Scanning and Reconnaissance

Instructor Note: The intent of this class is for MIDN to perform their own scanning and reconnaissance given nmap and OpenVAS.

MIDN should read the tool documentation as needed, and search the Internet for solutions to challenges they encounter. Some common challenges and their solutions are provided in the instructor notes below (not visible to the MIDN).

MIDN will most likely run into issues installing and configuring OpenVAS. The OpenVAS documentation is explicit, but there are plenty of forums dedicated to solving common pitfalls. MIDN must visit these and figure out any issues on their own. Some common pitfalls are described below for the Professor.

OpenVAS is no longer included by default with Kali Linux. To setup OpenVAS perform the following steps. Make sure you have the repository available in the sources.list file. **nano /etc/apt/sources.list**

And make sure the following line is present. If it is not, they should add it. **deb http://http.kali.org/kali kali-rolling main non-free contrib**

MIDN can now install OpenVAS with the following commands: **apt update**,**apt install openvas**,**openvas-setup**.

The openvas-setup command takes a while to complete, so MIDN should not become impatient. When it finishes running, MIDN need to copy the password into text editor and save. Most will not read the prompts and skip over this, which will require a rebuild. To rebuild the OpenVAS database they will need to execute the following command: **openvasmd –rebuild**.

This command will also take a while to complete. Once it completes, MIDN can access the web interface at **https://localhost:9392**. The username is **admin** and the password previously saved. If MIDN do not save the password they can Google how to change it via the Command Line. In short, they can execute:

- **openvas-stop**
- **openvasmd --create-user=admin --role=Admin**
- **openvasmd --user=admin --new-password=admin**
- **openvas-start**

Overview

The key to a successfully offensive cyber operation against a target system is about the information we have. The first step for penetration is the scanning and reconnaissance. In this lab, MIDN will learn how to use tools to scan and retrieve information from a targeting system. MIDN 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 and Windows XP. MIDN will use the nmap and OpenVAS on Kali Linux to scan the vulnerable Linux and Windows XP targets.

MIDN will need to complete the following steps:

- Launch Kali Linux VM (SY401_Kali_alpha)
- Launch Target VM's (Metasploitable Linux 2 and Windows XP) of your assigned group (SY401_GroupX_Metasploitable & WinXPsp1_Group#)
- Obtain Target IP Addresses (Metasploitable Linux 2 and Windows XP)
- Perform nmap scan - acquire screen captures of each target (Metasploitable Linux 2 and Windows XP)
- Install and configure OpenVAS
- Perform OpenVAS scan - acquire screen captures of each target (Metasploitable Linux 2 and Windows XP)
- Submit screen captures as your deliverable to the Professor (details below)
- Describe the difference between the nmap and OpenVAS output, and the scenarios by which each would be beneficial over the other.

MIDN should read the tool documentation, installation guides, and perform Internet searches to find solutions to challenges they encounter. The Professor will provide minimal assistance beyond what is provided below. Documentation can be found:

- Network Mapper (nmap)
- SANS Nmap Cheat Sheet
- OpenVAS

Each MIDN must login to their Kali Linux virtual machine (VM), and their respective Windows XP and Metasploitable VM's. Your VM's can be found by SY401_XP_ALPHA / SY401_META_ALPHA. The Professor will provide you the passwords to each VM.

Lab Deliverables

MIDN will submit a single PDF document to your Professor that contains the screenshots described below as your deliverable. The screenshots should be properly labeled. It is suggested that MIDN insert each of the required screenshots into a Microsoft Word document and export to a .PDF file. Here is a quad chart that summarizes the four deliverables:

Lab 3: Scanning and Reconnaissance
One set of deliverables per person

	OPEN VAS	NMAP
Metasploit Linux X Target	Screen Shot (deliverable)	Screen Shot (deliverable)
WIndows XP Target	Screen Shot (deliverable)	Screen Shot (deliverable)

- Windows XP vulnerability scan via Nmap (Screenshot of the terminal after command is successfully executed).
- Metasploitable Linux 2 vulnerability scan via Nmap (Screenshot of the terminal after command is successfully executed).
- Windows XP vulnerability scan via OpenVAS (Screenshot of the GUI results after successfully execution).
- Metasploitable Linux 2 vulnerability scan via OpenVAS (Screenshot of the GUI results after successfully execution).

