ETHICAL HACKING
LAB SERIES

Lab 1: Reconnaissance with Nmap & Amap

Material in this Lab Aligns to the Following Certification Domains/Objectives		
Certified Ethical Hacking (CEH) Domains	Offensive Security (PWK) Objectives	SANS GPEN Objectives
2: Footprinting and Reconnaissance 3: Scanning Networks	3: The Essential Tools (netcat, ncat, wireshark, tcpdump) 6: Trojans and Backdoors	7: Intel Target Scanning 15: Scanning for Targets

Document Version: 2016-03-09

Contents

Introduction

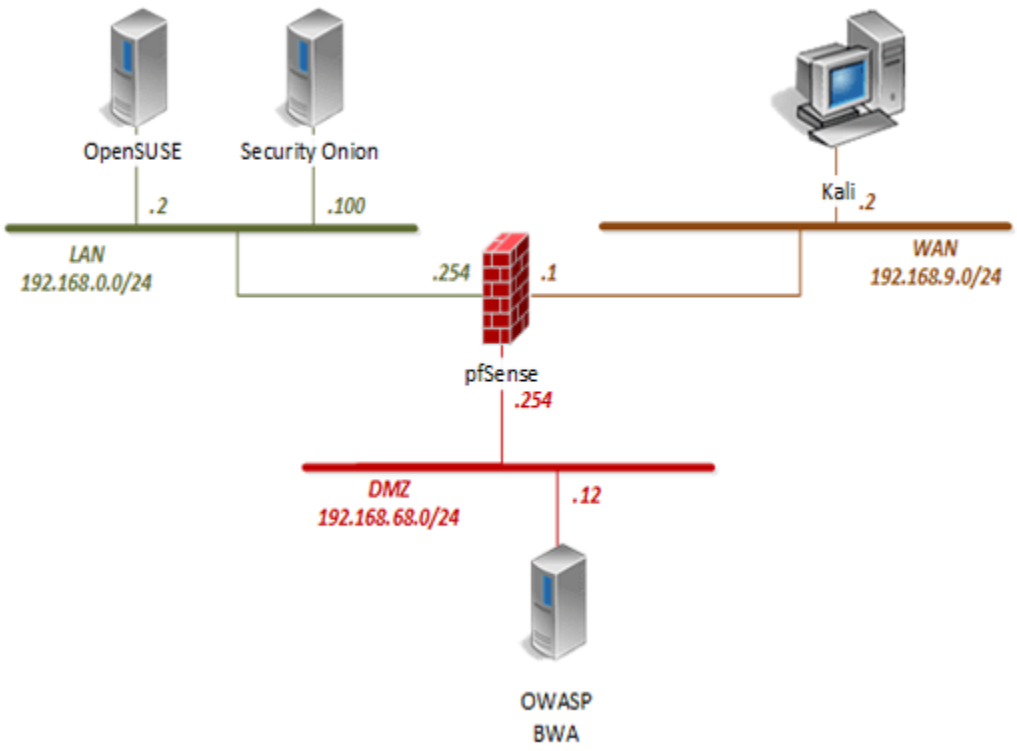
This lab introduces *Nmap* the "network mapper" and its usage to perform basic network port reconnaissance and scanning. Additionally, the use of the *Amap* "application mapper" tool in order to determine which applications are running on listening ports.

Objective

In this lab, you will be conducting ethical hacking practices using various tools. You will be performing the following tasks:

1. Reconnaissance Using Nmap
2. Using Amap for Reconnaissance

Pod Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Kali Linux	192.168.9.2	root	toor
pfSense	192.168.0.254 192.168.68.254 192.168.9.1	admin	pfsense
OWASP Broken Web App	192.168.68.12	root	owaspbwa
OpenSUSE	192.168.0.2	osboxes	osboxes.org
Security Onion	192.168.0.100	ndg	password123

1 Reconnaissance Using Nmap

1. Click on the **Kali** graphic on the *topology page*.
2. Click anywhere within the Kali console window and press **Enter** to display the login prompt.
3. Enter `root` as the *username*. Click **Next**.
4. Enter `toor` as the *password*. Click **Sign In**.
5. Open a new terminal by clicking on the **Terminal** icon located on the left panel.

