Last Updated: April, 2025

# Use Case:

- Onboarding to new networks
- Network/Inventory auditing
- Vulnerability scanning

# Deliverables:

- Up-to-date network diagrams (Layer 2/3; logical)
- Asset inventory
- Identification of unknown/rogue devices
- Security Findings summary
- Onboarding summary report with recommendations

# Ongoing Scanning Cadence Recommendations:

Running scans on a regular cadence can be automated with scripting or completed manually, but is encouraged to ensure inventories stay accurate and rogue devices are identified quickly.

I recommend a quarterly scan to identify network/inventory changes and keep documentation up to date. Scanning is not very efficient for identifying rogue endpoints, this identification is just a possible incidental outcome of scanning. For rogue endpoint monitoring, instead traffic logging / netflow information should be utilized to generate security alerts for provisioned IPs in such networks.

- Regardless of cadence/tool chosen, run periodic Network or Asset scans.
- Keep version control diagrams current with change history
- Integrate vulnerability scanners and ticketing systems for best practices

# Toolbox

| Suggested | Use | Alternatives |
|---|---|---|
| nmap | Network scanning | Masscan; Angry IP Scanner |
| Open-AudIT | Asset Discovery | NetBox, Lansweeper |
| draw.io | Diagram software | Visio |
| OneNote | Note Taking | Evernote, Joplin, Trillium, OpenNote |
| >> [layer 2 standard] show lldp (neighbors) | Link layer discovery protocol; | >> [cisco proprietary] show cdp (neighbors) |
| Nessus | Vuln Scanning | Wazuh (ELK stack), OpenSCAP, OpenVAS |
| Wireshark | Packet Capture | tcpdump |

# Play by play:

# Step 1: Secure initial network access, credentials, and perms

1. Begin a running document to record all steps taken as well as findings
    a. OneNote, Evernote, Atom.io, etc.
    b. DO NOT record credentials in the notes
2. Ensure you are appropriately credentialed for network access
    a. Firewalls, routers, switches, controllers
3. Confirm IPs of infrastructure management devices
    a. Firewalls, routers, switches, controllers that will be used to initialize mapping
4. Secure permission from directors and network owners to perform a network scan/probe
5. Review and note existing documentation/diagrams

# Step 2: Define Scope and segments permitted for scanning

1. Note known VLANs, subnets, DMZ, VPN, and cloud connections
2. Define and note core segments/zones (considerations below, not a checklist; logic for notation is dependant on the enterprise network structure)
    a. Trust v. Untrust
    b. Production v. Development / QA
    c. Operations and/or Userspace
    d. Corporate v. remote offices / VPN
    e. DMZ / IoT / Guest
    f. Management Interfaces
    g. Egress/Ingress points/ranges
3. Build out and populate a table, noting the following columns:
    IP/mask | Type | VLAN ID | Firewall Zone | Notes

# Step 3: Scanning & Discovery

1. Use **nmap** on each CIDR range permitted in Step 1 for Active Scanning
    a. Ex: >> nmap -sS -sV -O -T4 -p- 10.10.10.0/24
        i. **-sS**: TCP SYN packet scan
        ii. **-sV**: Probe open ports to determine service/version info
        iii. **-O**: Enable OS detection
        iv. **-T4**: Second highest timing template (0-5)
        v. **-p-**:Scan all ports

2. Mirror/Tap via Wireshark for Passive Scanning (if permitted;beware data privacy laws)
    a. SPAN Port (Switched Port Analyzer) [aka Port Mirroring]
        i. Connect wireshark device to SPAN port to watch feed
        ii. Note: SPAN can drop packets at high load - not good for heavy networks
    b. TAP device between router and firewall to run wireshark and copy packets.
        i. Preferred for lossless or low latency monitoring permitted environments.

# Step 4: SNMP Enumeration

1. Attempt SNMP polling on network devices:
2. Extract:
    a. Interface indexes and descriptions
    b. APR / MAC tables
    c. Device model numbers and serial numbers
3. Map Layer 2 connections from neighbors:
    (cisco) >> show cdp neighbors
    (agnostic) >> show lldp neighbors

# Step 5: Diagram Creation

1. Layered Diagrams:
    a. Layer 2: Switches, VLANs, Trunks/Uplinks
    b. Layer 3: Subnets, Routers, network edges
    c. Security Zones: Firewalls, ACLs, NATs
    d. Logical Application Maps: Servers to DB, API Flows, etc.

# Step 6: Validate Findings with Shareholders

1. Common Shareholders to reach out to
    a. Immediate PoC (if consulting)
    b. Network Engineering
    c. Security
    d. Application Owners
    e. IT Support
    f. IT/Infrstructure Director
2. Collect Feedback, redraft, and seek validation again

# Additional Followup Steps Recommended

1. Centralize network diagram/documentation for relevant teams to access
2. Update asset inventories to ensure documentation is complete, and identify anomalous connections
    a. Notify security / investigate anomalies
3. **Security Controls Mapping**
    a. Document ACLs, firewall zones, routes, and RBAC
    b. Identify:
        i. Any-any-allow rules
        ii. Overlapping subnets
        iii. Public exposure and routing leaks
    c. Note baseline communication norms via Netflow or firewall logs, and deliver suggestions for hardening if bad practices are found.