The subject line of the email should be in the following format:

```
SY401 [Section Number]: [NAME OF LAB] (alpha)
```

For example:

```
SY401 1111: Lowering the Barrier to Entry - Open Source Tools (m123456)
```

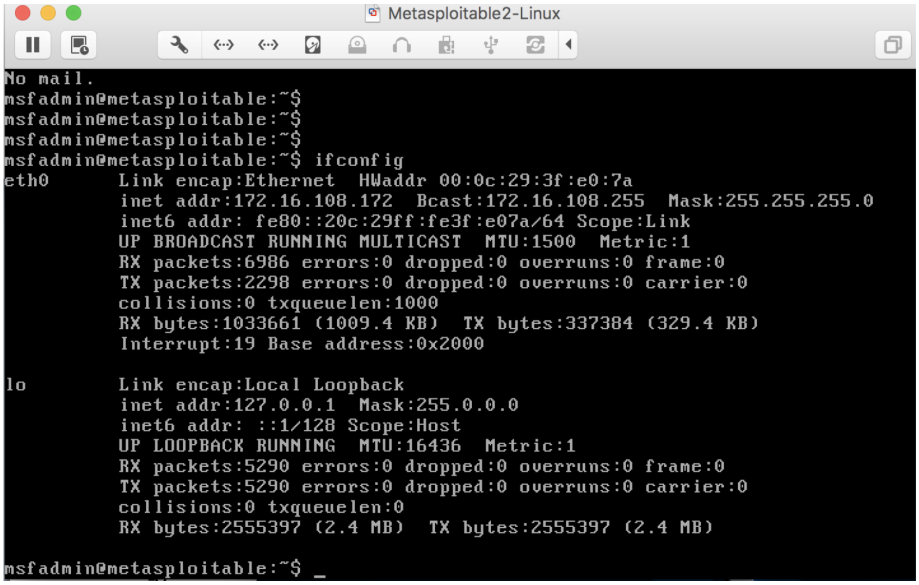
MIDN should gracefully shutdown their Virtual Machines (VMs) at the end of class, or whenever they are not using them. Failing to do so will result in a non-graceful shutdown from SY401 Faculty each day. Students risk losing work if this simple process is not followed.

Lab Hints/Solution:

Finding the IP Address of the Targets

For the purpose of this lab, we will use the Windows XP and Metasploitable2-Linux host as our targets. First, we need to find the hosts IP addresses to scan the targets. MIDN can use the command "ipconfig" (for Windows XP) and "ifconfig" (ipconfig is the UNIX equivalent). This command allows you to find all the connected interfaces and network cards.

The visual below highlights the results of the 'ifconfig' command being executed on the target machine.

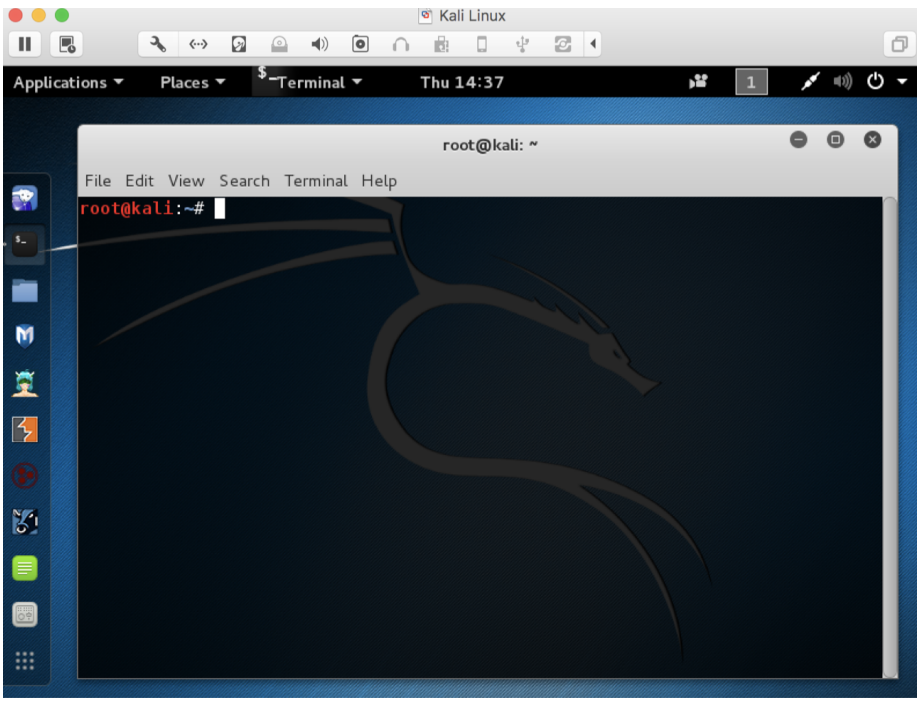


From the visual above, we can see that the IP address of the network interface, eth0, is 172.16.108.172. This is the IP address for the target that MIDN would use later in this lab. When MIDN work on the lab in the classroom, they will get a different IP address for their Windows XP and Metaploitable2-Linux virtual machines. 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.