6. Open and review *Nmap's* manual by typing the command below followed by pressing **Enter**.

```
man nmap
```

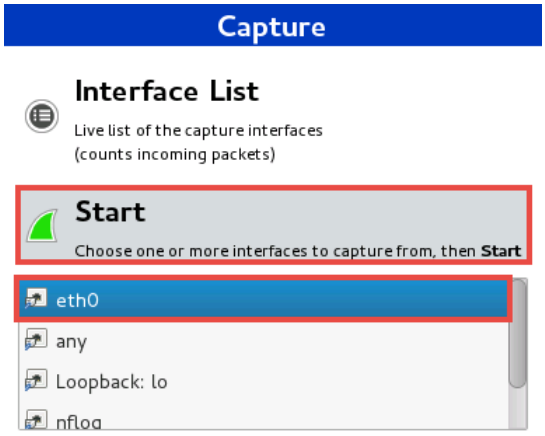
Nmap has many options, including its own scripting engine. Review the man pages to get familiar with the switches and options. Press the **Spacebar** to go to the next page or press **Enter** to go to the next line.

7. Once finished reviewing the man page, press the **Q** character to quit and bring the shell prompt back.
8. Launch *Wireshark* to observe what happens when a scan is triggered. Type the command below followed y pressing **Enter**.

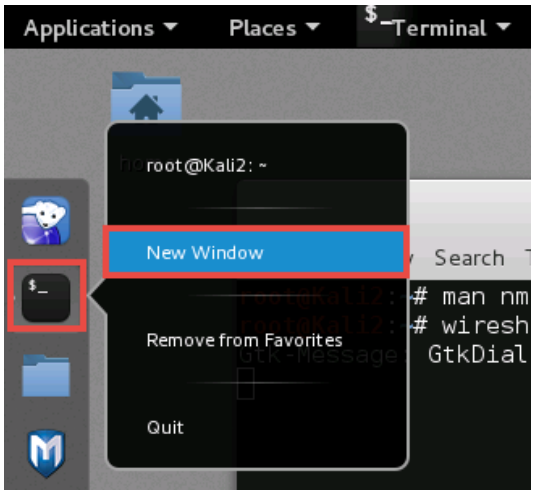
```
wireshark
```

If an error message appears, click **OK** to continue.

9. In the *Capture* panel, select **eth0** from the list and click **Start**.



10. Minimize the **Wireshark** window.
11. On the *Desktop*, right-click the **Terminal** icon in the left pane and select **New Window**.



