ETHICAL HACKING V2
LAB SERIES

Lab 03: Reconnaissance with Nmap/Zenmap and Masscan

Document Version: 2020-08-24

Material in this Lab Aligns to the Following	
Books/Certifications	**Chapters/Modules/Objectives**
All-In-One CEH Chapters ISBN-13: 978-1260454550	3: Scanning and Enumeration
EC-Council CEH v10 Domain Modules	3: Scanning Networks 4: Enumeration
CompTIA Pentest+ Objectives	2.1 Given a scenario, conduct information gathering using appropriate techniques 4.1 Given a scenario, use Nmap to conduct information gathering exercises 4.2: Compare and contrast various use cases of tools
CompTIA All-In-One PenTest+ Chapters ISBN-13: 978-1260135947	2: Getting to Know Your Targets 3: Network Scanning and Enumeration

Contents

Introduction

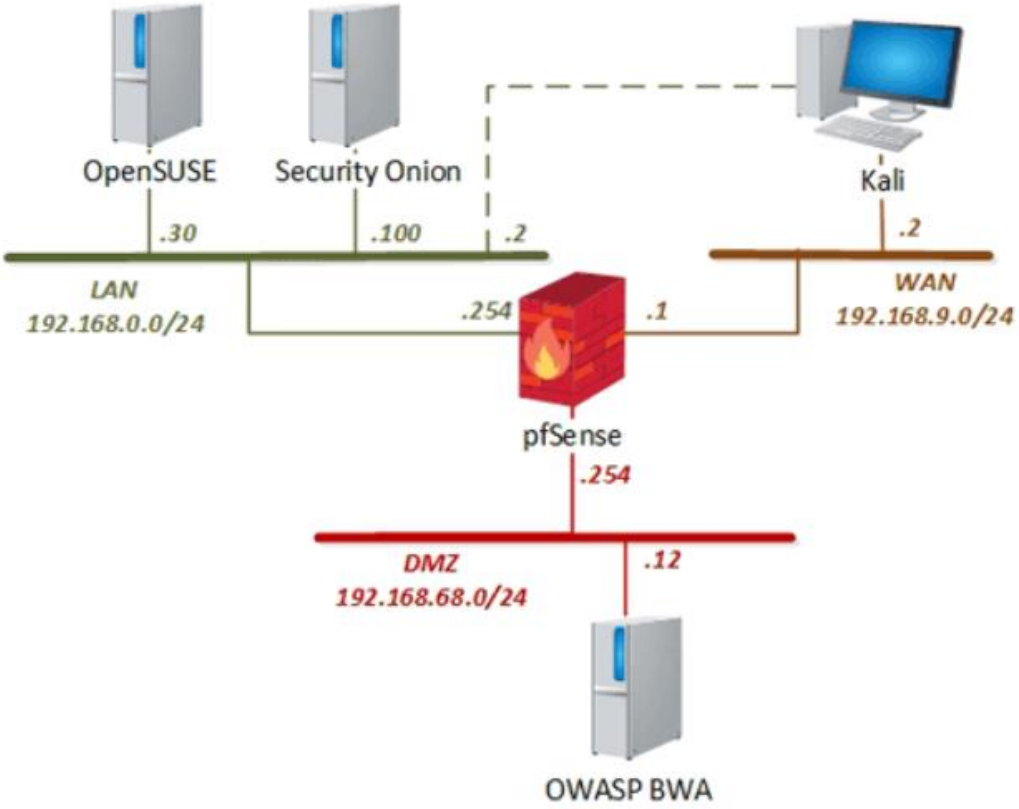
This lab introduces *Nmap* the "network mapper" and its usage to perform basic network port reconnaissance and scanning. You will also explore the GUI version, *Zenmap*, and its benefits. Finally, you will compare these two to the speed of *masscan*.

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. Reconnaissance Using Zenmap
3. Reconnaissance Using masscan

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	192.168.9.2 192.168.0.2	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	192.168.0.30	osboxes	osboxes.org
Security Onion	192.168.0.100	ndg	password123

1 Reconnaissance Using Nmap

Nmap is a utility for network discovery and security auditing. There are many options available with Nmap, allowing it to be flexible and powerful at the same time.

1. Click on the **Kali** tab.
2. Click within the console window and press **Enter** to display the login prompt.
3. Enter **root** as the *username*. Press **Tab**.
4. Enter **toor** as the *password*. Click **Log In**.
5. Open a new terminal by clicking on the **Terminal** icon located at the top of the page, if the terminal is not already opened.
6. Before you begin, you will need to disable the Docker service on this machine as it interferes with this lab. Failure to do so will cause a segmentation fault on step 11. To disable the Docker service, type the command below, followed by pressing **Enter.**

```
systemctl stop docker
```

```
root@kali:~# systemctl stop docker
root@kali:~#
```

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

```
man nmap
```

```
NMAP(1)                         Nmap Reference Guide                         NMAP(1)

NAME
       nmap - Network exploration tool and security / port scanner

SYNOPSIS
       nmap [Scan Type ...] [Options] {target specification}

DESCRIPTION
       Nmap ("Network Mapper") 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.
Output omitted...
```

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.