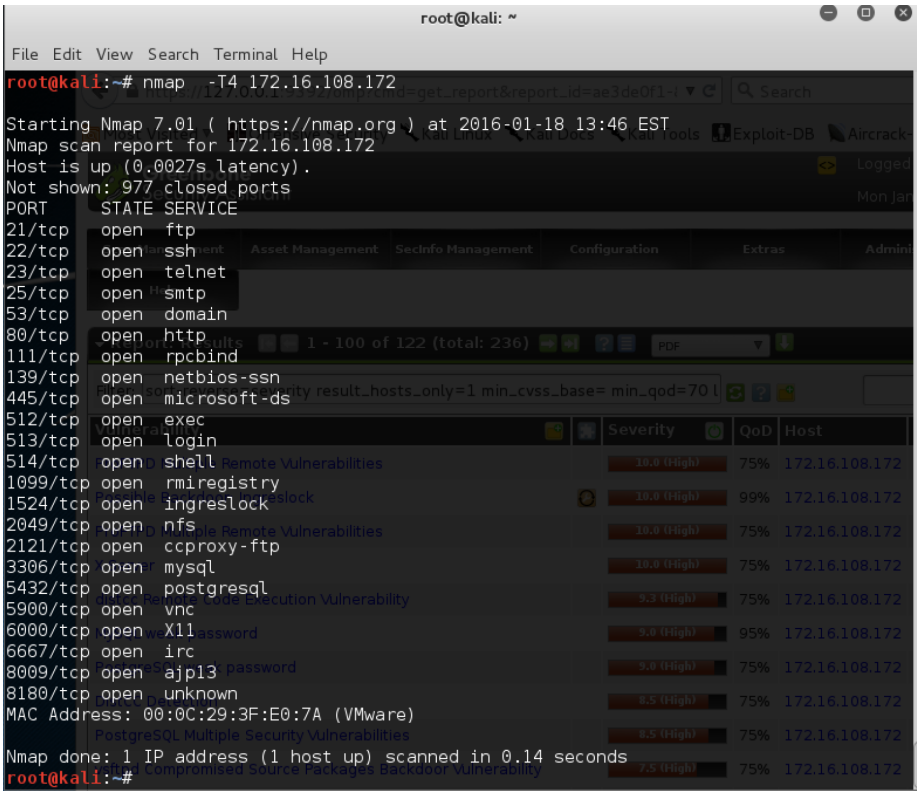
Go to the Kali Linux, and open up a terminal.



Since nmap has been installed on the Kali Linux, MIDN 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, MIDN will have a different IP address when working on this with the VMs in the lab environment.

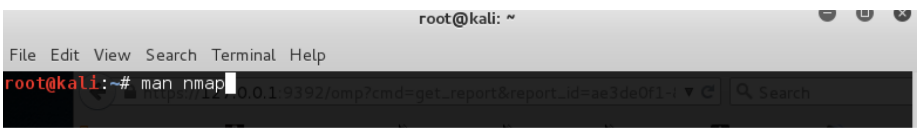


The screenshot above shows a quick scan of the target machine using nmap. MIDN can see that there are many open ports and services on the target system including FTP, SSH, HTTP, and MySQL. These services may contain vulnerabilities that can be exploited.

