

## Methodology & Tools Documentation

### 1. Tooling:

- **Primary Scanner:** Nmap (Network Mapper) v7.9x
- **Environment:** Linux Terminal (Ubuntu)

### 2. Scanning Strategy:

We utilized a two-phase approach to ensure comprehensive coverage while maintaining efficiency.

- **Phase 1: Host Discovery (Ping Sweep)**
  - *Objective:* Identify active endpoints within the subnet.
  - *Command:* `nmap -sn [IP_RANGE]`
- **Phase 2: Comprehensive Service Discovery**
  - *Objective:* Identify open ports and enumerate service versions on active hosts.
  - *Command:* `nmap -sV -p- -T4 -Pn [TARGET_IP]`

### 3. Parameter Explanation:

- `-sV`: Service Version Detection (Crucial for identifying specific software versions like OpenSSH 8.9).
- `-p-`: Full port scan (1-65535) to detect non-standard services (e.g., Redis on 9111).
- `-T4`: Aggressive timing to speed up the scan process.
- `-Pn`: Disable host discovery (assume online) to bypass potential ICMP blocks.