Penetration Testing Report

TheCyberViking

Module 1

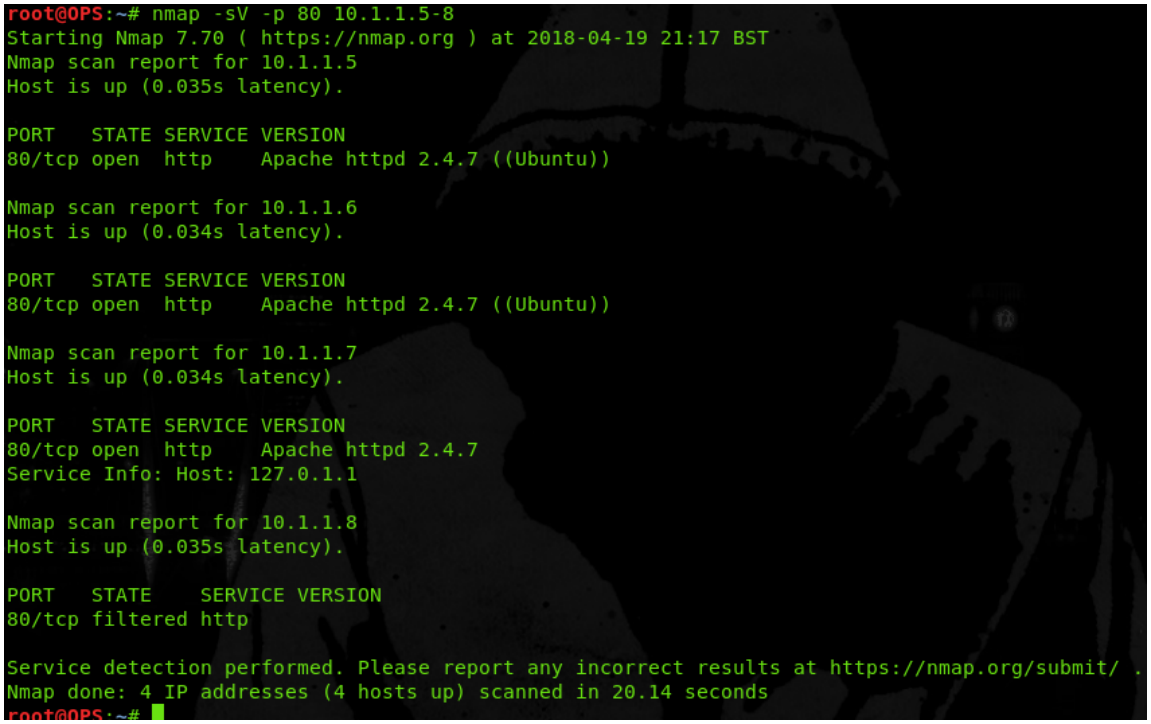
Exercise:

- **Task 1:** Scan all hosts in VIP lab for open port 80
- **Task 2:** Scan SKYWALKER and report all open ports on it, there is a firewall in-place.
- **Task 3:** Put together a report of open ports on each host and for SKYWALKER describe the method used for bypassing the firewall (insert screenshots of the commands used).

IP List:

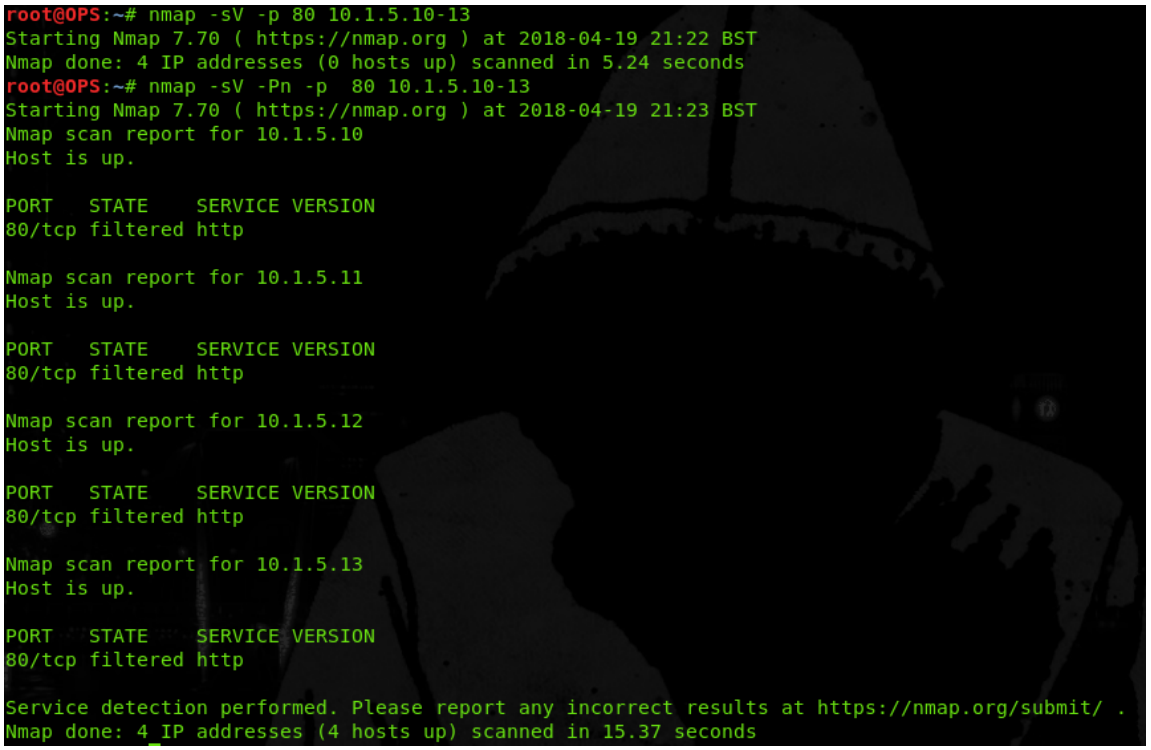
HOST	IP ADDRESS
MAGWITH	10.1.1.5
PALPATINE	10.1.1.6
SNAKE	10.1.1.7
ADDY	10.1.1.8
CLAUFIELD	10.1.5.10
CATHULHU	10.1.5.11
DOROTHY	10.1.5.12
STROBE	10.1.5.13
SAVITRI	10.1.2.20
ROBIN	10.0.2.244
SNIFFER	10.1.3.10
WEBSERVER	10.1.3.100
VICTIM	10.1.3.5
SKYWALKER	10.0.1.12

Scan range 10.1.1.5-8 = **nmap –sV –p 80 10.1.1.5-8**



Scan range 10.1.5.10-13 = **nmap –sV –p 80 10.1.5.10-13**

After trying the above scan for the range I received “0 hosts are available” since I could see the system are online through the web application, this could mean there is a possible firewall, I decided to give a passive scan the command I used was, **nmap –sV –Pn –p 80 10.1.5.10-13**



Scan IP address 10.1.2.20 = **nmap –sV –p 80 10.1.2.20**

```
root@OPS:~# nmap -sV -p  80 10.1.2.20
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-19 21:27 BST
Nmap scan report for 10.1.2.20
Host is up (0.033s latency).

PORT   STATE    SERVICE VERSION
80/tcp filtered http

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.76 seconds
```

Scan IP address 10.0.2.244 = **nmap –sV –p 80 10.1.2.244**

This command returned with a note “host seems down. If it is really up, but blocking our ping probes, try –Pn” this is similar to before so I ran the command **nmap –sV –Pn –p 80 10.1.2.244**

```
root@OPS:~# nmap -sV -p  80 10.1.2.244
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-19 21:28 BST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.23 seconds
root@OPS:~# nmap -sV -Pn -p  80 10.1.2.244
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-19 21:29 BST
Nmap scan report for 10.1.2.244
Host is up.

PORT   STATE    SERVICE VERSION
80/tcp filtered http

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.34 seconds
```