12. In the new *Terminal* window, initiate a general *Nmap* scan with no options.

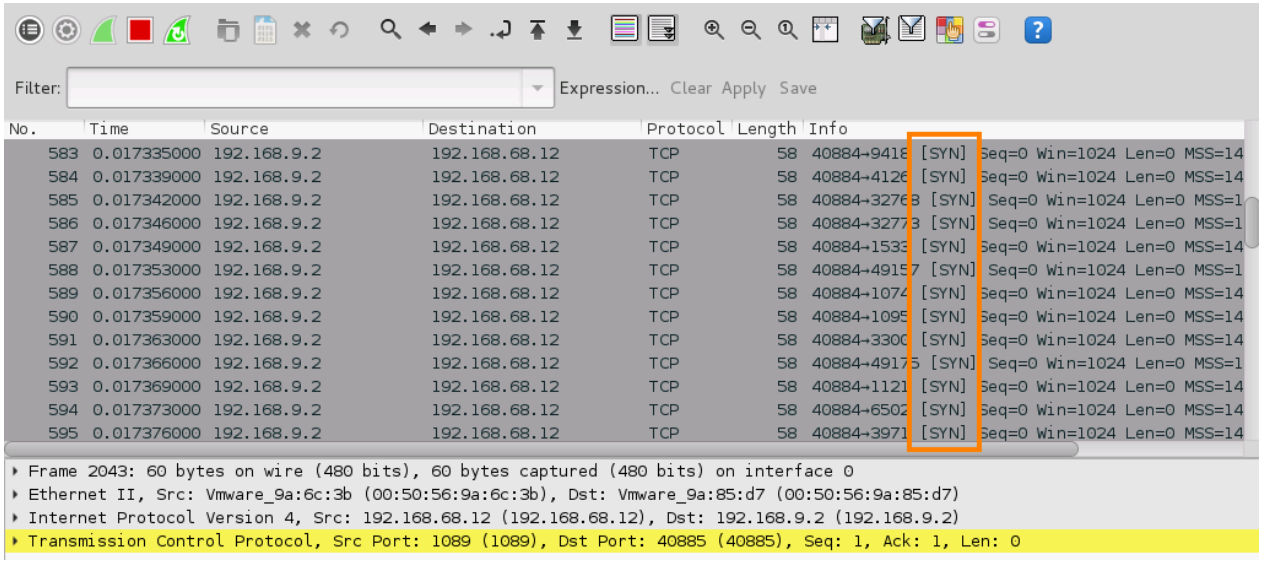
```
nmap 192.168.68.12
```

Press **Enter** and wait for the scan to complete.

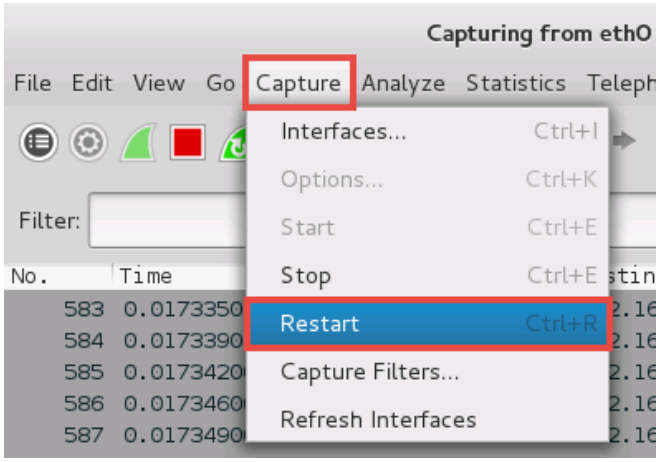
```
root@Kali2:~# nmap 192.168.68.12

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-12-15
mass_dns: warning: Unable to determine any DNS servers. Rev
 Try using --system-dns or specify valid servers with --dns
Nmap scan report for 192.168.68.12
Host is up (0.0043s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
5001/tcp open  commplex-link
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 1.20 seconds
```

13. Navigate back to the *Wireshark* window by clicking on the **Wireshark** icon located in the left panel.

14. Scroll through the Wireshark output and notice how *Nmap* uses *[SYN]* flags against all the ports to see if they are open or closed.



