📊 Security Audit Report

Project: Consolidate and Document Scan Results

Task Reference: DEV-355

Date: January 2026

1. 📝 Executive Summary

A comprehensive security assessment was conducted on the organization's production subnet to establish a baseline of active assets and exposed services. The audit followed a strict non-destructive methodology (DEV-353) and verified all findings through manual validation.

Key Findings:

- Total Assets Scanned: 15 Hosts [1]
- Total Open Ports: 39 Ports Detected
- Critical Risks: 2 Hosts exposing database services (Redis) to the public internet.
- Compliance Status: Mixed. While SSH access is standardized and secure, the presence of management interfaces (Consul/MinIO) on public IPs requires immediate remediation.

---

2. 🗺️ Master Findings Table

The following table aggregates the port scan data and service fingerprinting results for all 15 validated hosts.

Asset ID	IP Address	Port	Protocol	Service	Risk Level
Server-01	64.23.130.208	22	TCP	OpenSSH 8.9p1	🟢 Low
Server-02	157.230.47.60	22	TCP	OpenSSH 8.9p1	🟢 Low
		8500	TCP	Consul Agent	🟡 Medium
		9000	TCP	MinIO (Storage)	🟡 Medium
		9001	TCP	MinIO Console	🟡 Medium

Asset ID	IP Address	Port	Protocol	Service	Risk Level
Server-03	159.223.62.168	22	TCP	OpenSSH 8.9p1	🟢 Low
		8500	TCP	Consul Agent	🟡 Medium
Server-04	139.59.245.244	22	TCP	OpenSSH 8.9p1	🟢 Low
Server-05	143.198.94.161	22	TCP	OpenSSH 8.9p1	🟢 Low
Server-06	188.166.250.175	80	TCP	OpenResty (Web)	🟢 Low
		443	TCP	OpenResty (SSL)	🟢 Low
		9111	TCP	Redis Key-Value	🔴 High
Server-07	139.59.117.80	80	TCP	OpenResty (Web)	🟢 Low
		443	TCP	OpenResty (SSL)	🟢 Low
		9111	TCP	Redis Key-Value	🔴 High
Server-08	134.209.107.38	8085	TCP	Apache httpd	🟢 Low
		8500	TCP	Consul Agent	🟡 Medium
Server-09	146.190.97.129	8500	TCP	Consul Agent	🟡 Medium
Server-10	128.199.134.178	8500	TCP	Consul Agent	🟡 Medium
Server-11	167.172.66.204	6001	TCP	Uvicorn (App)	🟡 Medium
		8500	TCP	Consul Agent	🟡 Medium
Server-12	139.59.113.219	8000	TCP	Uvicorn (App)	🟡 Medium
Server-13	159.89.196.66	8500	TCP	Consul Agent	🟡 Medium
Server-14	139.59.230.32	22	TCP	OpenSSH 8.9p1	🟢 Low
Server-15	139.59.99.241	443	TCP	SSL Service	🟢 Low

3. 🛡️ Risk Assessment & Recommendations

🔴 Critical Findings (Immediate Action Required)

1. Exposed Database Services (Redis)

- Affected Assets: Server-06, Server-07
- Observation: Redis is listening on Port 9111 on a public interface.
- Risk: Unauthorized data access, data manipulation, or Remote Code Execution (RCE) if authentication is weak.
- Recommendation: Bind Redis to localhost (127.0.0.1) or restrict access via UFW firewall to trusted internal IPs only.

🟡 Warning Findings (Review Needed)

1. Public Management Interfaces

- Affected Assets: Server-02, 03, 08, 09, 10, 11, 13
- Observation: HashiCorp Consul (8500) and MinIO Console (9001) are accessible from the internet.
- Risk: Information disclosure regarding infrastructure topology.
- Recommendation: Place these services behind a VPN or strictly whitelist access to the corporate office IP.

---

4. ✅ Conclusion

The infrastructure follows a microservices architecture pattern utilizing Consul for service discovery and OpenResty for ingress. While the perimeter is generally functional, the exposure of data layers (Redis) and management planes (Consul/MinIO) contradicts the principle of least privilege.