RedOps AI Attack Report - 192.168.1.53

Timestamp: 2025-08-07 12:00:58.356149

>> Nmap Scan Result:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 11:59 IST
Nmap scan report for 192.168.1.53
Host is up (0.0085s latency).
Not shown: 991 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)
1521/tcp open  oracle-tns     Oracle TNS Listener 10.2.0.1.0 (for 32-bit Windows)
3306/tcp open  mysql          MySQL (unauthorized)
5357/tcp open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
5560/tcp open  http           Oracle Application Server httpd 9.0.4.1.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Oracle Application Server Containers for J2EE 10g
|_http-server-header: Oracle Application Server Containers for J2EE 10g (9.0.4.1.0)
MAC Address: F8:54:F6:B7:84:C5 (AzureWave Technology)
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=34246%PV=Y%DS=1%DC=D%G=Y%M=F854F6%T
OS:M=68944800%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10B%TI=I%CI=I%II=I
OS:%SS=S%TS=A)SEQ(SP=104%GCD=1%ISR=10C%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=105%
OS:GCD=1%ISR=10D%TI=I%CI=I%TS=A)SEQ(SP=107%GCD=1%ISR=10B%TI=I%CI=I%II=I%SS=
OS:S%TS=A)SEQ(SP=F9%GCD=1%ISR=FF%TI=I%CI=I%II=I%SS=S%TS=A)OPS(O1=M5B4NW8ST1
OS:1%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O4=M5B4NW8ST11%O5=M5B4NW8ST11%O6=M5B4ST
OS:11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=80
OS:%W=FFFF%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R
OS:=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=0%S=Z%A=O%F=
OS: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(R=Y%DF=Y%T=
OS: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%F=R%O=%RD=0
OS:%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=1
OS:64%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-08-07T06:30:16
|_  start_date: N/A
|_nbstat: NetBIOS name: ADITYA, NetBIOS user: <unknown>, NetBIOS MAC: f8:54:f6:b7:84:c5 (AzureWave Technology)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

TRACEROUTE
HOP RTT     ADDRESS
1   8.47 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 39.00 seconds
```

>> AI Suggested Tool: nikto

>> Command: nikto -host 192.168.1.53

>> Attack Output: