Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-20 22:06 +0530

NSE: Loaded 158 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 22:06

Completed NSE at 22:06, 0.00s elapsed

Initiating NSE at 22:06

Completed NSE at 22:06, 0.00s elapsed

Initiating NSE at 22:06

Completed NSE at 22:06, 0.00s elapsed

Initiating Parallel DNS resolution of 1 host. at 22:06

Completed Parallel DNS resolution of 1 host. at 22:06, 1.00s elapsed

Initiating SYN Stealth Scan at 22:06

Scanning 192.168.72.1 [1000 ports]

Discovered open port 445/tcp on 192.168.200.297

Discovered open port 139/tcp on 192.168.200.297

Discovered open port 135/tcp on 192.168.200.297

Discovered open port 902/tcp on 192.168.200.297

Discovered open port 912/tcp on 192.168.200.297

Completed SYN Stealth Scan at 22:06, 0.12s elapsed (1000 total ports)

Initiating Service scan at 22:06

Scanning 5 services on 192.168.200.297

Completed Service scan at 22:06, 6.11s elapsed (5 services on 1 host)

Initiating OS detection (try #1) against 192.168.200.297

Retrying OS detection (try #2) against 192.168.200.297

Retrying OS detection (try #3) against 192.168.200.297

Retrying OS detection (try #4) against 192.168.200.297

Retrying OS detection (try #5) against 192.168.200.297

NSE: Script scanning 192.168.200.297.

Initiating NSE at 22:06

Completed NSE at 22:06, 14.18s elapsed

Initiating NSE at 22:06

Completed NSE at 22:06, 0.07s elapsed

Initiating NSE at 22:06

Completed NSE at 22:06, 0.00s elapsed

Nmap scan report for 192.168.200.297

Host is up (0.00052s latency).

Not shown: 995 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)

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=7.98%E=4%D=10/20%OT=135%CT=1%CU=43079%PV=Y%DS=0%DC=L%G=Y%TM=68F66

OS:511%P=i686-pc-windows-windows)SEQ(SP=100%GCD=1%ISR=10A%TI=I%CI=I%II=I%SS

OS:=S%TS=A)SEQ(SP=101%GCD=1%ISR=106%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=103%GCD

OS:=1%ISR=10A%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=F7%GCD=1%ISR=109%TI=I%CI=I%II

OS:=I%SS=S%TS=A)OPS(O1=MFFD7NW8ST11%O2=MFFD7NW8ST11%O3=MFFD7NW8NNT11%O4=MFF

OS:D7NW8ST11%O5=MFFD7NW8ST11%O6=MFFD7ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FF

OS:FF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y

OS:%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD

OS:=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%

OS:S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(

OS:R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F

OS:=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G

OS:%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Uptime guess: 0.090 days (since Mon Oct 20 19:56:59 2025)

Network Distance: 0 hops

TCP Sequence Prediction: Difficulty=259 (Good luck!)

IP ID Sequence Generation: Incremental

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

| smb2-time:

|   date: 2025-10-20T16:36:22

|\_  start\_date: N/A

| smb2-security-mode:

|   3.1.1:

|\_    Message signing enabled and required

NSE: Script Post-scanning.

Initiating NSE at 22:06

Completed NSE at 22:06, 0.00s elapsed

Initiating NSE at 22:06

Completed NSE at 22:06, 0.00s elapsed

Initiating NSE at 22:06

Completed NSE at 22:06, 0.00s elapsed

Read data files from: C:\Program Files (x86)\Nmap

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 32.29 seconds

           Raw packets sent: 1080 (51.090KB) | Rcvd: 2343 (107.685KB)