	Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune		DI No.: ACAD/DI/72
Academic Year: 2021-22	Weekly Report Format for Internship		Revision : 00 Dated : 20/11/2019
Term – II	Department : Computer Engineering		Date of Preparation : 3/01/2022

Weekly Report for Internship

Roll No: TACO19108

Name of the Student: Ojus Jaiswal


Name of the Company: T A L A K U N C H I Networks Pvt. Ltd.

Domain of Internship: Cyber Security (Ethical Hacking)

Name of the Internal Guide: Mrs. Nalini Jagtap

Name of the External Guide: Mrs. Poojitha Nandimandalam

Duration of Internship: 2 Months

	Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune		DI No.: ACAD/DI/72
Academic Year: 2021-22	Weekly Report Format for Internship		Revision : 00 Dated : 20/11/2019
Term – II	Department : Computer Engineering		Date of Preparation : 3/01/2022

Week - V

Dates: 7 February, 2022 to 13 February, 2022

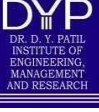
Description of work done till date:

In fifth week, we were given project no. 3 i.e., Scanning for Open ports and attacking them. In this project we have to use Nmap scanning for checking open ports and Rapid7 for exploiting open ports.

We were first told to attend sessions from LMS which will cover basics regarding the topic. Then after completion of sessions from LMS, live hands-on lecture was conducted in which the instructor showed us practical implementation of project. Then doubt session was conducted for clearing our doubts and to check if we were facing any problem in project execution.

Student Sign

Internal Guide Sign

	<p align="center">Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune</p>		<p align="center">DI No.: ACAD/DI/72</p>
<p>Academic Year: 2021-22</p>	<p align="center">Weekly Report Format for Internship</p>		<p>Revision : 00 Dated : 20/11/2019</p>
<p align="center">Term – II</p>	<p align="center">Department : Computer Engineering</p>		<p>Date of Preparation : 3/01/2022</p>

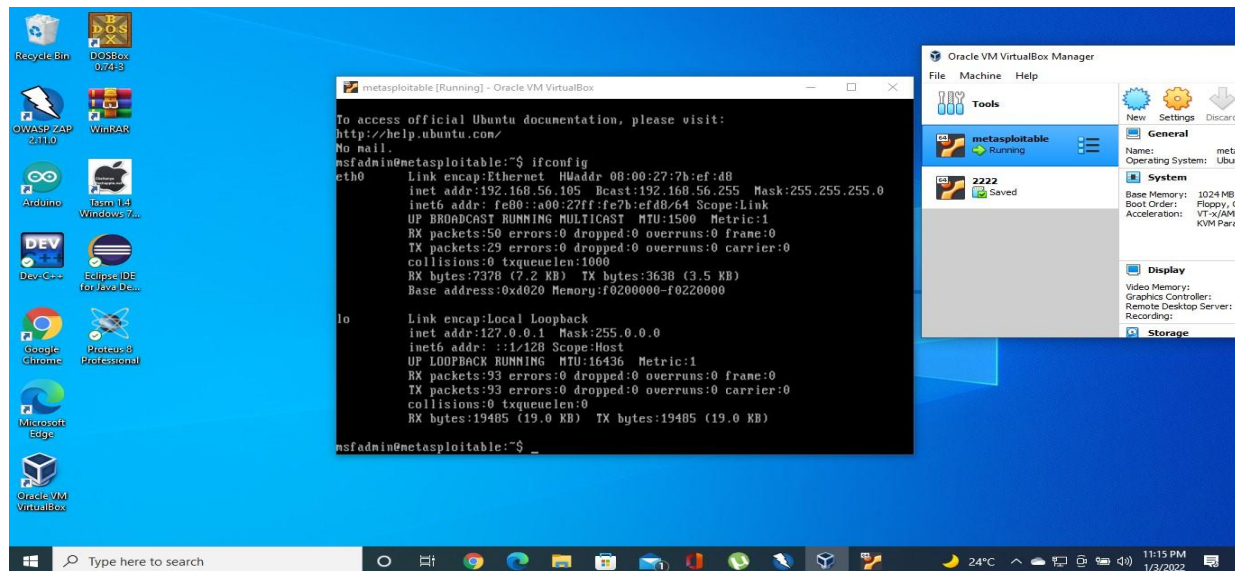
Supporting Documents:

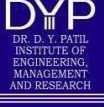
Project 3

Scanning for Open ports and attacking them

Task 1 :- Login to Metasploit and extract IP address.

