SHADOWFOX TASK REPORT

Varshin Tej Pabba

Varshin Tej Pabba

Report-Date: 26/06/2024

Task Level: Beginner & Intermediate

Batch Id: June B1

varshintej@gmail.com

TABLE OF CONTENTS

SHADOWFOX TASK REPORT

TASK LEVEL (BEGINNER):

TASK 1

FIND ALL THE PORTS THAT ARE OPEN ON THE WEBSITE HTTP://TESTPHP.VULNWEB.COM/

I used DNSRecon to find the IP addresses of my target and then utilized Nmap to scan these addresses, discovering one open port. Based on these findings, the next steps include conducting a vulnerability scan and performing a deeper analysis of the service running on the open port to identify any potential security weaknesses.

TARGET ADDRESS: HTTP://TESTPHP.VULNWEB.COM

TARGET IP ADDRESS: 44.228.249.3

```
┌──(varshin㉿varshin)-[~/VarshinTejPabba]
└─$ dnsrecon -d http://testphp.vulnweb.com
[*] std: Performing General Enumeration against: http://testphp.vulnweb.com...
[!] Wildcard resolution is enabled on this domain
[!] It is resolving to 44.228.249.3
[!] All queries will resolve to this list of addresses!!
[-] DNSSEC is not configured for http://testphp.vulnweb.com
[*]      A http://testphp.vulnweb.com 44.228.249.3
[*]      TXT http://testphp.vulnweb.com v=spf1 -all
[*]      TXT _dmarc.http://testphp.vulnweb.com v=spf1 -all
[*]      TXT _domainkey.http://testphp.vulnweb.com v=spf1 -all
[*]      TXT _dmarc._domainkey.http://testphp.vulnweb.com v=spf1 -all
[*] Enumerating SRV Records
[-] No SRV Records Found for http://testphp.vulnweb.com
```

ENUMERATION

I have performed service enumeration to discover information about the services provided by web server that may reveal critical details that could be leveraged to bypass security and gain an initial foothold into the system.

COMMAND: NMAP -SS 44.228.249.3

```
┌──(varshin㉿varshin)-[~/VarshinTejPabba]
└─$ sudo nmap -sS 44.228.249.3
[sudo] password for varshin:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 13:29 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.018s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 15.55 seconds
```

Initial Nmap scan have all revealed that only HTTP port 80 was open.

MITIGATIONS

When an attacker using Nmap send multiple requests to the IP to find the open ports and other details. There are some mitigations needed to be taken from the Victim side. Use a strong firewall to separate incoming and outgoing traffic to limit the nonessential ports and services, and allow only essential services to communicate. Uses an intrusion detection prevention system to monitor network traffic and detect suspicious or Malicious activity, including Nmap scans. • Update all systems and software with the latest security patches to prevent vulnerabilities that can be exploited by Nmap. Apply a rate limit to the network to control the number of connection requests from a single source to prevent malicious attacks and slow down detection efforts

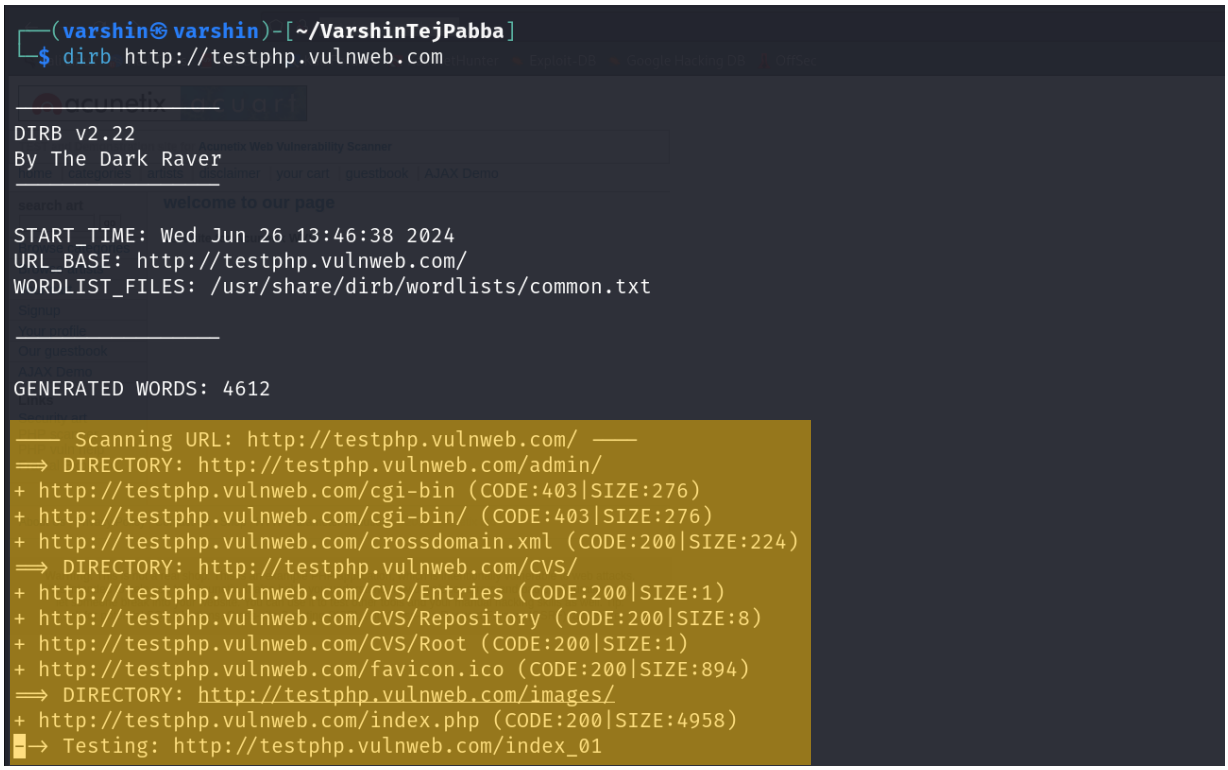
Task 2

BRUTE FORCE THE WEBSITE HTTP://TESTPHP.VULNWEB.COM/ AND FIND THE DIRECTORIES THAT ARE PRESENT IN THE WEBSITE.