8. Once finished reviewing the man page, press the **Q** character to quit and bring the shell prompt back.

9. In the *Terminal* window, initiate a general *Nmap* scan on the OWASP BWA machine, with no options.

```
nmap 192.168.68.12
```

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

```
root@kali:~# nmap 192.168.68.12
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-26 16:29 EDT
Nmap scan report for 192.168.68.12
Host is up (0.00057s 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 1.31 seconds
root@kali:~#
```

10. This time, initiate a specific *TCP* connect scan. Type the command below, followed by pressing **Enter**.

```
nmap -sT 192.168.68.12
```

```
root@kali:~# nmap -sT 192.168.68.12
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-26 16:36 EDT
Nmap scan report for 192.168.68.12
Host is up (0.49s 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 1.21 seconds
root@kali:~#
```

Notice the results are not different as the host only has TCP ports open.

11. *Nmap* scans can be noisy at times with its default port scanning range. Limit *Nmap* to only scan the most popular ports by initiating the command below.

```
nmap -F 192.168.68.12
```

```
root@kali:~# nmap -F 192.168.68.12
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-26 16:47 EDT
Nmap scan report for 192.168.68.12
Host is up (0.00056s latency).
Not shown: 92 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
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 1.27 seconds
root@kali:~#
```

Notice that port 5001 is missing from this output. This is a non-standard port.

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

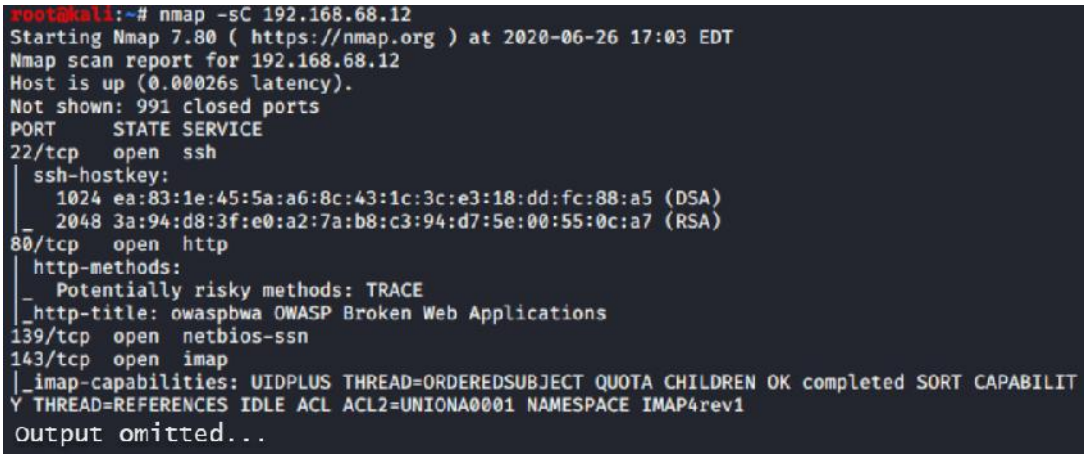
```
nmap -A 192.168.68.12
```

```
root@kali:~# nmap -A 192.168.68.12
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-26 16:51 EDT
Nmap scan report for 192.168.68.12
Host is up (0.00036s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ea:83:1e:45:5a:a6:8c:43:1c:3c:e3:18:dd:fc:88:a5 (DSA)
|_  2048 3a:94:d8:3f:e0:a2:7a:b8:c3:94:d7:5e:00:55:0c:a7 (RSA)
80/tcp   open  http        Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30
 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL ... )
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosi
n-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_
Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
|_http-title: owaspbwa OWASP Broken Web Applications
Output omitted...
```

Notice there is more information about the target machine. This command will take some time to execute.

