**Identified IP Addresses and Status**

From the TCP and UDP scan logs, the following **active hosts** were scanned and completed:

* **Active IPs:**
  + 192.168.43.1
  + 192.168.43.2
  + 192.168.43.3
  + 192.168.43.10
  + 192.168.43.11
  + 192.168.43.12
  + 192.168.43.13
  + 192.168.43.14
  + 192.168.43.15
  + 192.168.43.16
  + 192.168.43.17
  + 192.168.43.18
  + 192.168.43.20
  + ... (and many more up to 192.168.43.254)

**Active Hosts Identified:**

1. **192.168.201.48**
2. **192.168.201.126**

**🔓 Open Ports and Services:**

**📌 Host: 192.168.201.48**

* **53/tcp** — open — domain (DNS)

**📌 Host: 192.168.201.126**

* **135/tcp** — open — msrpc
* **139/tcp** — open — netbios-ssn
* **445/tcp** — open — microsoft-ds (SMB over TCP)
* **2869/tcp** — open — icslap (Internet Connection Sharing)
* **7070/tcp** — open — realserver (RealAudio/RealVideo streaming)

**🧠 Interpretation:**

* **192.168.201.48** is likely a DNS server or a system running a DNS service.
* **192.168.201.126** has multiple open ports typical of a **Windows machine**, possibly running:
  + Windows File and Printer Sharing (SMB)
  + Remote procedure call services
  + RealServer streaming or admin tools
  + UPnP (port 2869)

**Research Common Services Running on Found Ports**

From your data:

* **Port 443 (TCP)** is the most frequent destination.
* This indicates **HTTPS (Hypertext Transfer Protocol Secure)** traffic—used for secure web communication.

**Common Ports and Services:**

| **Port** | **Protocol** | **Common Service** |
| --- | --- | --- |
| 80 | TCP | HTTP (Unsecured Web Traffic) |
| 443 | TCP | HTTPS (Secure Web Traffic) |
| 21 | TCP | FTP (File Transfer Protocol) |
| 22 | TCP | SSH (Secure Shell) |
| 23 | TCP | Telnet (Remote Shell - insecure) |
| 25 | TCP | SMTP (Email Sending) |
| 53 | UDP/TCP | DNS (Domain Name System) |
| 110 | TCP | POP3 (Email Receiving) |
| 445 | TCP | SMB (Windows File Sharing) |

You can research services by port using:

* https://www.speedguide.net/port.php
* IANA Service Name Port Number Registry

**⚠️ Step 7: Identify Potential Security Risks from Open Ports**

Now that you’ve identified open ports (mainly **443** in your case), you should determine the risks they pose:

**🔐 Port 443 (HTTPS)**

* **Normal Use**: Secure communication with web servers.
* **Risks**:
  + If HTTPS is misconfigured (e.g., self-signed certificates, old SSL versions), it can be vulnerable to:
    - **SSL stripping**
    - **Man-in-the-middle (MITM)** attacks
    - **Heartbleed (if using old OpenSSL)**
  + Services on this port might host **web applications** vulnerable to:
    - **SQL Injection**
    - **Cross-Site Scripting (XSS)**
    - **Authentication bypass**