- **COMMAND:**

dirb http://testphp.vulnweb.com

To systematically enumerate all directories within the specified website, begin by employing the command `dirb http://testphp.vulnweb.com`. This command is an integral part of a web content scanner tool designed to identify directories and files hosted on a web server. First, open your terminal and input the `dirb` command followed by the target URL. Upon execution, the tool will initiate a comprehensive scan of the specified website, uncovering all accessible directories and files. The results will provide a detailed understanding of the website's structure, including any potentially hidden pathways. This process is essential for conducting a thorough security assessment and vulnerability analysis of web application.



SHADOWFOX TASK REPORT

MITIGATIONS

A brute force attack is a type of cyber-attack in which an attacker attempts to gain unauthorized access to a system or account by systematically trying all possible combinations of usernames and passwords until the correct one is found. These attacks are often automated and can be a significant threat to systems with weak or easily guessable credentials.

To mitigate these attacks:

- Enforce strong password policies that require complex passwords with a combination of uppercase and lowercase letters, numbers, and special characters. • Implement rate limiting on login attempts to restrict the number of login requests from a single IP address or user within a specified time frame. This makes it more difficult for attackers to conduct large-scale brute force attacks.
- Implement IP whitelisting to restrict access to certain systems or services basedon predefined IP addresses. This can help prevent unauthorized access from unknown or suspicious locations.

Keep all software, including operating systems and authentication mechanisms, up to date with the latest security patches. Vulnerabilities in outdated systems can be exploited by attackers to facilitate brute force attacks.

Conduct regular security audits and penetration testing to identify and address vulnerabilities in your systems. This proactive approach helps discover and fix potential weaknesses before they can be exploited.

TASK 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.

filter used:

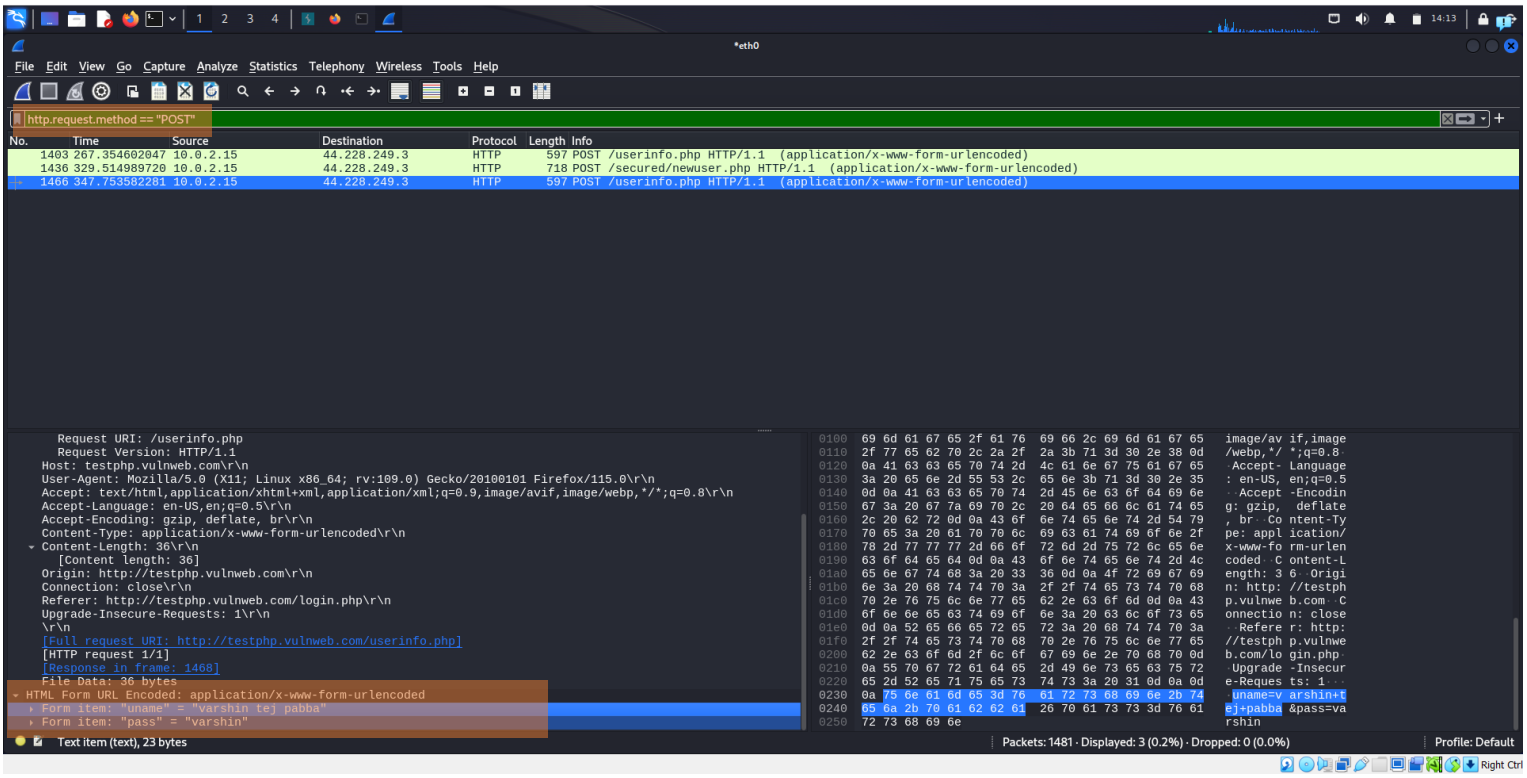
http.request.method == "POST"

