



SCAN-20260130-025500

DATE: January 29, 2026

HOST: 1cebcfff2541d5493c00e85aa8352b05b715c9965975c8682bf434ad2e67524f

PATH: /Users/brucedombrowski/Security (Security)

SUBJECT: Automated Security Scan Attestation

1. Purpose

This document attests that automated security scans were executed against the subject host at the specified path using the Security Verification Toolkit. The scans verify alignment with NIST SP 800-53 security controls.

2. Scan Environment

- **Scan Timestamp:** 2026-01-30T02:53:32Z
- **Toolkit Version:** v1.17.10 (db60cd4)
- **Toolkit Repository:** <https://github.com/brucedombrowski/Security>

3. Host Inventory Reference

A host inventory snapshot was collected at scan time to establish a verifiable system thumbprint. This enables integrity verification while keeping sensitive machine data (MAC addresses, serial numbers) separate from shareable scan results.

| | |
|------------------------|-----------------------------------|
| Inventory File | host-inventory-2026-01-30.txt |
| SHA256 Checksum | 1cebcfff2541d549... |
| NIST Control | CM-8 (System Component Inventory) |

Note: The host inventory contains sensitive information. All scan outputs reference this checksum rather than embedding the actual data, allowing scan results to be shared without exposing machine-specific details.

4. NIST Control Mapping

The following NIST SP 800-53 Rev 5 controls were verified:



| Control | Family | Verification Method |
|---------|-------------------------------|-------------------------------------|
| CM-6 | Configuration Management | Host security posture |
| CM-8 | Configuration Management | Host inventory collection |
| RA-5 | Risk Assessment | Vulnerability scanning (Nmap/Lynis) |
| SA-11 | System & Services Acquisition | Secrets and credential scanning |
| SC-8 | System & Comms Protection | MAC address detection |
| SI-2 | System & Info Integrity | Flaw remediation assessment |
| SI-3 | System & Info Integrity | ClamAV malware scanning |
| SI-4 | System & Info Integrity | System monitoring (port scan) |
| SI-12 | System & Info Integrity | PII pattern detection |

5. Scan Results

| Scan | NIST Control | Result | Findings |
|--------------------|--------------|---------------------------|-----------------------------|
| Host Security | CM-6 | PASS | All checks passed |
| Vulnerability Scan | RA-5 | PASS | No critical vulnerabilities |
| Secrets Scan | SA-11 | PASS w/ exceptions | 16 reviewed exceptions |
| MAC Address Scan | SC-8 | PASS | No MAC addresses detected |
| Malware Scan | SI-3 | PASS | No malware detected |
| PII Scan | SI-12 | PASS w/ exceptions | 74 reviewed exceptions |

Summary: 6 passed, 0 failed

Overall Result: **PASS**

PASS w/ exceptions = reviewed exceptions documented in Section 6

6. Reviewed Exceptions

Items flagged by automated scans but reviewed and accepted as non-issues are documented in allowlist files. Each exception includes a SHA256 hash for integrity verification and reviewer justification.

6.1 PII Scan Exceptions

| | |
|-------------------|---------------------------|
| Allowlist File | .allowlists/pii-allowlist |
| SHA256 (first 16) | 420afc59fdf92c62 |
| Total Exceptions | 74 |



| # | Justification |
|----|--|
| 1 | Documenting localhost quick-accept feature |
| 2 | X.509 OID example, not an IP address |
| 3 | Version string example, not an IP address |
| 4 | Shell command syntax, not PII data |
| 5 | X.509 OID documentation note |
| 6 | X.509 OID for Email Protection (1.3.6.1.5.5.7.3.4) |
| 7 | X.509 OID for Document Signing (1.3.6.1.4.1.311.10.3.12) |
| 8 | Historical command log, not active PII |
| 9 | Placeholder pattern (build-time substitution) |
| 10 | LaTeX template placeholder (replaced at runtime) |
| 11 | Example/placeholder data (not real PII) |
| 12 | Example/placeholder data (not real PII) |
| 13 | Placeholder pattern (build-time substitution) |
| 14 | Localhost/loopback address (127.0.0.1) |
| 15 | Localhost/loopback address (127.0.0.1) |
| 16 | Localhost/loopback address (127.0.0.1) |
| 17 | Example/placeholder data (not real PII) |
| 18 | Placeholder pattern (build-time substitution) |
| 19 | Example/placeholder data (not real PII) |
| 20 | Placeholder pattern (build-time substitution) |

6.2 Secrets Scan Exceptions

| | |
|--------------------------|-------------------------------|
| Allowlist File | .allowlists/secrets-allowlist |
| SHA256 (first 16) | 093da78e91bea9a6 |
| Total Exceptions | 16 |

| # | Justification |
|----|---|
| 1 | Internal controlled variable assignment (safe eval) |
| 2 | Internal controlled variable assignment (safe eval) |
| 3 | Internal controlled variable assignment (safe eval) |
| 4 | Test fixture or mock data |
| 5 | Test fixture or mock data |
| 6 | Test fixture or mock data |
| 7 | Test fixture or mock data |
| 8 | Test fixture or mock data |
| 9 | Test fixture or mock data |
| 10 | Test fixture or mock data |
| 11 | Test fixture or mock data |
| 12 | Test fixture or mock data |
| 13 | Test fixture or mock data |
| 14 | Test fixture or mock data |
| 15 | Test fixture or mock data |
| 16 | Test fixture or mock data |

Note: Full details including file paths and SHA256 hashes are in the respective allowlist files.



7. Scan Output Checksums

The following SHA256 checksums were generated for scan output files:

| Scan Output File | SHA256 (first 16) |
|----------------------|---------------------|
| host-inventory | 1cebcfff2541d549... |
| host-security-scan | 105bbc48f13c9e3a |
| mac-address-scan | ac42be9e37f99288 |
| malware-scan | e5c17b50438ab273 |
| pii-scan | 663e4c560ca00c6d |
| secrets-scan | 40d52ba93b57c8bc |
| vulnerability-scan | |
| security-scan-report | e30afd2369863880 |

checksums.md SHA256 (full):

7933437ac2b22479c6c424155051ae3b5d516ee1b842b6f0a95a06c2fad66083

Full file names: *-2026-01-30-T025332Z.txt. The checksums.md file contains full SHA256 hashes for all scan outputs.

8. Verification Chain

This document establishes a chain of trust for verifying scan integrity:

Chain of Trust:

1. **Digital Signature** → This PDF is digitally signed, establishing authenticity
2. **checksums.md Hash** → This PDF includes the SHA256 hash of checksums.md (Section 7)
3. **Scan File Hashes** → checksums.md contains full SHA256 hashes of all scan output files
4. **File Verification** → Any scan file can be verified against checksums.md

Verification Commands:

```
# 1. Verify PDF signature (platform-dependent)
# 2. Extract checksums.md hash from PDF Section 7
# 3. Verify checksums.md integrity:
shasum -a 256 .scans/checksums.md

# 4. Verify all scan files against checksums.md:
cd .scans && shasum -a 256 -c checksums.md
```



9. Attestation

This document certifies that:

- (a) Automated security scans were executed against the subject host at the specified path
- (b) Scan results are accurately represented in this document
- (c) The Security Verification Toolkit version and commit hash are recorded for traceability
- (d) Detailed scan logs are available in the `.scans/` directory
- (e) The verification chain above enables independent validation of all scan outputs