Solution :-



	Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune		DI No.: ACAD/DI/72
Academic Year: 2021-22	Weekly Report Format for Internship		Revision : 00 Dated : 20/11/2019
Term – II	Department : Computer Engineering		Date of Preparation : 3/01/2022

```

root@kali: /home/kali
File Actions Edit View Help

root@kali: /home/kali
# nmap -sA -p21 -sV -O 192.168.56.105
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-03 17:39 CST
Nmap scan report for 192.168.56.105
Host is up (0.049s latency).

PORT      STATE      SERVICE VERSION
21/tcp    unfiltered ftp
Device type: switch|router|power-device|general purpose|printer|specialized
Running: Adtran AOS 10.X|18.X, Adtran embedded, Eaton embedded, Fujian Ruijie embedded, HP HP-UX 11.X, Lexmark embedded, Micr
osoft Windows 2000, NTI embedded
OS CPE: cpe:/o:adtran:aos:10 cpe:/o:adtran:aos:18.02.01.00.e cpe:/h:eaton:powerware_9170 cpe:/h:fujianruijie:star-s2800 cpe:/
o:hp:hp-ux:11.23 cpe:/o:microsoft:windows_2000::sp4:server
Too many fingerprints match this host to give specific OS details

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 2.72 seconds

root@kali: /home/kali
# nmap -sF -p21 -sV -O 192.168.56.105
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-03 17:40 CST
Nmap scan report for 192.168.56.105
Host is up (0.047s latency).

PORT      STATE      SERVICE VERSION
21/tcp    open|filtered tcpwrapped
Device type: switch|router|power-device|general purpose|printer|specialized
Running: Adtran AOS 10.X|18.X, Adtran embedded, Eaton embedded, Fujian Ruijie embedded, HP HP-UX 11.X, Lexmark embedded, Micr
osoft Windows 2000, NTI embedded
OS CPE: cpe:/o:adtran:aos:10 cpe:/o:adtran:aos:18.02.01.00.e cpe:/h:eaton:powerware_9170 cpe:/h:fujianruijie:star-s2800 cpe:/
o:hp:hp-ux:11.23 cpe:/o:microsoft:windows_2000::sp4:server
Too many fingerprints match this host to give specific OS details

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 7.15 seconds

root@kali: /home/kali

```

```

root@kali: /home/kali
File Actions Edit View Help

root@kali: /home/kali
# nmap -sA 192.168.56.105
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-03 17:49 CST
Nmap scan report for 192.168.56.105
Host is up (0.049s latency).
All 1000 scanned ports on 192.168.56.105 are filtered
Device type: switch|router|power-device|general purpose|printer|specialized
Running: Adtran AOS 10.X|18.X, Adtran embedded, Eaton embedded, Fujian Ruijie embedded, HP HP-UX 11.X, Lexmark embedded, Micr
osoft Windows 2000, NTI embedded
OS CPE: cpe:/o:adtran:aos:10 cpe:/o:adtran:aos:18.02.01.00.e cpe:/h:eaton:powerware_9170 cpe:/h:fujianruijie:star-s2800 cpe:/
o:hp:hp-ux:11.23 cpe:/o:microsoft:windows_2000::sp4:server
Too many fingerprints match this host to give specific OS details
Network Distance: 6 hops

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 1.12 ms 192.168.64.1
2 6.90 ms 192.168.43.1
3 57.17 ms 10.174.42.246
4 ...
5 64.15 ms 10.174.165.81
6 55.52 ms 192.168.56.105

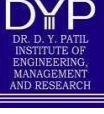
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.88 seconds

root@kali: /home/kali
# nmap -sA 192.168.56.105
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-03 17:53 CST
Nmap scan report for 192.168.56.105
Host is up (0.045s latency).
All 1000 scanned ports on 192.168.56.105 are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 21.36 seconds

root@kali: /home/kali

```

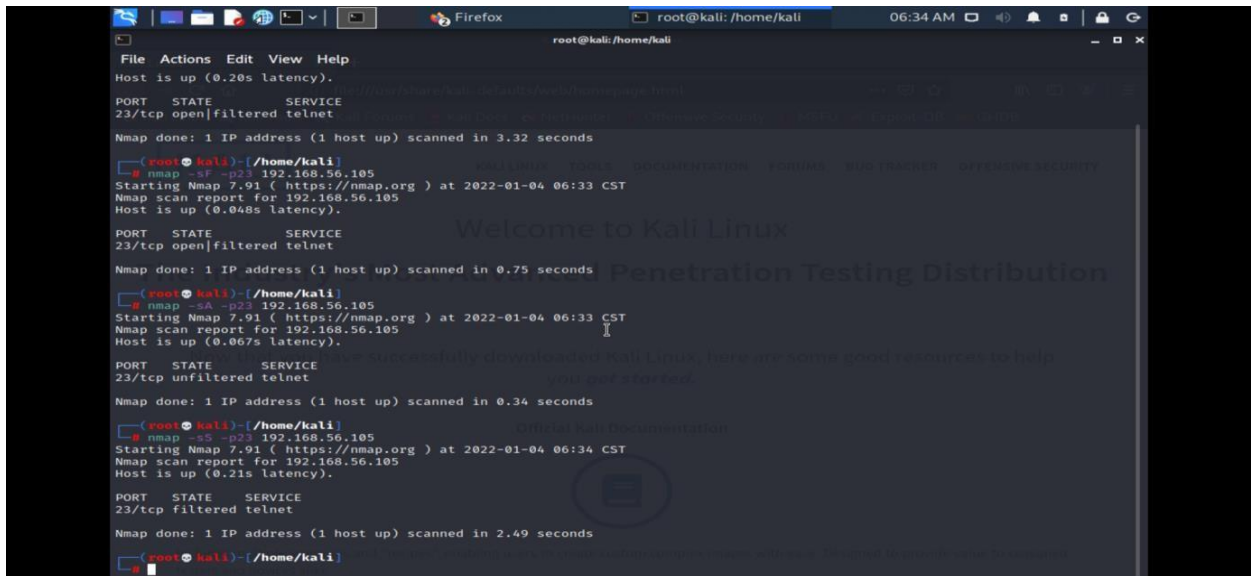
	Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune	DI No.: ACAD/DI/72
Academic Year: 2021-22	Weekly Report Format for Internship	Revision : 00 Dated : 20/11/2019
Term – II	Department : Computer Engineering	Date of Preparation : 3/01/2022