13. *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
```



This command may take some time to execute.

14. Leave the Terminal window open for the next task.

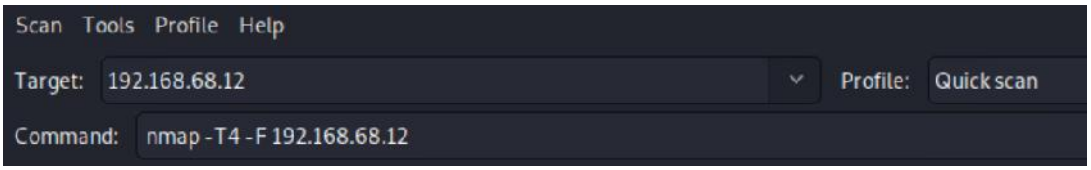
2 Reconnaissance Using Zenmap

Nmap is a very powerful tool and in the right hands, you can script different scans and work with the output. *Zenmap* is a GUI version of *Nmap* and allows you to get a better visual representation of the same information.

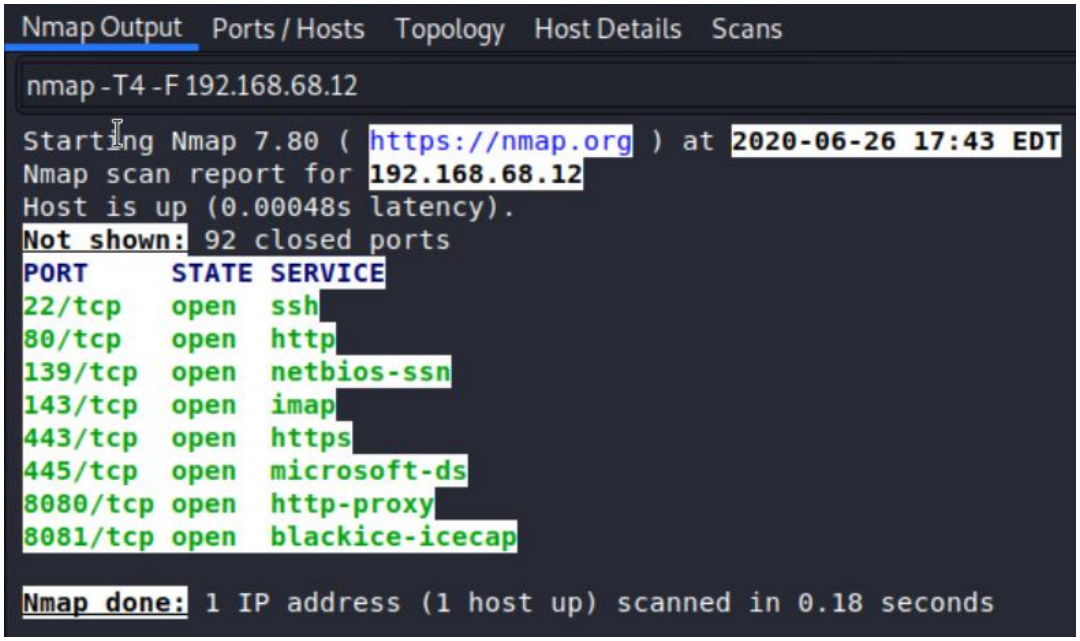
1. Using the same Terminal window, open *Zenmap* by typing the command below, followed by pressing **Enter.**

