RedOps AI Attack Report - 192.168.1.76

Timestamp: 2025-08-07 12:06:01.804636

>> Nmap Scan Result:
Starting Nmap 7.95 (https://nmap.org) at 2025-08-07 12:03 IST
Nmap scan report for 192.168.1.76
Host is up (0.0030s latency).
Not shown: 993 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)
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
MAC Address: DC:F5:05:EF:9F:DB (AzureWave Technology)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 11 21H2 (94%), Microsoft Windows Server 2022 (90%), Microsoft Windows
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: DITISSL26, NetBIOS user: <unknown>, NetBIOS MAC: dc:f5:05:ef:9f:db (AzureWave Technolo
| smb2-security-mode:
| 3:1:1:
|_   Message signing enabled but not required
| smb2-time:
| date: 2025-08-07T06:34:09
|_ start_date: N/A

TRACEROUTE
HOP RTT   ADDRESS
1   2.95 ms 192.168.1.76

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 60.37 seconds

>> AI Suggested Tool: nikto
>> Command: nikto -host 192.168.1.76

>> Attack Output:
- Nikto v2.5.0

+ 0 host(s) tested