Lab 3: Scanning and Reconnaissance

Introduction

The key to successfully exploit or intrude a remote system is about the information you have. The first step for penetration is the scanning and reconnaissance. In this lab, you will learn how to use tools to scan and retrieve information from a targeting system. You will be using nmap and OpenVAS to scan a vulnerable machine and identify exploits that can be used to attack it. We will use two Linux virtual machines: One is a Kali Linux with nmap and OpenVAS installed; and the other one is intentionally vulnerable Linux. We will use the nmap and OpenVAS on Kali Linux to scan the vulnerable Linux machine.

Software Requirements

- The VMWare Software
  http://apps.eng.wayne.edu/MPStudents/Dreamspark.aspx

- The Kali Linux, Penetration Testing Distribution
  https://www.kali.org/downloads/

- Metasploitable2: Vulnerable Linux Platform
  http://sourceforge.net/projects/metasploitable/files/Metasploitable2/

- nmap: the Network Mapper - Free Security Scanner
  https://nmap.org/

- OpenVAS: Open Vulnerability Assessment System
  http://www.openvas.org/index.html
Starting the Lab 3 Virtual Machines

We need to use two VMs for this lab: the Kali Linux and the Metasploitable2-Linux.

First, select the Kali Linux and press Start up.

Login the Kali Linux with username root, and password [TBA in the class]. Below is the screen snapshot after login.
Then, you select **Metasploitable2-Linux**, and press Start up. This is an intentionally vulnerable Linux VM that you will attack against.

If you see the window below, just click OK. This is due to running two VM at the same time.
Log into the virtual machine with username, msfadmin, and password [TBA in Class].

After you log into the VM, you will see the screen below.
Finding the IP Address of the Attacking Target

For the purpose of this lab, it uses Metasploitable2-Linux as the attacking target. First, we need to find the host IP address of the target to launch a scanning. You can use the command “ifconfig” (ipconfig is the windows equivalent). This command allows you to find all the connected interfaces and network cards.

Go to the Metasploitable2-Linux VM, and execute the following command

$ ifconfig

From the screenshot above, we can see that the IP address of the network interface, eth0, is **172.16.108.172**. This is the IP address for the target that you will use later in this lab. When you work on the lab in the classroom, you will get a different IP address for your Metasploitable2-Linux VM. Note that this is not a public IP but we can access it within the subset.
Scanning the Target Using nmap

nmap ("Network Mapper") is an open source tool for network exploration and security auditing. Though it was designed to rapidly scan large networks, we use it for scanning the target host in this lab.

Go to the Kali Linux, and open up a terminal by clicking the icon.

Since nmap has been installed on the Kali Linux, we can just launch the scanning in the terminal by typing the following command:

```
$ nmap -T4 172.16.108.172
```

nmap is the execution command; option -T4 means faster execution; and 172.16.108.172 is the IP address of the target. As mentioned, you will have a different IP address when working on this with the VMs in the classroom.
The screenshot above shows a quick scan of the target machine using **nmap**. We can see that there are many open ports and services on the target system including FTP, SSH, HTTP, and MySQL. These services may contain vulnerabilities that you can exploit.

**nmap** provides many useful functions that we can use. You can find more information from the man page of **nmap**

From this link: [http://linux.die.net/man/1/nmap](http://linux.die.net/man/1/nmap)

Or execute the following command in a terminal:

```
$ man nmap
```
The screenshot above shows the man page of `nmap`.

<table>
<thead>
<tr>
<th>NAME</th>
<th>Nmap Reference Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYNOPSIS</td>
<td>nmap - Network exploration tool and security / port scanner</td>
</tr>
<tr>
<td>DESCRIPTION</td>
<td>Nmap (&quot;Network Mapper&quot;) is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.</td>
</tr>
</tbody>
</table>

The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key among that information is the "interesting ports table". That table lists the port number and protocol, service name, and state. The state is either open, filtered, closed, or unfiltered. Open means that an application on the target machine is listening for connections/packets on that port. Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed. Closed ports have no application listening on them, though they could open up at any time. Ports are classified as unfiltered when they are responsive to Nmap's probes, but Nmap cannot determine whether they are open or closed. Nmap reports the state combinations open|filtered and closed|filtered when it cannot determine which of the two states describe a port. The port.
Vulnerability Scanning Using OpenVAS

OpenVAS is an open-source framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. In our Kali Linux image, OpenVAS has been installed and setup for you.

If you want to setup OpenVAS in your own machine, you can follow the steps below.

```
root@kali:~# apt-get update
root@kali:~# apt-get dist-upgrade
root@kali:~# apt-get install openvas
root@kali:~# openvas-setup
```

Since the Kali Linux image has everything setup for you, you don’t need to run the setup commands. You can run the following command to check if the OpenVAS manager, scanner, and GSAD services are listening:

```
root@kali:~# netstat –antp
```

Otherwise, just start the services by executing the following command

```
root@kali:~# openvas-start
```
Connecting to the OpenVAS Web Interface

Go to the Kali Linux, and open the browser, Iceweasel, by clicking the icon 🌐

Then, go to https://127.0.0.1:9392 and accept the self-signed SSL certificate.
Input the username as admin, and the password [TAB in the classroom].

The screenshot on next page is the homepage of OpenVAS. Type the IP address of the target in the “Quick start” box, and press “Start Scan”. It will do the following for you:

1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress
After finishing the scanning, you can look at the reports as shown in the screenshot below.
Assignments for the Lab 3

1. Read the lab instructions above and finish all the tasks.
2. Use nmap to scan the target and find the software version of the OS and the running services (list at least 3 of them).
3. Use OpenVAS to find two vulnerabilities of the target, and briefly describe them.

Happy Scanning!