Assignment 3

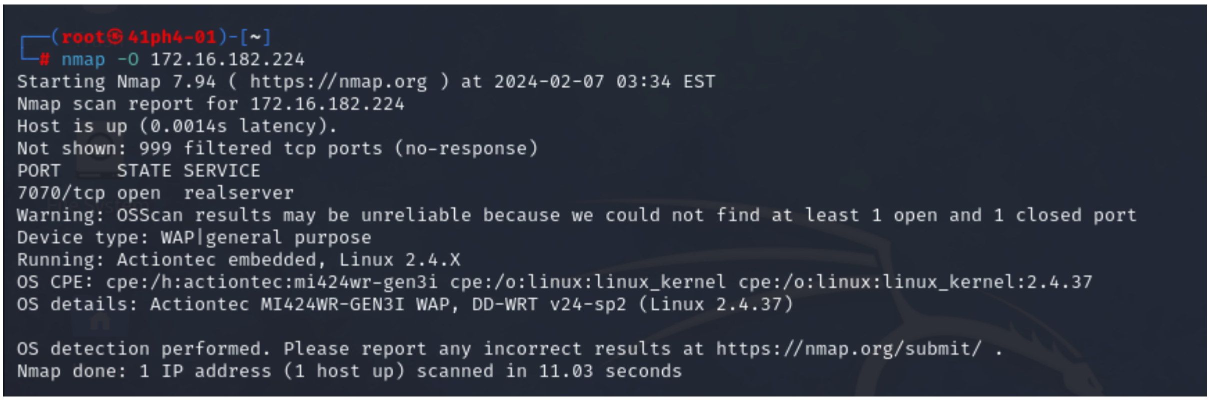
Title: obtain network services from an attacker’s perspective using Nmap

Theory:

1.syntax:- nmap -O <IP Address>

Command:-nmap -O 192.168.70.135

Output:-



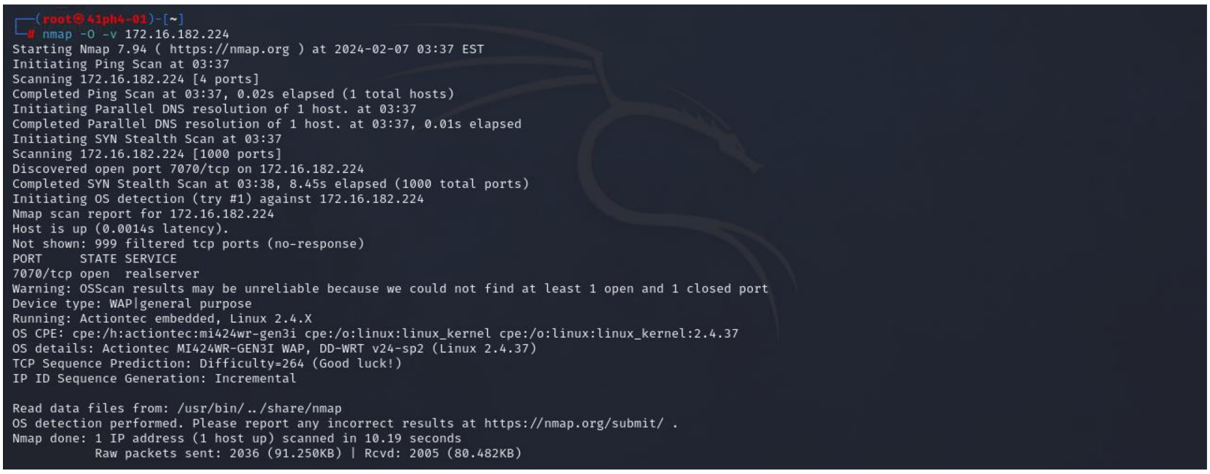
```
┌──(root㉿41ph4-01)-[~]
└─# nmap -O 172.16.182.224
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-07 03:34 EST
Nmap scan report for 172.16.182.224
Host is up (0.0014s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
7070/tcp open  realserver
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux 2.4.X
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37)

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.03 seconds
```

