Nmap for Scanning

When you perform a penetration test, the team will provide you a subnet, or a list of IP addresses for scanning. Scanning outside of the allowed list will cause issues such as bringing down production servers, affecting the performance of production servers. Scanning is to help you discover vulnerabilities on each of the scanned servers. You need to consider what arguments you should use for scanning. Even you are provided with the IP list, scanning them all at once may introduce unexpected problems (the router/switch or IPS/IDS cannot bear the load you deliver).

Before attacking any device, you will need to know the detail information of the device. Knowing the OS will help you find what vulnerabilities are available on that OS; knowing opened ports will help you know what services the device is offering

1. To find all live hosts in a network, use the below command and **take a screenshot of your findings.** This only uses the **`ping`** scan to discover the hosts; therefore, it is not too penetrative. Replace the network with your Kali's network

```
root@UMBkali:~# nmap -sP 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2018-
```

2. If you want to scan the whole network segment and exclude a specific IP address, use the following command and **take a screenshot** of your result. Replace the network with your Kali's network, and exclude your Win7 out of the scan

```
root@UMBkali:~# nmap -sS -PS --exclude 192.168.1.154 192.168.1.1/24
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-23 16:31 EST
Nmap scan report for 192.168.1.10
Host is up (0.0011s latency).
```

3. When having the result of live hosts, you are taking the next step to find more information. To find the OS version, run the following command with your target IP address, and **take a screenshot** of your findings. Make sure include the scanned time in your screenshot (in seconds)

```
root@UMBkali:~# nmap -sV 192.168.1.152
Starting Nmap 7.70 ( https://nmap.org )
```

4. If you want to set the amount of probes to use, you can use the argument **`--version-intensity`** . The more probes you use, the higher chance you will be discovered. **Take a screenshot** and note how many seconds **`nmap`** used to scan this

time? Is it shorter or longer than the previous step?

```
root@UMBkali:~# nmap -sV --version-intensity 2 192.168.1.152
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-23 15:20 EST
```

5. Another way to hide the **nmap** scan from being discovered is using the scan with *random* data. Packets generated by **nmap** scans usually just have the *protocol headers* set. To decrease the detection by security tools, **nmap** uses random data as payloads. Execute the following command and **take a screenshot of the result**

```
root@UMBkali:~# nmap -sS -PS --data-length 300 192.168.1.154
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-23 16:22 E
Nmap scan report for 192.168.1.154
Host is up (0.00089s latency).
```

6. When using **ping** scan, it does not perform port or service scan. Sometimes, the penetration tester knows what port he/she wants to scan for a specific vulnerability. To do that, execute the following command and **take a screenshot** of your result. This is to find if the device is offering direct TCP/IP network access service. This can be used for hacking at a later time.

```
root@UMBkali:~# nmap -p445 192.168.1.154
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-23 15:54 EST
Nmap scan report for 192.168.1.154
Host is up (0.00030s latency).
```

7. If you want to include more than 1 port in the scan, use the following command, and **take a screenshot of your result**

```
root@UMBkali:~# nmap -p445,80,443,139 192.168.1.154
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-23
Nmap scan report for 192.168.1.154
Host is up (0.00078s latency).
```

8. If you want a wider range, use the following command and **take a screenshot of your result**

```
root@UMBkali:~# nmap -p[1-1024] 192.168.1.154
Starting Nmap 7.70 ( https://nmap.org ) at 2018-
Nmap scan report for 192.168.1.154
Host is up (0.00038s latency).
```

Exercise 2: `nmap` with external vulnerability scanning script and database.

The default configuration of `nmap` provides the capability to check multiple flaws of the server. However, if we want to look further into what vulnerabilities the server is having, we will need to download additional `nse` scripts. The script was written by Marc Ruef to facilitate the vulnerability checking. Follow the below procedure to achieve the task.

1. Copy the `vulscan` folder from your Kali `/opt/vulscan` to the directory `/usr/share/nmap/scripts/vulscan` . If you practice on your own Kali, download the source from **github**:
   a.
   ```
   # git clone https://github.com/scipag/vulscan.git
   ```
   b. Copy the whole folder to the following directory and **take a screenshot of your directory**
   ```
   root@UMBkali:/usr/share/nmap/scripts/vulscan# ls
   _config.yml  exploitdb.csv  README.md          securitytracker.csv
   COPYING.TXT  openvas.csv    scipvuldb.csv      vulscan.nse
   cve.csv      osvdb.csv      securityfocus.csv  xforce.csv
   ```
2. Go to the directory and run the following command. **Take a screenshot of the success**
   ```
   root@UMBkali:/usr/share/nmap/scripts/vulscan# nmap -sV --script=vulscan/vulscan.
   nse --script-args vulscandb=securitytracker.csv 192.168.1.154 | more
   Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-25 16:06 EST
   ```
3. List all the vulnerabilities that you can find as following (the screenshot is one of many found vulnerabilities)
   ```
   |
   |_
   139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
   | vulscan: securitytracker.csv:
   ```
4. This list will help you know what vulnerabilities you can plan for attacks.
5. The last step in this exercise is running the script in the vulnerability category to see what we can attack. Run the following command and **take a screenshot** of your findings (replace the IP address with your Windows 7 IP address)
   ```
   root@UMBkali:/usr/share/nmap/scripts# nmap -sV --script vuln 192.168.1.154
   Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-25 16:45 EST
   Nmap scan report for 192.168.1.154
   ```

Zenmap exercise

1. Logon to your Kali, go to ***Application, Information Gathering***, and select ***Zenmap***
2. In the target box, put in your ***Win7*** IP address, select *Intense Scan* and click *Scan*
3. **Take a screenshot** of all open port the tool found
4. Go to *Host Details*, and **take a screenshot** of the information the tool discovered
5. Go back to the profile box, and select *Slow comprehensive scan*

6. What *differences* can you see between the intense scan and comprehensive scan? The scan will take a few minutes. When it finishes, the *high risk* ports should be listed in **green**. **Take a screenshot of the green list**
7. Look into the detail and **take a screenshot** of the **smb** version this device uses