15. Clear the Wireshark scan results by clicking on the **Capture** menu item followed by clicking on **Restart**.

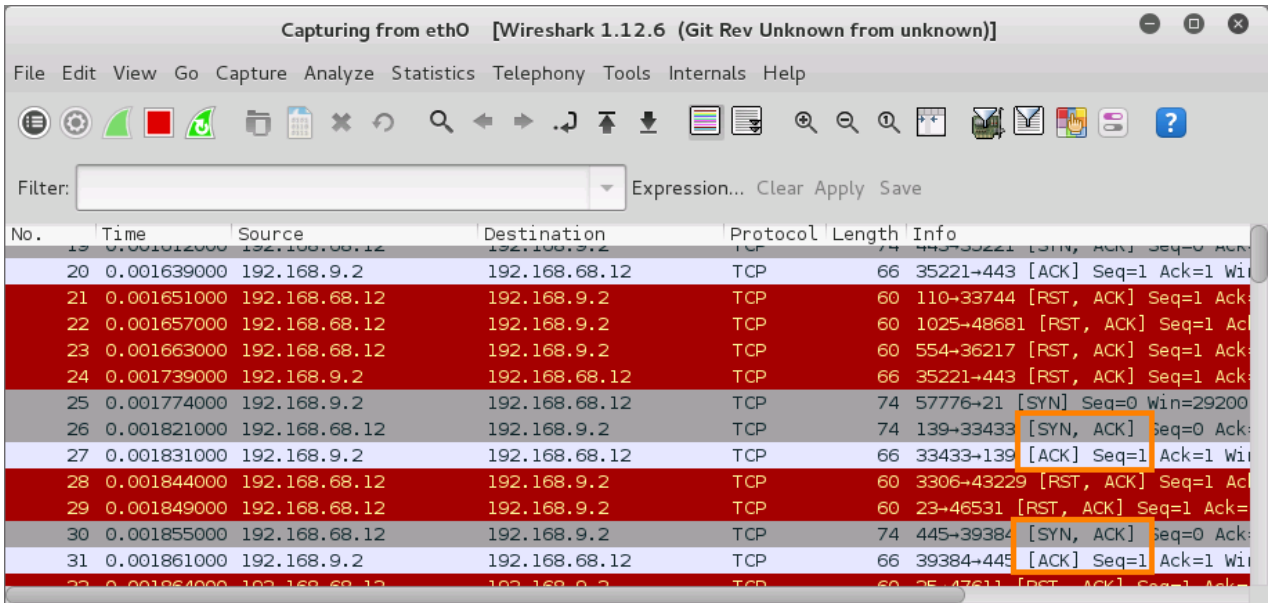


16. Minimize the **Wireshark** window.
17. Navigate back to the **Terminal** that the *Nmap* scan was initiated from, if closed, open a new **Terminal**.
18. This time, initiate a specific *TCP* connect scan. Type the command below followed by pressing **Enter**.

```
nmap -sT 192.168.68.12
```

19. Once the scan is completed, navigate back to the **Wireshark** window.

20. In the given *Wireshark* output, notice a few connections are being attempted using *[SYN, ACK]* followed by a *[SYN]*.



21. Minimize **Wireshark**.
22. Navigate back to the **Terminal** that the *Nmap* scan was initiated from, if closed, open a new **Terminal**.
23. *Nmap* scans can be noisy at times with its default port scanning range. Limit *Nmap* to only scan to the most popular ports by initiating the command below.

```
nmap -F 192.168.68.12
```

24. Use *Nmap* to try to identify versions of software running on the ports. Type the command below followed by pressing **Enter**.

```
nmap -A 192.168.68.12
```

25. Notice a lot more information is given about the target machine. *Nmap* has a set of scripts installed we can use to test for vulnerabilities. Initiate the command below to run a general set of default scripts.

```
nmap -sC 192.168.68.12
```

Notice *Nmap* tries a set of scripts against the target to look for some general vulnerabilities.

26. Leave the Terminal window for the next task.

2 Using Amap for Reconnaissance

1. Using the same Terminal window, open and review *Amap's* manual by typing the command below followed by pressing **Enter**.

```
man amap
```

Amap has many options. Review the man pages to get familiar with the switches and options. Press the **Spacebar** to go to the next page or press **Enter** to go to the next line.

2. Once finished reviewing the man page, press the **Q** character to quit and bring the shell prompt back.
3. From the previous task, using *Nmap*, the open ports are known. Initiate an *Amap* scan against port **80** by typing the command below followed by pressing **Enter**.

```
amap -A 192.168.68.12 80
```

```
root@Kali2:~# amap -A 192.168.68.12 80
amap v5.4 (www.thc.org/thc-amap) started at 2015-12-15
PPING mode

Protocol on 192.168.68.12:80/tcp matches http
Protocol on 192.168.68.12:80/tcp matches http-apache-2

Unidentified ports: none.

amap v5.4 finished at 2015-12-15 10:46:27
```

4. Using the same scan type, initiate a scan against port **22** by typing the command below. Press Enter.

```
amap -A 192.168.68.12 22
```

5. Initiate a banner grabbing command for port **22**.

```
amap -B 192.168.68.12 22
```

```
root@Kali2:~# amap -B 192.168.68.12 22
amap v5.4 (www.thc.org/thc-amap) started at 2015-12-15 10:49:40 - BANNER mode

Banner on 192.168.68.12:22/tcp : SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu4\r\n

amap v5.4 finished at 2015-12-15 10:49:40
```

Notice the complete version number displayed from the banner grab technique. *Amap* is known to be a powerful reconnaissance tool.

6. Close the **Kali** PC viewer.

