

NMAP

Objective:

Learn how to scan a host using Nmap and understand the results.

Purpose:

Nmap (Network Mapper) is one of the most common tools used among hackers and system administrators. It is used to scan a host, which can be a server, pc, network, etc. When running an Nmap scan, the goal is usually to discover various pieces of information about a target system or network. Examples of such information include: the devices that are connected to a network, the ports that are open on a device, the services that are running on these ports, whether the device is up, and whether there is a firewall protecting the device, among others.

Tool:

Kali Linux

Topology:

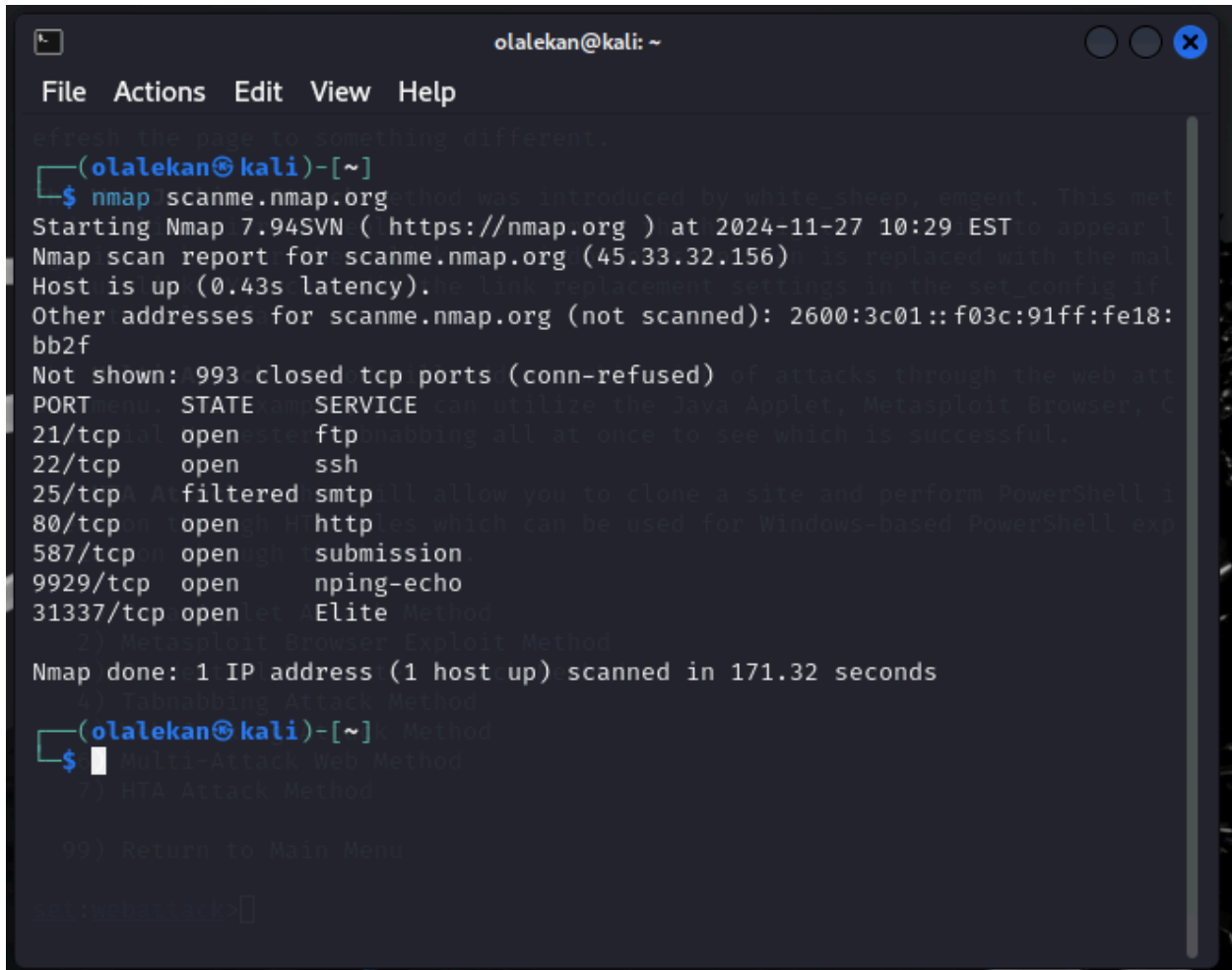
You can use Kali Linux in a virtual machine for the purpose of this lab. Scan the following site: scanme.nmap.org

Note: This site has been developed by Nmap for the purpose of scanning. Never scan any site, system, or network without prior permission from the owner.