• CREDENTIALS:

Username: varshin tej pabba

Password: varshin

SHADOWFOX TASK REPORT



Proof

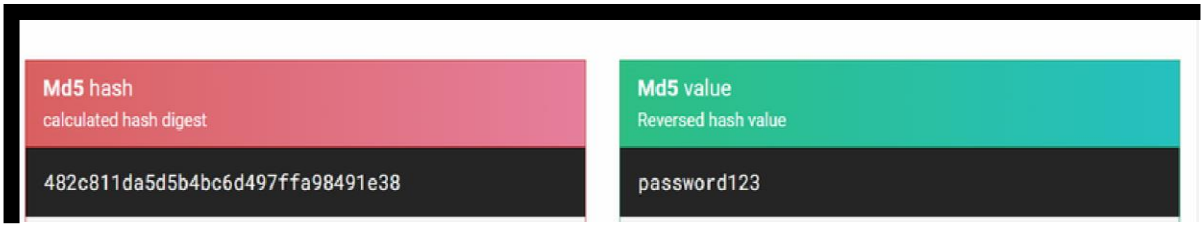
TASK LEVEL (INTERMEDIATE):

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.

HASH DECODING:

I began by accessing the encoded.txt file, which contained the password in a hashed format. To decode the hash and retrieve the original password, I used an online hash decoding tool. This tool allowed me to input the hashed password and provided the plain text password in return

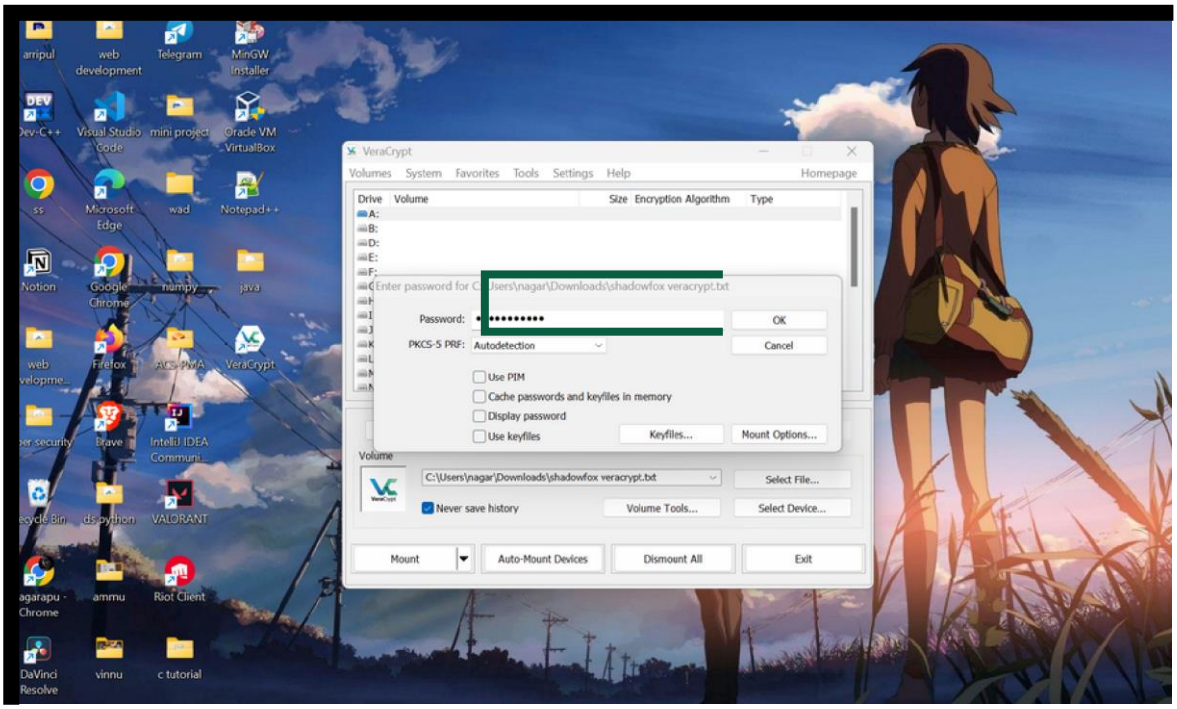


USING VERACRYPT:

With the decoded password in hand, I downloaded and installed VeraCrypt on my Windows system. VeraCrypt is a robust disk encryption tool that enables secure access to encrypted files.

I launched VeraCrypt and selected the encrypted file that needed to be unlocked.