```
zenmap
```

2. In the *Target* field, enter **`192.168.68.12`** and select **Quick scan** from the Profile dropdown. Notice the *Command* field and compare it to what you did in the last task. Click **Scan** to begin.

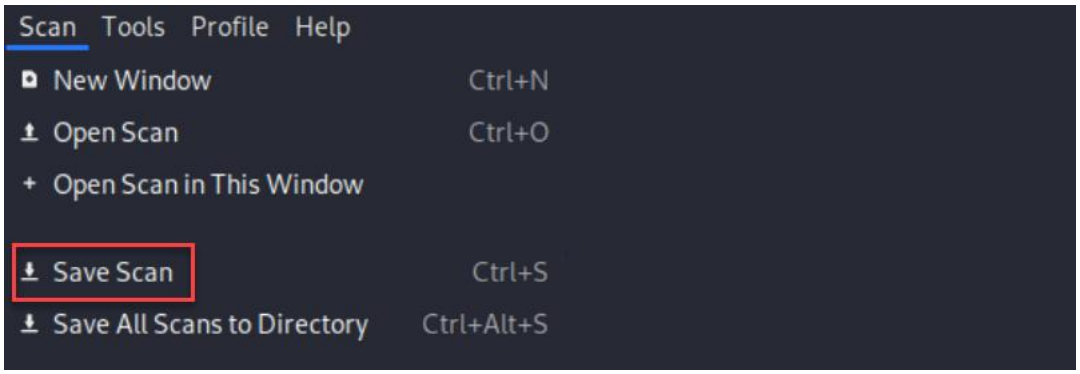


3. In the **Nmap Output** tab, note the output is similar to the command you ran earlier.



4. Click on the **Ports / Hosts** tab. Notice the clean, organized output.

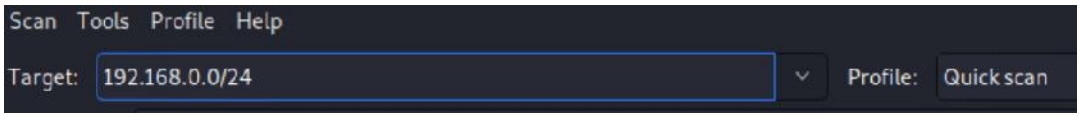
5. Click on **Scan** menu and then click **Save Scan.** This allows you to save the scan information for use later.



6. In the *Name* field, type **`scan1.xml`** and click the **Save** button in the lower-right.

> By saving the scan, you can load the results later. You can also combine multiple scans together to collect more information.

7. You can also scan an entire network. In the *Target* field, type **`192.168.0.0/24`** and click **Scan.** Leave the *Profile* field set to **Quick scan**.



8. On the left, notice the additional hosts that were found. You may need to expand the column to see the full IP addresses.

9. Click on the **Topology** tab. You can zoom in and change the view. This is helpful during an audit as you can save this image and add it to your report.

10. Click on the **Scans** tab. Notice the second scan is not saved. If you saved prior scans, you could load them in here, so you end up creating a database with all the information collected. In our case, notice that all the information you collected from both scans is combined.

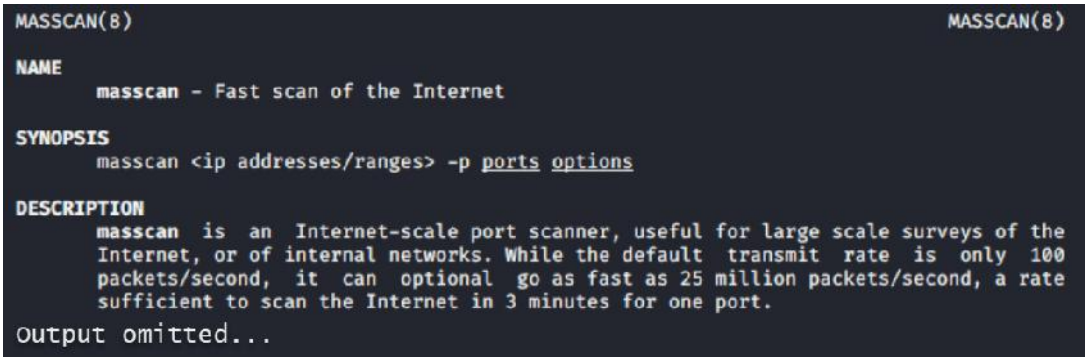
11. Click the **X** in the upper-right to close *Zenmap*. Click on **Close anyway** to ignore the results of the second scan.
12. You can leave the terminal window open for the next task.

3 Reconnaissance Using Masscan

Masscan is labeled as the "fastest Internet port scanner," capable of scanning the entire internet in under 6 minutes.

1. Open and review *masscan's* manual by typing the command below, followed by pressing **Enter**.

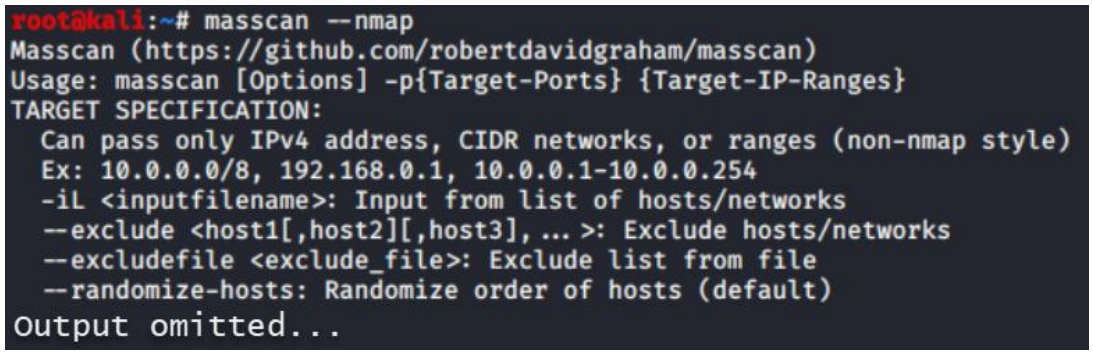
```
man masscan
```



Masscan 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. *Masscan* also has many nmap-like features. In the *Terminal* window, review these features by typing the following command, press **Enter,** and review the output:

```
masscan --nmap
```



4. To get started, let's do a simple scan of the 192.168.0.0/24 LAN network in our topology. We will only scan for devices that have port 80 open, using a TCP SYN scan technique. Type the following command, followed by pressing **Enter**:

```
masscan -sS 192.168.0.0/24 -p 80
```

```
root@kali:~# masscan -sS 192.168.0.0/24 -p 80

Starting masscan 1.0.6 (http://bit.ly/14GZzcT) at 2020-06-26 22:15:59 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 256 hosts [1 port/host]
Discovered open port 80/tcp on 192.168.0.254
Discovered open port 80/tcp on 192.168.0.30
root@kali:~#
```

Note the scan is over in a very short amount of time, there is just a delay at the end to allow for responses.

5. You may now end your reservation.