Walkthrough:

Task 1:

Nmap comes pre-installed in Kali Linux. Just open a terminal, type “nmap scanme.nmap.org” without the inverted commas. This will initiate a scan of the target and will attempt to determine which ports are open and what services are open on these ports.



```
olalekan@kali: ~  
File Actions Edit View Help  
refresh the page to something different.  
(olalekan@kali)-[~]  
$ nmap scanme.nmap.org  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-27 10:29 EST  
Nmap scan report for scanme.nmap.org (45.33.32.156)  
Host is up (0.43s latency).  
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f  
Not shown: 993 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
25/tcp    filtered smtp  
80/tcp    open  http  
587/tcp   open  submission  
9929/tcp  open  nping-echo  
31337/tcp open  Elite Method  
Nmap done: 1 IP address (1 host up) scanned in 171.32 seconds  
(olalekan@kali)-[~]  
$
```

Task 2:

In this step, we will be scanning the same target, scanme.nmap.org, but with a more advanced scan. Let's say we want to determine the versions for the services running on each

port, so that we can determine if they are out of date and potentially vulnerable to exploitation. We also want to determine the operating system of the webserver running the target site. We will run the following scan to determine this information:

```
(olalekan@kali)-[~]: Exploit Method
$ nmap -v -sT -sV -O scanme.nmap.org
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!
[olalekan@kali]-[~]
$ sudo su -
[sudo] password for olalekan:
(root@kali)-[~]
#
```

```
root@kali: ~
File Actions Edit View Help
Initiating Connect Scan at 10:40
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 21/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 587/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
Increasing send delay for 45.33.32.156 from 0 to 5 due to 22 out of 73 dropped probes since last increase.
Connect Scan Timing: About 25.66% done; ETC: 10:42 (0:01:30 remaining)
Increasing send delay for 45.33.32.156 from 5 to 10 due to max_successful_try no increase to 4
Increasing send delay for 45.33.32.156 from 10 to 20 due to max_successful_try no increase to 5
Increasing send delay for 45.33.32.156 from 20 to 40 due to max_successful_try no increase to 6
Discovered open port 31337/tcp on 45.33.32.156
Connect Scan Timing: About 48.90% done; ETC: 10:42 (0:01:13 remaining)
Discovered open port 9929/tcp on 45.33.32.156
Connect Scan Timing: About 71.75% done; ETC: 10:42 (0:00:39 remaining)
Completed Connect Scan at 10:42, 157.47s elapsed (1000 total ports)
Initiating Service scan at 10:42
Scanning 6 services on scanme.nmap.org (45.33.32.156)
Completed Service scan at 10:42, 8.57s elapsed (6 services on 1 host)
Initiating OS detection (try #1) against scanme.nmap.org (45.33.32.156)
Retrying OS detection (try #2) against scanme.nmap.org (45.33.32.156)
NSE: Script scanning 45.33.32.156.
Initiating NSE at 10:43
```

```
root@kali: ~
File Actions Edit View Help

Initiating NSE at 10:43
Completed NSE at 10:43, 2.31s elapsed
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.49s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 993 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.4
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Lin
25/tcp    filtered smtp
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
587/tcp    open  smtp     Postfix smtpd
9929/tcp   open  nping-echo Nping echo
31337/tcp  open  tcpwrapped

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port587-TCP:V=7.94SVN%I=7%D=11/27%Time=67473DF8P=x86_64-pc-linux-gnu%r
SF:(NULL,48,"451\x20Request\x20action\x20aborted\x20on\x20MFE\x20proxy,\x2
SF:0SMTP\x20server\x20is\x20not\x20available\.\r\n");
Device type: general purpose
Running (JUST GUESSING): Linux 3.X|4.X (86%)
OS CPE: cpe:/o:linux:linux_kernel:3.8 cpe:/o:linux:linux_kernel:4.4
Aggressive OS guesses: Linux 3.8 (86%), Linux 4.4 (85%)
No exact OS matches for host (test conditions non-ideal).
```