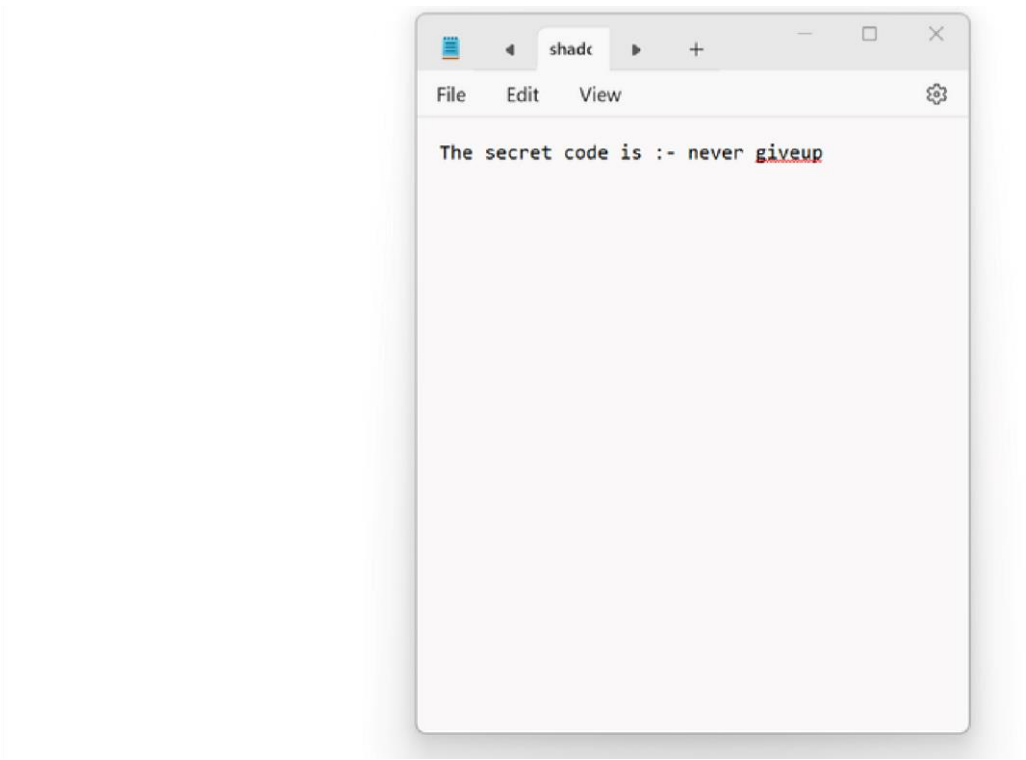
I clicked on "Mount" and entered the decoded password when prompted. VeraCrypt successfully authenticated the password and mounted the encrypted file as a virtual drive, making its contents accessible.



RETRIEVING THE SECRET CODE

After mounting the virtual drive, I navigated through the contents to locate the file containing the secret code.

I opened the file and extracted the secret code.



SHADOWFOX TASK REPORT

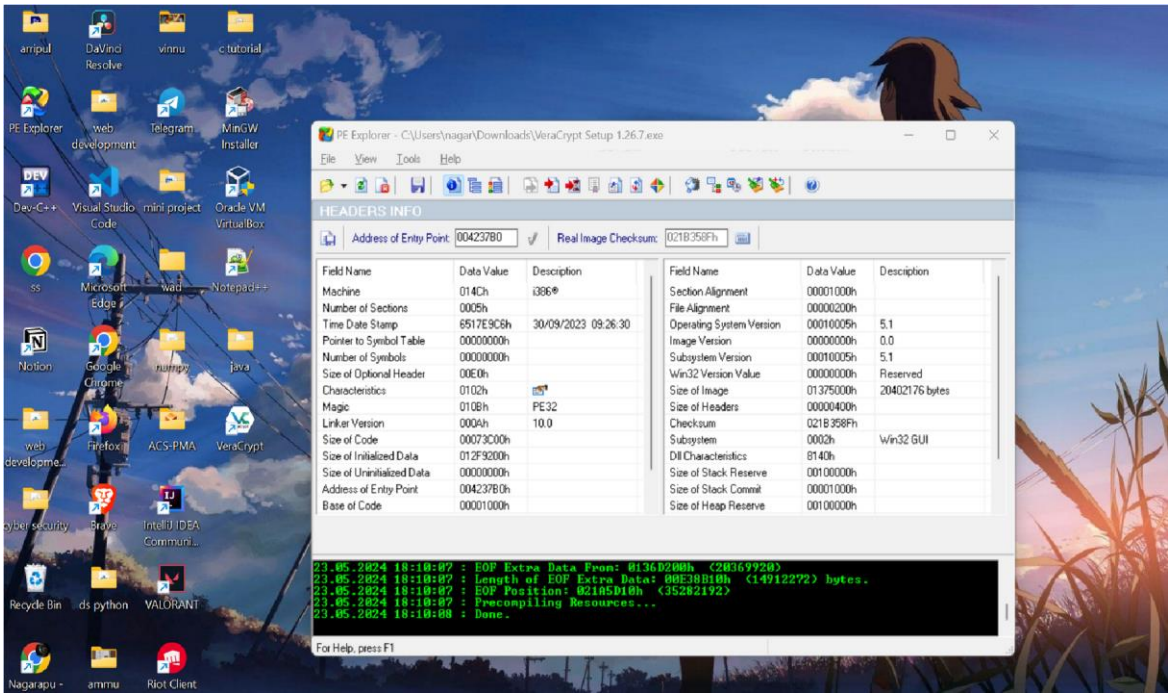
TASK 2

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.

- Download and install PE Explorer.
- Open PE Explorer and load the VeraCrypt executable via File > Open.
- Locate the "Optional Header" in the "PE Header" section.
- Find the "Address of Entry Point" field, which contains the entry point address.
- Take a screenshot showing this value.
- Save and share the screenshot as needed.

