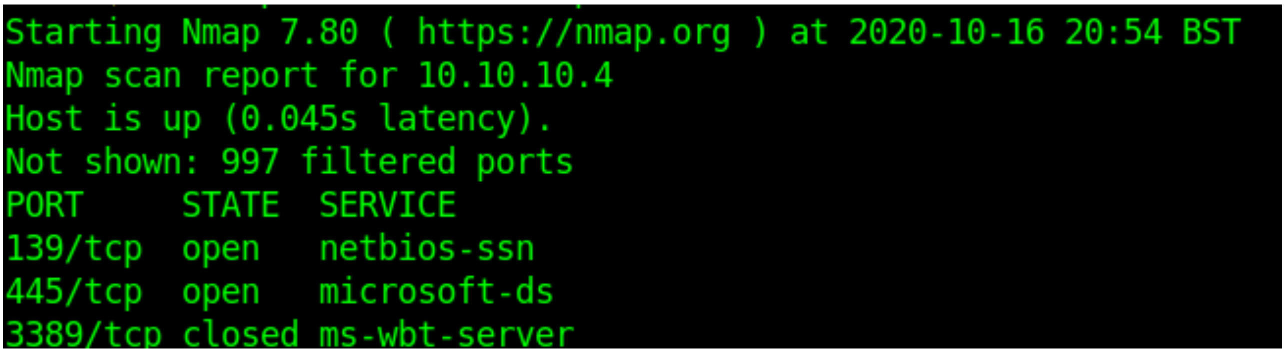
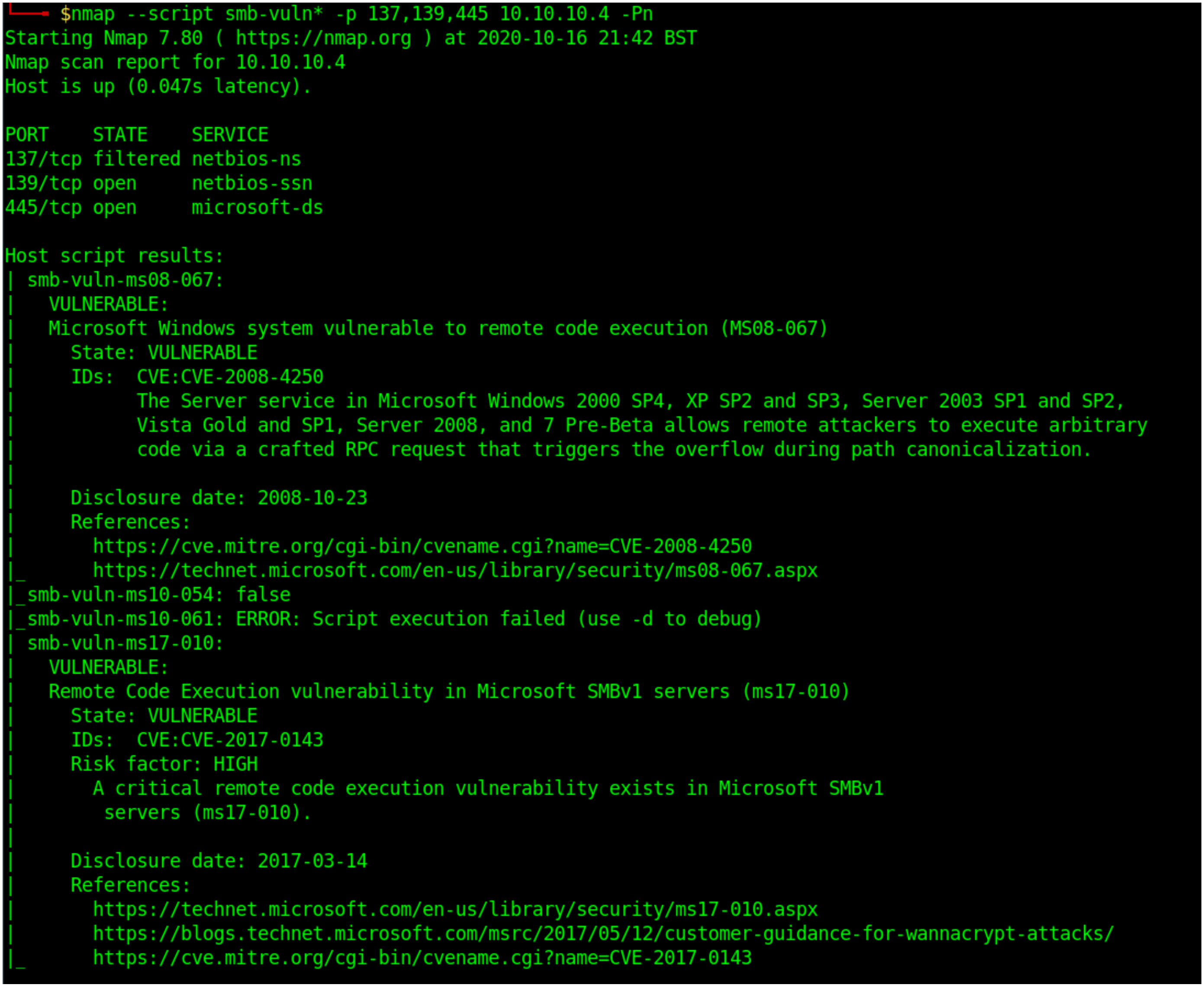
Legacy

nmap:



```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-16 20:54 BST
Nmap scan report for 10.10.10.4
Host is up (0.045s latency).
Not shown: 997 filtered ports
PORT     STATE  SERVICE
139/tcp  open   netbios-ssn
445/tcp  open   microsoft-ds
3389/tcp closed ms-wbt-server
```

smbmap and smbclient can't get nothing from the port 139 and 445.
A deeper scan on this port will give us what we need:



```
└──╼ $nmap --script smb-vuln* -p 137,139,445 10.10.10.4 -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-16 21:42 BST
Nmap scan report for 10.10.10.4
Host is up (0.047s latency).

PORT    STATE    SERVICE
137/tcp filtered netbios-ns
139/tcp open     netbios-ssn
445/tcp open     microsoft-ds

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_      https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| smb-vuln-ms17-010:
|   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://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
```

Using the CVE-2008-4250 on metasploit framework we'll be in in less than a second with the Administrator account.
Now you just need to type:
type C:\Documents and Settings\john\Desktop\user.txt

```
        <user flag will be prompted>
    type C:\Documents and Settings\Administrator\Desktop\root.txt
        <root flag will be prompted>
```

And this was Legacy!