RedOps AI Attack Report - 192.168.1.77

Timestamp: 2025-08-07 12:02:28.118974

>> Nmap Scan Result:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 12:00 IST
Nmap scan report for 192.168.1.77
Host is up (0.0055s latency).
Not shown: 997 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?
MAC Address: BC:17:B8:33:C1:F1 (Intel Corporate)
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: PRIYANSHUKR10, NetBIOS user: <unknown>, NetBIOS MAC: bc:17:b8:33:c1:f1 (Intel Corporat
| smb2-time:
|   date: 2025-08-07T06:31:15
|_  start_date: N/A
|_clock-skew: -1s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

TRACEROUTE
HOP RTT     ADDRESS
1   5.54 ms 192.168.1.77

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 57.29 seconds
```

>> AI Suggested Tool: msfconsole

>> Command: use exploit/windows/smb/ms17_010_eternalblue

>> Attack Output:

[!] Skipped execution. No valid tool found.