FINDINGS: ENTRY POINT ADDRESS: 004237B0



SHADOWFOX TASK REPORT

TASK 3

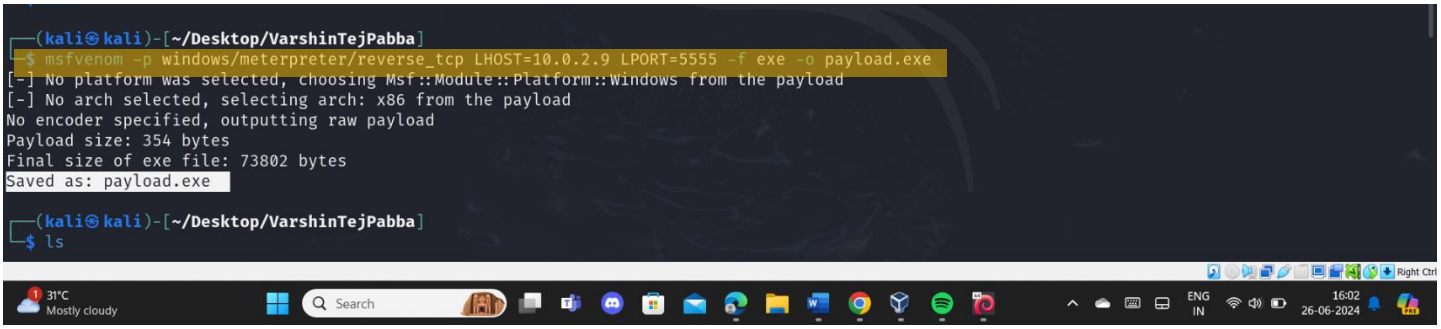
CONNECTION FROM A WINDOWS 10 MACHINE IN YOUR VIRTUAL MACHINE SETUP.

I FIRST CREATED TWO VIRTUAL MACHINES:

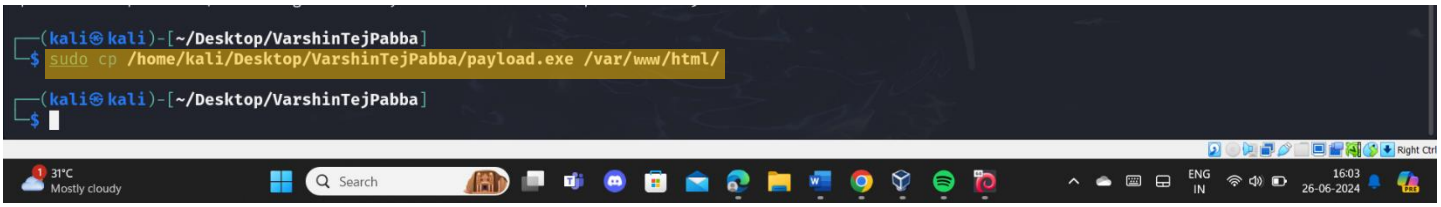
KALI LINUX IP: 10.0.2.9

WINDOWS 10 IP: 10.0.2.7, Then I configure the network to ensure each machine can ping each other.

I then used “msfvenom” to create the windows reverse_tcp payload. With the below command:



