Nmap Network Scan Report

Scan Summary
Date & Time: Mon Sep 22 2025, 21:18–21:19 IST
Command Run: nmap -sS -oN scan_results.txt 192.168.1.0/24
Scope: 256 possible IPs (192.168.1.0–192.168.1.255)
Hosts Up: 11
Duration: 65.79 seconds

Detected Hosts & Open Ports

IP Address	MAC / Vendor	Open Ports & Services	Notes
192.168.1.1	20:0C:86:60:11:D0 (GX India Pvt)	53 DNS, 80 HTTP, 443 HTTPS	Likely router/gateway
192.168.1.3	46:84:F6:80:2B:1D (Unknown)	None	Client device with firewall
192.168.1.6	62:D3:32:07:0D:27 (Unknown)	Multiple filtered high ports	Verify device identity
192.168.1.7	F8:45:2D:CD:19:7F (Unknown)	135 MSRPC, 139 NetBIOS, 445 SMB, 5500 Hotline, 7070 RealServer	Windows PC/file-sharing host
192.168.1.10	3A:BE:05:99:B5:1C (Unknown)	None	Normal client
192.168.1.11	46:21:49:F5:45:74 (Unknown)	None	Normal client
192.168.1.15	F8:45:2D:CD:19:7F (Unknown)	None	Normal client
192.168.1.16	2C:3B:70:E4:9F:1F (AzureWave)	135 MSRPC, 139 NetBIOS, 445 SMB	Windows PC or NAS
192.168.1.19	72:C1:EA:D8:87:46 (Unknown)	None	Normal client
192.168.1.20	60:E9:AA:CA:82:05 (Cloud Network Technology)	135 MSRPC, 139 NetBIOS, 445 SMB, 5357 WSDAPI	Windows device or printer

Observations & Risks

- Windows File Sharing (Ports 135/139/445): Present on multiple hosts. Risk of SMB exploits. Patch & firewall required.
- Router/Web Interface (Ports 80/443 on 1.1): Ensure strong admin password and firmware updates.
- Filtered High Ports on 1.6: Verify legitimacy of this device.
- No Open Ports on several hosts: Good firewall hygiene.

Recommended Next Steps

1. Inventory devices and map IPs to physical hardware.
2. Update firmware and OS patches, disable SMBv1.
3. Restrict or firewall unneeded services (SMB, NetBIOS).
4. Re-run scans periodically to monitor changes.