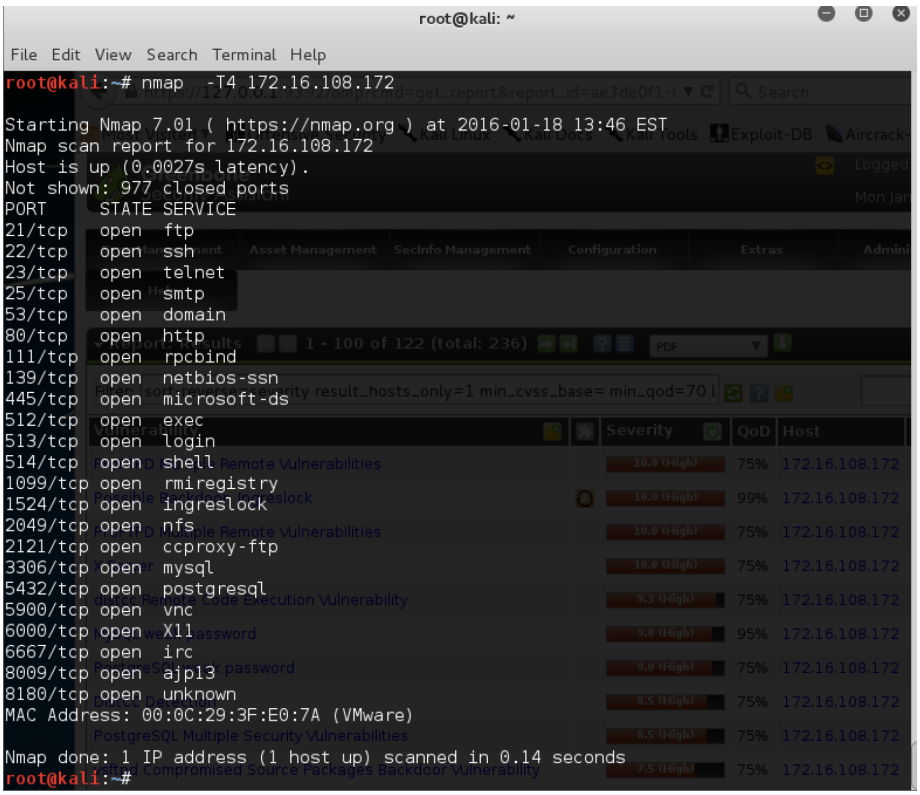
nmap provides many useful functions that can be used. MIDN can find more information from the man page of **nmap**.

Or execute the following command in a terminal:

```
man nmap
```



The visual below shows the man page of nmap.



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. MIDN will need to install and configure OpenVAS on their Kali Linux virtual machine.

MIDN should run the following commands to install OpenVAS.

```
apt-get update
apt-get dist-upgrade
apt-get install openvas
openvas-setup
```

You can run the following command to check if the OpenVAS manager, scanner, and GSAD services are listening:

```
netstat –antp
```

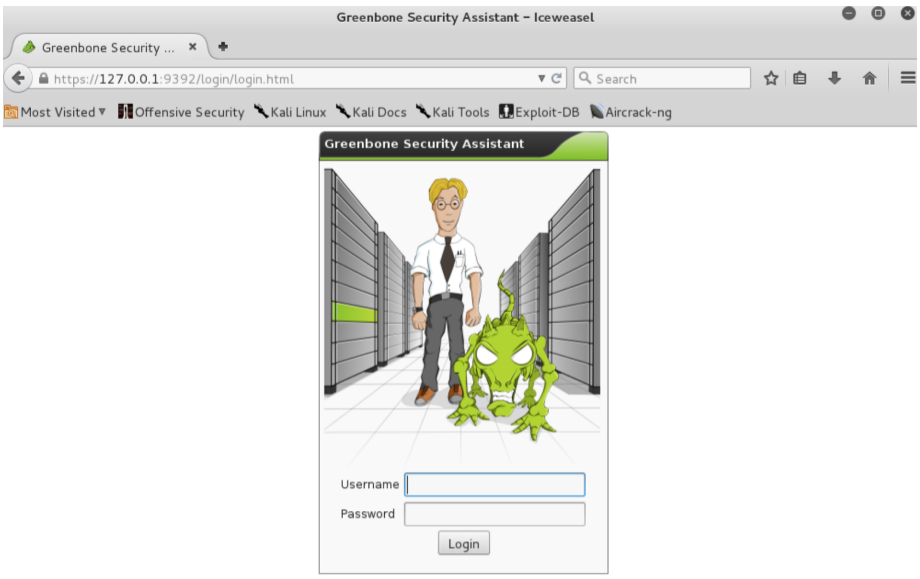
Otherwise, just start the services by executing the following command:

```
openvas-start
```

Next, go to the Kali Linux and open the browser.

Then, go to **https://127.0.0.1:9392** and accept the self-signed SSL certificate.