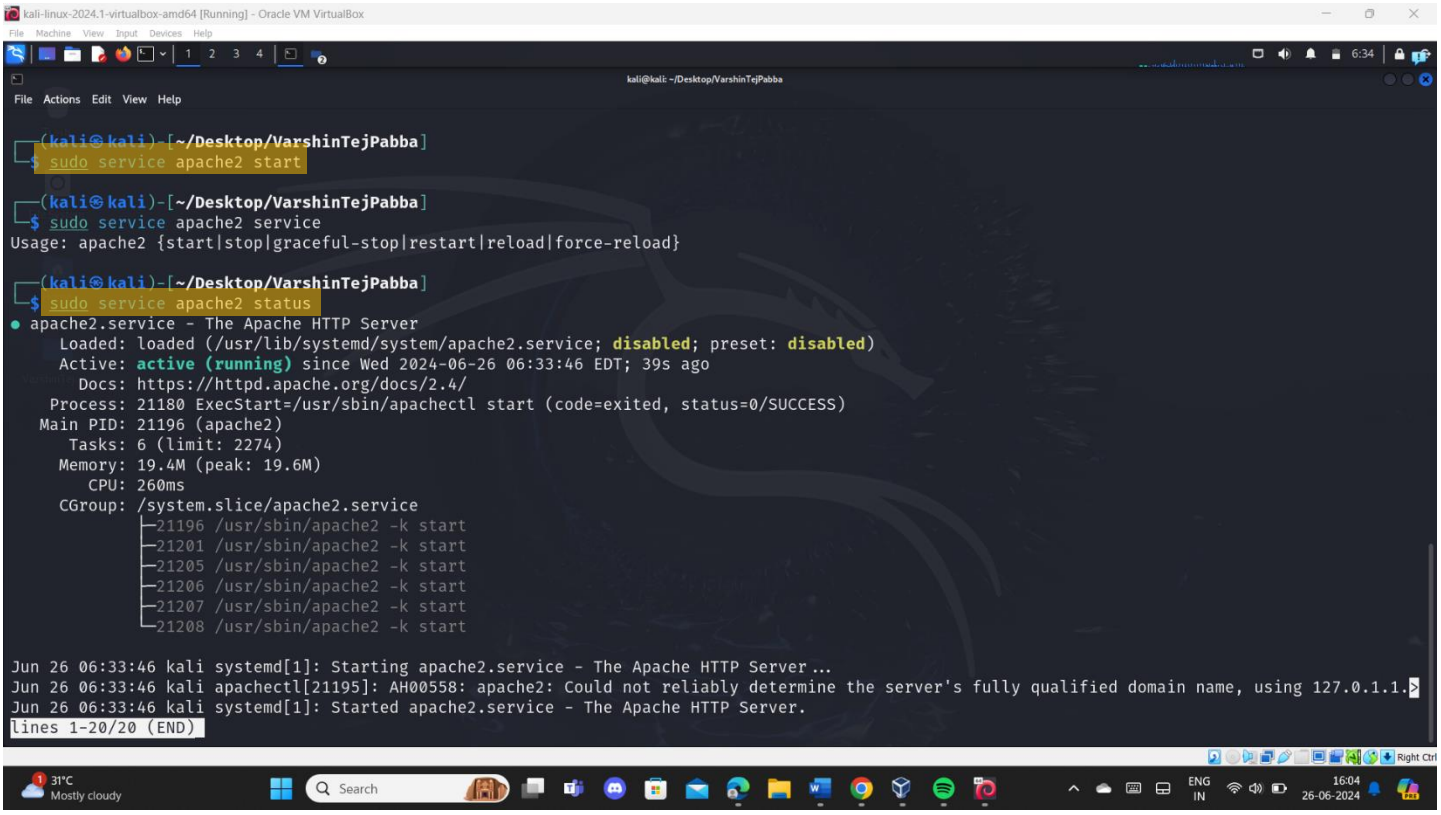
Later, I copied that,



I copied the exploit file from the desktop to the webserver: "/var/www/html/" directory. I then started the apache2 server by using the following command: • "Service apache2 start"

I then verified the apache2 service was running by using the following command:

• "Service apache2 status"



SHADOWFOX TASK REPORT

COMMAND EXPLANATION:

MSFVENOM:

Msfvenom 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.

Abbreviations / Flags:

Lhost= (IP of Kali)

Lport= (any port you wish to assign to the listener)

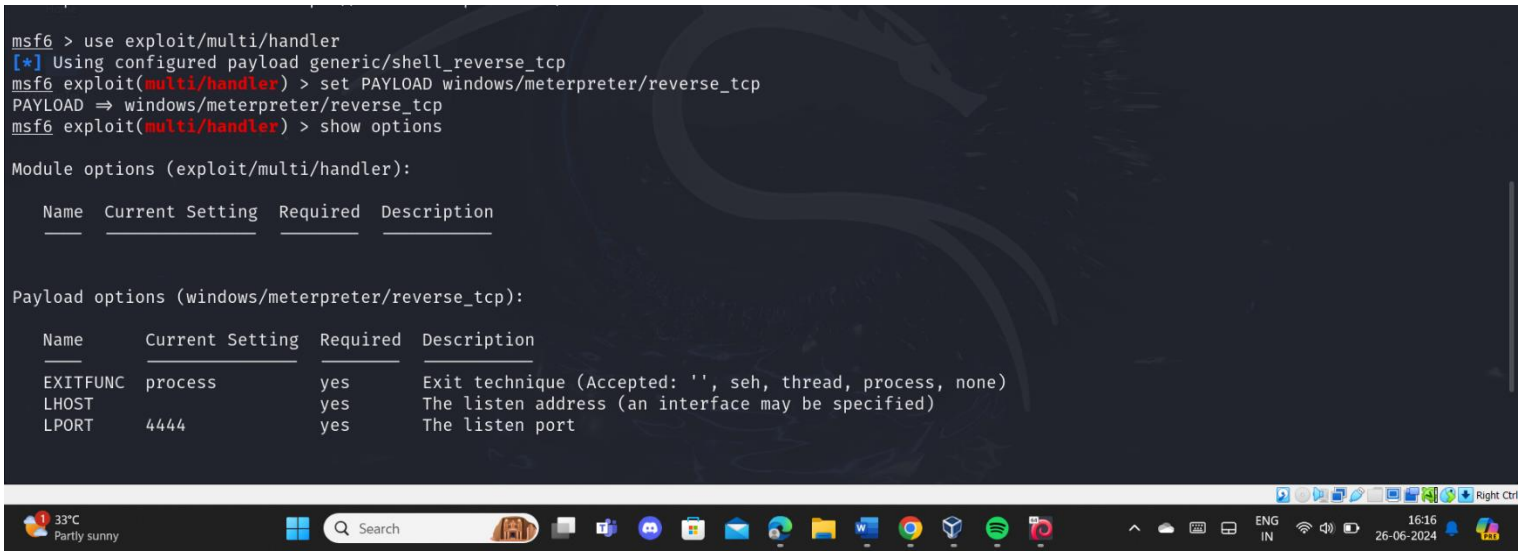
P= (Payload I.e. Windows, Android, PHP etc.)

F= file extension (i.e. windows=exe, android=apk etc.) o = “out file” to write to a location

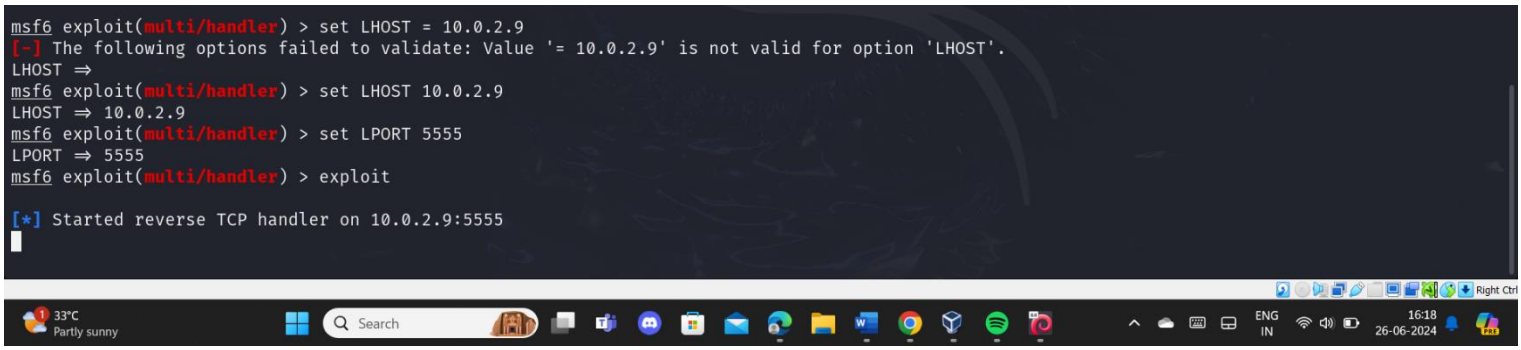
The payload will then download to the desktop since we used the “-o” flag to write the file to the desktop

