```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-03 12:53 Hora est. Pacífico, Sudamérica
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:53
Completed NSE at 12:53, 0.00s elapsed
Initiating NSE at 12:53
Completed NSE at 12:53, 0.00s elapsed
Initiating NSE at 12:53
Completed NSE at 12:53, 0.00s elapsed
Initiating ARP Ping Scan at 12:53
Scanning 192.168.239.4 [1 port]
Completed ARP Ping Scan at 12:53, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:53
Completed Parallel DNS resolution of 1 host. at 12:54, 12.11s elapsed
Initiating SYN Stealth Scan at 12:54
Scanning 192.168.239.4 [1000 ports]
Discovered open port 135/tcp on 192.168.239.4
Discovered open port 445/tcp on 192.168.239.4
Discovered open port 53/tcp on 192.168.239.4
Discovered open port 139/tcp on 192.168.239.4
Discovered open port 49157/tcp on 192.168.239.4
Discovered open port 49158/tcp on 192.168.239.4
Discovered open port 49155/tcp on 192.168.239.4
Discovered open port 464/tcp on 192.168.239.4
Discovered open port 3268/tcp on 192.168.239.4
Discovered open port 636/tcp on 192.168.239.4
Discovered open port 49154/tcp on 192.168.239.4
Discovered open port 88/tcp on 192.168.239.4
Discovered open port 593/tcp on 192.168.239.4
Discovered open port 3269/tcp on 192.168.239.4
Discovered open port 389/tcp on 192.168.239.4
Completed SYN Stealth Scan at 12:54, 4.55s elapsed (1000 total ports)
Initiating Service scan at 12:54
Scanning 15 services on 192.168.239.4
Completed Service scan at 12:55, 53.59s elapsed (15 services on 1 host)
Initiating OS detection (try #1) against 192.168.239.4
NSE: Script scanning 192.168.239.4.
Initiating NSE at 12:55
Completed NSE at 12:55, 40.14s elapsed
Initiating NSE at 12:55
Completed NSE at 12:55, 0.13s elapsed
Initiating NSE at 12:55
Completed NSE at 12:55, 0.00s elapsed
Nmap scan report for 192.168.239.4
Host is up (0.00s latency).
Not shown: 985 filtered ports
PORT       STATE SERVICE        VERSION
53/tcp    open  domain        Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB1446A)
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2022-09-03 17:54:19Z
135/tcp   open  msrpc         Microsoft Windows RPC
```

```
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: LABREDES.loc
445/tcp   open  microsoft-ds Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: LABREDES.loc
3269/tcp  open  tcpwrapped
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
MAC Address: 00:0C:29:7C:67:C6 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:micros
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows Embedded St
Uptime guess: 0.039 days (since Sat Sep 03 11:59:15 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: JUPITER; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1

Host script results:
|_clock-skew: mean: 1h40m00s, deviation: 2h53m12s, median: 0s
| nbstat: NetBIOS name: JUPITER, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:7c:67:c6 (
| Names:
|   JUPITER<20>        Flags: <unique><active>
|   JUPITER<00>        Flags: <unique><active>
|   LABREDES<00>       Flags: <group><active>
|   LABREDES<1c>       Flags: <group><active>
|_  LABREDES<1b>       Flags: <unique><active>
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standa
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: JUPITER
|   NetBIOS computer name: JUPITER\x00
|   Domain name: LABREDES.local
|   Forest name: LABREDES.local
|   FQDN: JUPITER.LABREDES.local
|_  System time: 2022-09-03T12:55:09-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2022-09-03T17:55:09
```

```
|_   start_date: 2022-09-03T07:35:27

TRACEROUTE
HOP RTT     ADDRESS
1    0.00 ms 192.168.239.4

NSE: Script Post-scanning.
Initiating NSE at 12:55
Completed NSE at 12:55, 0.00s elapsed
Initiating NSE at 12:55
Completed NSE at 12:55, 0.00s elapsed
Initiating NSE at 12:55
Completed NSE at 12:55, 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.or
Nmap done: 1 IP address (1 host up) scanned in 116.33 seconds
           Raw packets sent: 2023 (90.850KB) | Rcvd: 25 (1.422KB)
```