

## RedOps AI Attack Report - 192.168.1.54

Timestamp: 2025-08-07 12:49:23.414578

>> Nmap Scan Result:

Starting Nmap 7.95 ( <https://nmap.org> ) at 2025-08-07 12:48 IST

Nmap scan report for 192.168.1.54

Host is up (0.0038s latency).

Not shown: 993 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?	
---------	------	---------------	--

902/tcp	open	ssl/vmware-auth	VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
---------	------	-----------------	--

912/tcp	open	vmware-auth	VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
---------	------	-------------	---

2179/tcp	open	vmrpd?	
----------	------	--------	--

3306/tcp	open	mysql	MySQL (unauthorized)
----------	------	-------	----------------------

MAC Address: 4C:79:6E:BD:61:B8 (Intel Corporate)

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/submit/> ).

TCP/IP fingerprint:

OS:SCAN(V=7.95%E=4%D=8/7%OT=135%CT=1%CU=32739%PV=Y%DS=1%DC=D%G=Y%M=4C796E%T

OS:M=6894535B%P=x86\_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10C%TI=I%CI=I%II=I

OS:%SS=S%TS=A)SEQ(SP=105%GCD=1%ISR=10A%TI=I%CI=RD%II=I%SS=S%TS=A)SEQ(SP=105

OS:%GCD=2%ISR=107%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=108%GCD=1%ISR=10A%TI=I%CI

OS:=I%II=I%SS=S%TS=A)SEQ(SP=FF%GCD=1%ISR=105%TI=I%CI=I%II=I%SS=S%TS=A)OPS(O

OS:1=M5B4NW8ST11%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O4=M5B4NW8ST11%O5=M5B4NW8ST

OS:11%O6=M5B4ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R

OS:=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%

OS:RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=

OS:0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5

OS:(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O

OS:%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=

OS:N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%

OS:CD=Z)

Network Distance: 1 hop

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

| smb2-security-mode:

| 3:1:1:

|\_ Message signing enabled but not required

| smb2-time:

| date: 2025-08-07T07:18:37

|\_ start\_date: N/A

|\_nbstat: NetBIOS name: DITIISL04, NetBIOS user: <unknown>, NetBIOS MAC: 4c:79:6e:bd:61:b8 (Intel Corporate)

TRACEROUTE

HOP	RTT	ADDRESS
-----	-----	---------

1	3.82 ms	192.168.1.54
---	---------	--------------

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 48.60 seconds

>> AI Suggested Tool: msfconsole

>> Command: use exploit/windows/smb/ms17\_010\_eternalblue

>> Attack Output:

[!] Skipped execution. No valid tool found.