Then I opened a second terminal and used the “msfconsole” command to open the “Metasploit framework”

- Once inside the “Metasploit framework”
- I used the “use exploit/multi/handler” to configure the “PAYLOAD”

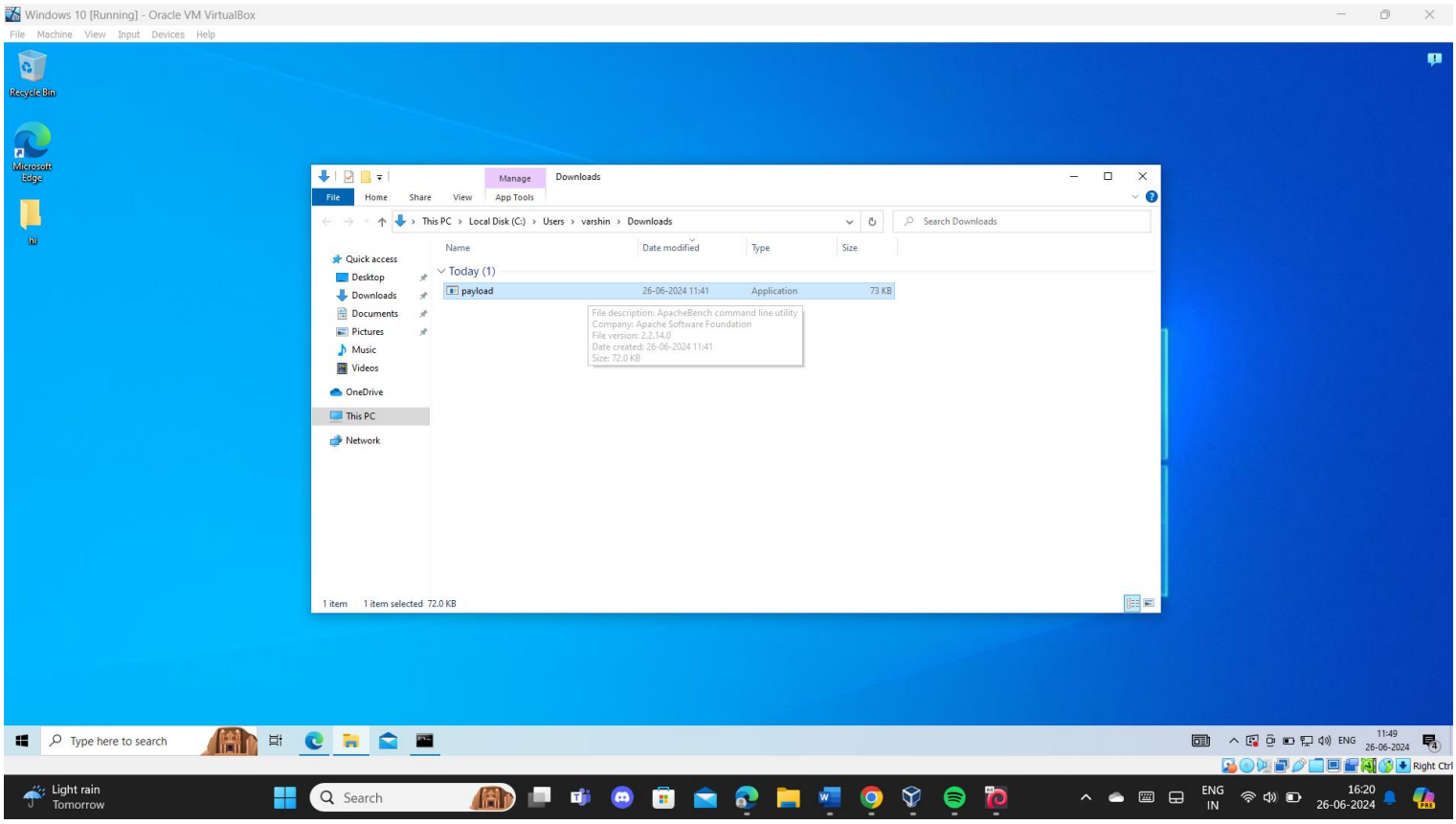


I then set the Listening port on the kali machine to listen on port “5555” Then used the “exploit command to run the handler.



