📘 Scan Accuracy & Validation Report

Project: Review and Validate Scan Accuracy

Task Reference: DEV-356

Date: January 2026

1. 📋 Objective

The primary objective of this phase was to audit the results of the initial infrastructure scan (DEV-352) for Accuracy and Completeness. Specifically, this task aimed to:

1. Address "Retransmission Cap Hit" warnings generated by Nmap on high-latency hosts to ensure no ports were missed due to network congestion.
2. Manually verify "High Risk" findings (e.g., exposed databases) to rule out False Positives.

2. 🛠️ Toolchain & Techniques

We employed a "Trust but Verify" approach using secondary tools to cross-reference Nmap's findings.

Tool	Category	Command/Technique	Purpose
Nmap	Validation	-T3 --top-ports 1000	Slower, more reliable re-scan on laggy hosts.
Netcat	Manual	nc -zv [IP] [PORT]	TCP Handshake verification (Connectivity Check).
Curl	Manual	curl -I [URL]	Application Layer verification (Service Response).

3. ⚙️ Execution Methodology

Phase 1: Retransmission Error Resolution

Context: Initial scans using -T4 (Aggressive Timing) flagged packet loss on 3 specific hosts (157.230.47.60, 128.199.134.178, 146.190.97.129).

- Action: Executed a targeted re-scan on these IPs using a polite timing template (-T3) to eliminate network throttling.

- Command:

Bash

```
nmap -sV --top-ports 1000 -T3 -Pn --open -iL validation_targets.txt
```

Phase 2: High-Risk "True Positive" Verification

Context: Nmap reported critical assets (Redis, MinIO) as "Open." We needed to prove these were accessible to an external attacker.

- Action:
    1. Redis (9111): Used netcat to attempt a TCP connection.
    2. Consul (8500): Used curl to request the HTTP status code.

---

4. 📊 Validation Findings

🛡️ Integrity Check (Scan vs. Re-Scan)

Comparing the initial "Fast Scan" results against the "Validation Scan" to check for missed data.

Target Host	Initial Findings (T4)	Validation Findings (T3)	Discrepancy?	Status
157.230.47.60	Ports: 22, 53, 8500, 8600, 9000, 9001	Identical Match	None	✅ Verified
128.199.134.178	Ports: 22, 8500	Identical Match	None	✅ Verified
146.190.97.129	Ports: 22, 8500	Identical Match	None	✅ Verified

🎯 Manual Spot Checks (False Positive Analysis)

Confirming that reported services are actually reachable.

Asset	Port	Service	Method	Result Output	Verdict
Server-06	9111	Redis	nc -zv	(UNKNOWN) [...] 9111 (?) open	🔴 Confirmed Exposed
Server-02	9000	MinIO	nc -zv	(UNKNOWN) [...] 9000 (?) open	🟡 Confirmed Exposed
Server-02	8500	Consul	curl -I	HTTP/1.1 200 OK	🟡 Confirmed Live

---

5. ✅ Conclusion

1. Completeness: No additional ports were discovered during the slower re-scan, proving the initial warnings did not result in data loss.
2. Accuracy: All critical findings (Redis, Consul, MinIO) have been manually validated as True Positives.