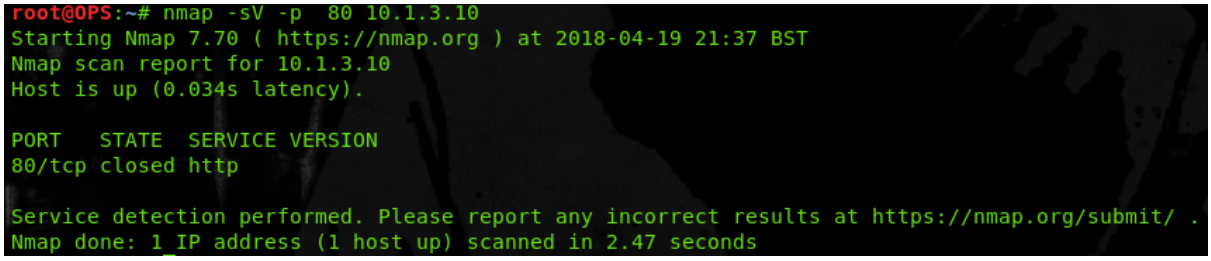
Scan IP address 10.1.3.5 = **nmap –sV –p 80 10.1.3.5**

```
root@OPS:~# nmap -sV -p  80 10.1.3.5
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-19 21:37 BST
Nmap scan report for 10.1.3.5
Host is up (0.031s latency).

PORT   STATE    SERVICE VERSION
80/tcp filtered http

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.74 seconds
```

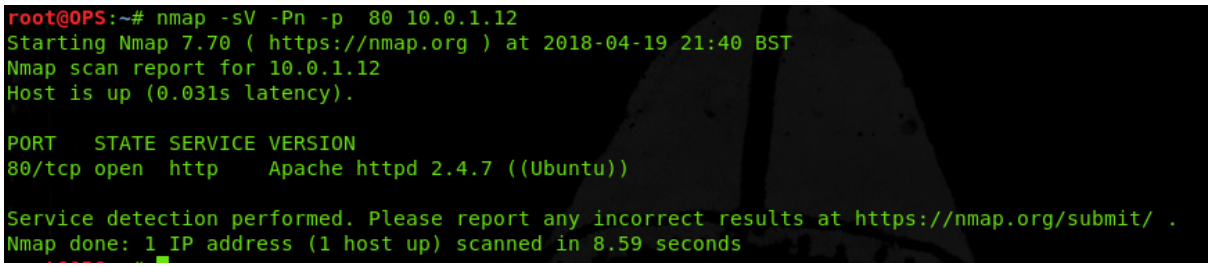
Scan IP address 10.1.3.5 = **nmap –sV –p 80 10.1.3.100**

```
root@OPS:~# nmap -sV -p 80 10.1.3.100
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-19 21:37 BST
Nmap scan report for 10.1.3.100
Host is up (0.031s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.71 seconds
```

Scan IP address 10.1.3.5 = **nmap –sV –p 80 10.1.3.10**



Finally a scan of SKYWALKER on IP address 10.0.1.12 since the scope said that SKYWALKER has a firewall I decided to make the scan passive with the follow command **nmap –sV –Pn –p 80 10.0.1.12**



Open Ports:

HOST	IP ADDRESS	Open Ports	Closed Ports	Filtered Ports
MAGWITH	10.1.1.5	80		
PALPATINE	10.1.1.6	80		
SNAKE	10.1.1.7	80		
ADDY	10.1.1.8			80
CLAUFIELD	10.1.5.10			80
CATHULHU	10.1.5.11			80
DOROTHY	10.1.5.12			80
STROBE	10.1.5.13			80
SAVITRI	10.1.2.20			80
ROBIN	10.0.2.244			80
SNIFFER	10.1.3.10		80	
WEBSERVER	10.1.3.100	80		
VICTIM	10.1.3.5			80
SKYWALKER	10.0.1.12	80		