2.syntax:- nmap -O -v <IP Address>

Command:- nmap -O -v 192.168.70.135

Output:-



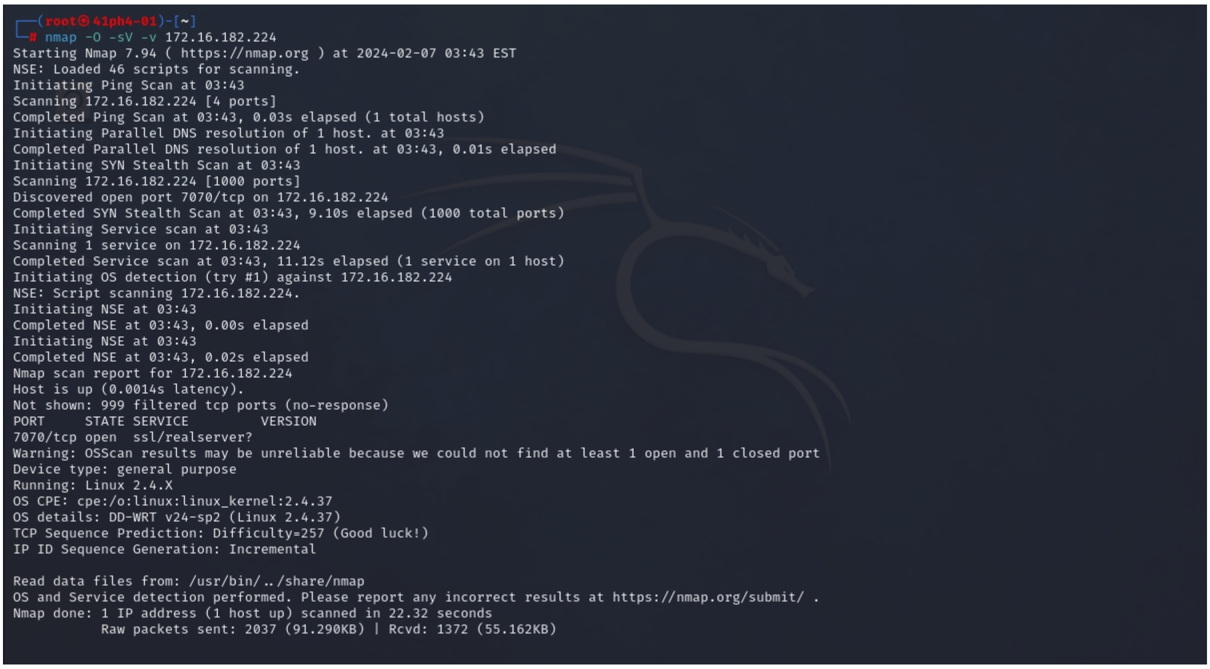
```
┌──(root㉿41ph4-01)-[~]
└─# nmap -O -v 172.16.182.224
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-07 03:37 EST
Initiating Ping Scan at 03:37
Scanning 172.16.182.224 [4 ports]
Completed Ping Scan at 03:37, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:37
Completed Parallel DNS resolution of 1 host. at 03:37, 0.01s elapsed
Initiating SYN Stealth Scan at 03:37
Scanning 172.16.182.224 [1000 ports]
Discovered open port 7070/tcp on 172.16.182.224
Completed SYN Stealth Scan at 03:38, 8.45s elapsed (1000 total ports)
Initiating OS detection (try #1) against 172.16.182.224
Nmap scan report for 172.16.182.224
Host is up (0.0014s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
7070/tcp open  realserver
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux 2.4.X
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37)
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.19 seconds
           Raw packets sent: 2036 (91.250KB) | Rcvd: 2005 (80.482KB)
```

3.Syntax:- nmap -sV -O -v <IP Address>

Command:- nmap -sV -O -v 192.168.70.135

Output:-



```
┌──(root㉿41ph4-01)-[~]
└─# nmap -O -sV -v 172.16.182.224
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-07 03:43 EST
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 03:43
Scanning 172.16.182.224 [4 ports]
Completed Ping Scan at 03:43, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:43
Completed Parallel DNS resolution of 1 host. at 03:43, 0.01s elapsed
Initiating SYN Stealth Scan at 03:43
Scanning 172.16.182.224 [1000 ports]
Discovered open port 7070/tcp on 172.16.182.224
Completed SYN Stealth Scan at 03:43, 9.10s elapsed (1000 total ports)
Initiating Service scan at 03:43
Scanning 1 service on 172.16.182.224
Completed Service scan at 03:43, 11.12s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 172.16.182.224
NSE: Script scanning 172.16.182.224.
Initiating NSE at 03:43
Completed NSE at 03:43, 0.00s elapsed
Initiating NSE at 03:43
Completed NSE at 03:43, 0.02s elapsed
Nmap scan report for 172.16.182.224
Host is up (0.0014s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE         VERSION
7070/tcp open  ssl/realserver?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4.37
OS details: DD-WRT v24-sp2 (Linux 2.4.37)
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.32 seconds
           Raw packets sent: 2037 (91.290KB) | Rcvd: 1372 (55.162KB)
```

4. nmap -Pn --script vuln nmap.scanme.org

5. -sS -p 80 IP

6. -sV -p 20,21,22 IP

7. - - top-port 20 IP

8. nmap -sV --script=http-malware-host nmap.scanme.org

9. Explore Metasploit Framework for following purpose

a.Consider any IP (targeted system) and explore details of port/ports like state, sevices, version etc..

b. using Metasploit Framework explore version details of open port

c. get all the details of version

d. change RHOSTS to your targeted system

e. show all the details.

f. exploit it

Conclusion:

FAQ:

1. **Explanation of all vulnerability (CSRF, SSRF, XSS, DOM based XSS, SLOWLORIS Attack and add any three vulnerabilities)**
2. **Usage of Metasploit Framework.**
3. **What are the modules supported by Metasploit Framework?**