RedOps AI Attack Report - 192.168.1.53

Timestamp: 2025-08-07 11:01:47.917736

>> Nmap Scan Result:
Starting Nmap 7.95 (https://nmap.org) at 2025-08-07 11:00 IST
Nmap scan report for 192.168.1.53
Host is up (0.0046s latency).
Not shown: 994 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?
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)
5357/tcp open http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
MAC Address: F8:54:F6:B7:84:C5 (AzureWave Technology)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 11|10|2022|2008|Phone|7 (96%)
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 (96%), Microsoft Windows 10 (91%), Microsoft Windows 10 1607
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:
|_nbstat: NetBIOS name: ADITYA, NetBIOS user: <unknown>, NetBIOS MAC: f8:54:f6:b7:84:c5 (AzureWave Technology)
| smb2-time:
| date: 2025-08-07T05:30:35
|_ start_date: N/A
|_clock-skew: -1s
| smb2-security-mode:
| 3:1:1:
|_   Message signing enabled but not required

TRACEROUTE
HOP RTT   ADDRESS
1   4.61 ms 192.168.1.53

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 61.11 seconds

>> AI Suggested Tool:
>> Command:

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