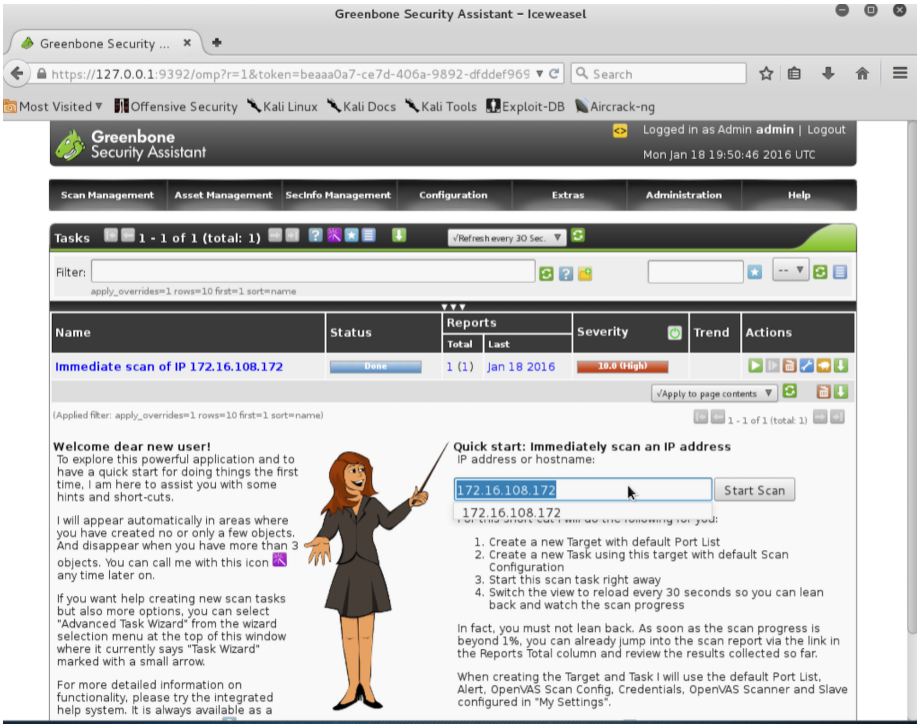
NOTE: If you are unsuccessful, visit online forums and troubleshoot until you are successful. The Professor will nudge you towards the solution, but not provide you the solution. You are successful when you receive a prompt similar to below:



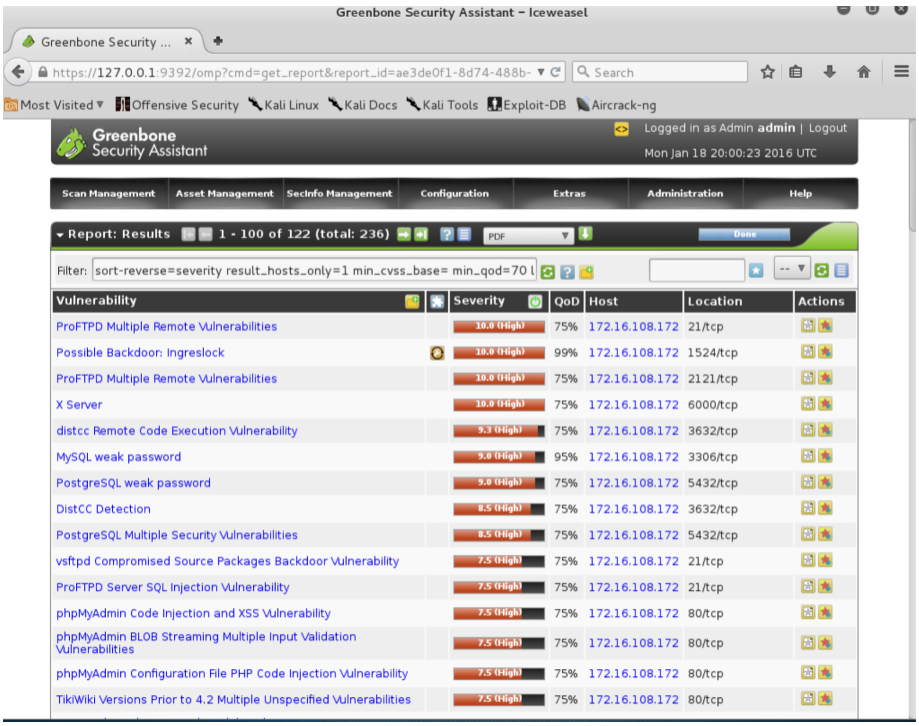
Input the username as admin, and the password, which was generated when you installed/configured OpenVAS.

The visual below 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:

- Create a new Target with default PortList.
- Create a new Task using this target with default Scan Configuration.
- Start this scan task right away.
- 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 visual below.



References

1. OpenVAS - OpenVAS - Open Vulnerability Assessment System. (n.d.). Retrieved February 20, 2018, from http://openvas.org/

2. (n.d.). Retrieved February 20, 2018, from http://www.openvas.org/setup-and-start.html

3. OpenVAS 8.0 Vulnerability Scanning. (2015, April 27). Retrieved February 20, 2018, from https://www.kali.org/penetration-testing/openvas-vulnerability-scanning/

4. Thread: What is default 'admin' password after installing openVAS. (n.d.). Retrieved February 20, 2018, from https://forums.kali.org/showthread.php?23212-What-is-default-admin-password-after-installing-openVAS