Nmap Scan Report

Date & Time: 2025-11-09 11:29 CST
Scanner: Nmap 7.94SVN (https://nmap.org)
Target Host: 192.168.100.130
MAC Address: 00:0C:29:EC:1A:AD (VMware)
Network Distance: 1 hop
Scan Type: SYN Stealth (-sS), Service detection (-sV), OS detection (-O), NSE scripts (default + vuln)
Total Ports Scanned: 1000 TCP ports

---

1. Host Status

IP Address	Host Status	Latency
192.168.100.130	Up	0.0059 s

Comments: Host is up and reachable via ARP ping.

---

2. Open / Closed Ports

All scanned ports are **in ignored states**.

Port	State	Service	Comments
All 1000 TCP	Filtered	Unknown	No response received; host firewall or filtering device likely in place

Notes:

- The host appears to be heavily firewalled or isolated; no TCP ports responded.
- No open services were detected, so direct service vulnerabilities cannot be enumerated.

---

3. OS Detection

- Nmap was **unable to determine the OS**: “Too many fingerprints match this host to give specific OS details.”
- MAC address indicates a **VMware virtual machine**.

---

4. Traceroute

Hop	RTT	Address
1	5.86 ms	192.168.100.130

Comment: Host is one network hop away, confirming LAN connectivity.

---

5. NSE Script Scans

- No NSE vulnerability scripts returned results (likely due to all ports being filtered).

---

6. Summary of Findings

Finding	Severity	Comment
No open ports detected	Low	Cannot enumerate services; host appears firewalled/filtered.
Host is up	Informational	Confirmed reachability on LAN.
OS not detected	Informational	Could not fingerprint OS.
VMware MAC	Informational	Likely a virtual machine.

Overall Risk Level: Low (no immediate attack surface detected)

---

7. Recommendations

1. **Network / Host Verification:** Verify the firewall rules or host-based filtering — ensure that required services are exposed if this host is meant to provide services.
2. **Future Scans:** If this is an internal host for security testing, consider using **authenticated scans** or scanning from inside the VM's network to see filtered services.
3. **Monitoring:** Add host to network inventory; periodically scan for changes (new services opening).
4. **Documentation:** Note MAC and network location in asset register.

---

8. Attachments / References

- Raw Nmap Output: last-scan.nmap
- XML for automated processing: last-scan.xml
- Grepable output: last-scan.gnmap
- Nmap commands used:

nmap -sS -sV -O --script vuln -T4 -oA ~/nmap/last-scan 192.168.100.130