IP address of Metasploitable2: 192.168.55.102
	7. Save your new custom policy.
5. Click the “Scans” tab.
	1. Press the play icon for the custom scan you just created.



1. You should now see the scan job running. This should take about 10 minutes to complete. In the meantime, you can click the job to see the vulnerabilities that Nessus has found so far. Vulnerabilities can be sorted by severity.

**Questions:**

* Do you think it would be difficult to compromise this system? Explain.
* Which vulnerabilities are critical? Of these, which appear to be most serious? Double-click a vulnerability in the report and read the description.
* What would be the first thing you would do to secure this system?
* **Consider:** What would be the first thing you would do to secure this system?