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

- A) Telnet
- B) FTP
- C) SSH

Solution :-

A) Telnet



```

root@kali: /home/kali
File Actions Edit View Help
Host is up (0.20s latency).
PORT      STATE      SERVICE
23/tcp    open|filtered telnet

Nmap done: 1 IP address (1 host up) scanned in 3.32 seconds

root@kali: /home/kali
nmap -sF -p23 192.168.56.105
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-04 06:33 CST
Nmap scan report for 192.168.56.105
Host is up (0.048s latency).
PORT      STATE      SERVICE
23/tcp    open|filtered telnet

Nmap done: 1 IP address (1 host up) scanned in 0.75 seconds

root@kali: /home/kali
nmap -sA -p23 192.168.56.105
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-04 06:33 CST
Nmap scan report for 192.168.56.105
Host is up (0.067s latency).
PORT      STATE      SERVICE
23/tcp    unfiltered telnet

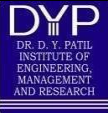
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds

root@kali: /home/kali
nmap -sS -p23 192.168.56.105
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-04 06:34 CST
Nmap scan report for 192.168.56.105
Host is up (0.21s latency).
PORT      STATE      SERVICE
23/tcp    filtered telnet

Nmap done: 1 IP address (1 host up) scanned in 2.49 seconds

root@kali: /home/kali

```


 <p>DR. D. Y. PATIL INSTITUTE OF ENGINEERING, MANAGEMENT AND RESEARCH</p>	<p align="center">Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune</p>	<p align="center">DI No.: ACAD/DI/72</p>
<p>Academic Year: 2021-22</p>	<p align="center">Weekly Report Format for Internship</p>	<p align="center">Revision : 00 Dated : 20/11/2019</p>
<p align="center">Term – II</p>	<p align="center">Department : Computer Engineering</p>	<p align="center">Date of Preparation : 3/01/2022</p>

B) FTP

```

root@kali: /home/kali
File Actions Edit View Help

root@kali:~/home/kali# nmap -ss -p21 192.168.56.105
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-04 06:27 CST
Nmap scan report for 192.168.56.105
Host is up (0.061s latency).

PORT      STATE      SERVICE
21/tcp    filtered  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.93 seconds

root@kali:~/home/kali# nmap -sA -p21 192.168.56.105
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-04 06:27 CST
Nmap scan report for 192.168.56.105
Host is up (0.065s latency).

PORT      STATE      SERVICE
21/tcp    unfiltered ftp

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds

root@kali:~/home/kali# nmap -sF -p21 192.168.56.105
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-04 06:27 CST
Nmap scan report for 192.168.56.105
Host is up (0.053s latency).

PORT      STATE      SERVICE
21/tcp    open|filtered ftp

Nmap done: 1 IP address (1 host up) scanned in 0.79 seconds

root@kali:~/home/kali# nmap -sX -p21 192.168.56.105
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-04 06:28 CST
Nmap scan report for 192.168.56.105
Host is up (0.042s latency).

PORT      STATE      SERVICE
21/tcp    open|filtered ftp

```

C) SSH

```

root@kali: /home/kali
File Actions Edit View Help

Host is up (0.071s latency).

PORT      STATE      SERVICE
22/tcp    filtered  ssh

Nmap done: 1 IP address (1 host up) scanned in 1.00 seconds

root@kali:~/home/kali# nmap -ss -p22 192.168.56.105
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-04 06:35 CST
Nmap scan report for 192.168.56.105
Host is up (0.068s latency).

PORT      STATE      SERVICE
22/tcp    filtered  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.96 seconds

root@kali:~/home/kali# nmap -sX -p22 192.168.56.105
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-04 06:36 CST
Nmap scan report for 192.168.56.105
Host is up (0.071s latency).

PORT      STATE      SERVICE
22/tcp    open|filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 0.98 seconds

root@kali:~/home/kali# nmap -sA -p22 192.168.56.105
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-04 06:36 CST
Nmap scan report for 192.168.56.105
Host is up (0.064s latency).

PORT      STATE      SERVICE
22/tcp    unfiltered ssh

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds

root@kali:~/home/kali#

```