SHADOWFOX TASK REPORT

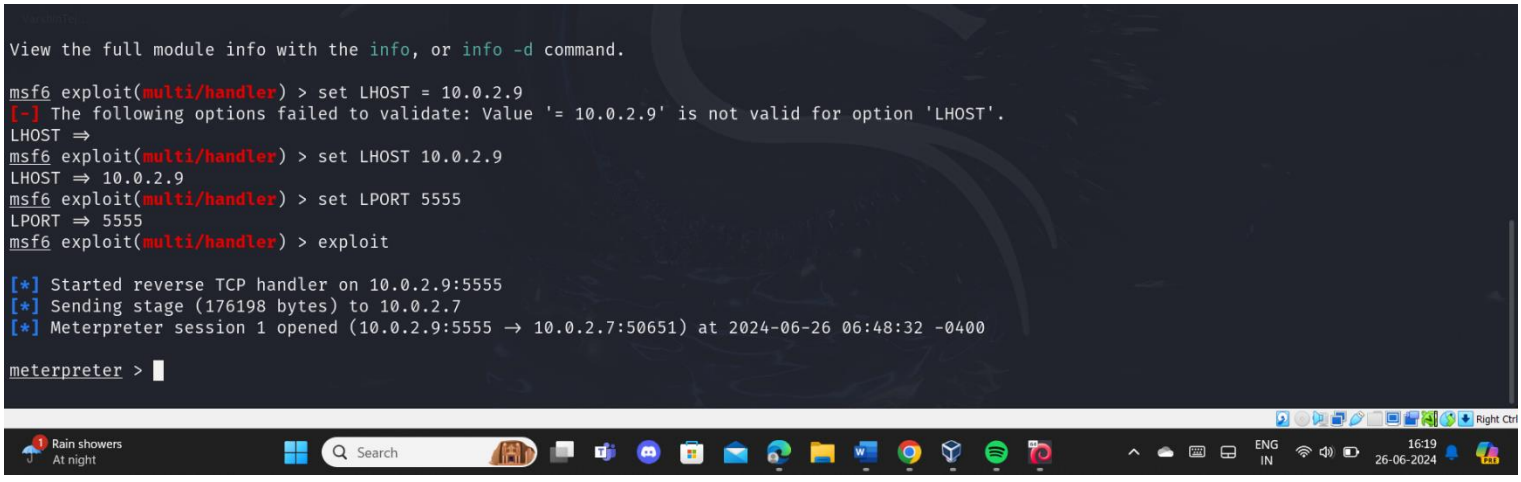
This means that from the victim's machine we can browse "http://10.0.2.9/payload.exe" and it will automatically

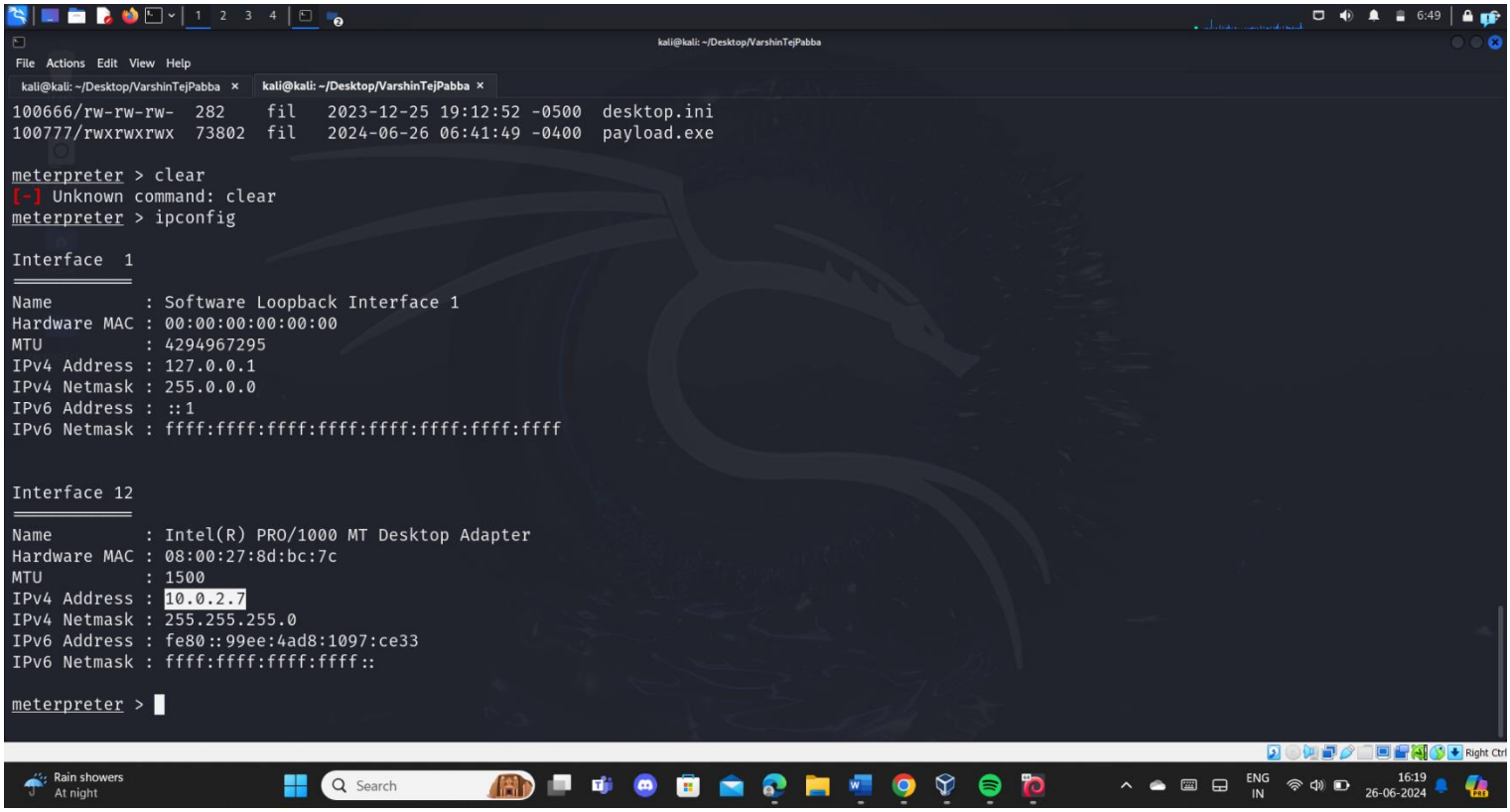


download the file, because I opened my Apache server.

I then "double-clicked" and ran the file.

Once the file ran successfully, I switched over to the kali machine and verified the connection was established and we now have access to the session of windows machine.





I verified by using ipconfig in the shell opened and it gave me the ip of win10 machine, which resulted me that, I have successfully opened the shell and session of win10 machine.