RedOps AI Attack Report - 192.168.1.127

Timestamp: 2025-08-07 11:40:44.649682

>> Nmap Scan Result:
Starting Nmap 7.95 (https://nmap.org) at 2025-08-07 11:39 IST
Nmap scan report for 192.168.1.127
Host is up (0.0013s latency).
Not shown: 995 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?
1234/tcp open http   Node.js Express framework
|_http-title: Site doesn't have a title (application/json; charset=utf-8).
3300/tcp open tcpwrapped
MAC Address: 18:60:24:A4:7B:E9 (Hewlett Packard)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone
Running (JUST GUESSING): Microsoft Windows 11|10|2022|Phone|2008 (97%)
OS CPE: cpe:/o:microsoft:windows_11 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2022 cpe:/o:mi
Aggressive OS guesses: Microsoft Windows 11 21H2 (97%), Microsoft Windows 10 (92%), Microsoft Windows Server 2
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
| date: 2025-08-07T06:09:32
|_ start_date: N/A
| smb2-security-mode:
| 3:1:1:
|_   Message signing enabled but not required
|_nbstat: NetBIOS name: DESKTOP-KAFQH9R, NetBIOS user: <unknown>, NetBIOS MAC: 18:60:24:a4:7b:e9 (Hewlett Pack

TRACEROUTE
HOP RTT   ADDRESS
1   1.31 ms 192.168.1.127

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 54.80 seconds

>> AI Suggested Tool:
>> Command:

>> Attack Output:
[!] Skipped execution. No valid tool found.