
# Scan Methodology

Security Posture Analysis Tool

by Antibody Cyber Technology, LLC • Version 1.0.0

SPAT conducts a **15-check external scan** plus **2 SSH checks** against a target domain. All checks operate against the domain name — not a specific URL path. The tool queries public DNS, makes direct TLS/socket connections, issues HTTP requests via `curl`, and calls threat intelligence APIs using only the bare hostname (e.g. `example.com`).

The scan starts from a score of **100** and deducts points for each finding with a non-zero score_impact. The final score maps to a letter grade (A / B / C / F).

Checks run **sequentially** in the order listed. Errors in individual checks are captured and surfaced as INFO findings without halting the scan.

## Scoring Formula

```
Final Score = 100 − Σ(score_impact) → clamped [0, 100]
```

| Grade | Score Range |
|---|---|
| A | 80 – 100 |
| B | 65 – 79 |
| C | 50 – 64 |
| F | 0 – 49 |

## Checks (15 External + 2 SSH)

### [1 / 17] DNS Resolution

**Category:** DNS **Method:** socket.getaddrinfo(hostname)

| Condition | Severity | Deduction |
|---|---|---|
| Failed to resolve | HIGH | –20 |
| Success — IPs recorded | INFO | 0 |

## [2 / 17] TLS Certificate

**Category:** TLS/SSL **Method:** Python ssl module, port 443

| Condition | Severity | Deduction |
|---|---|---|
| Certificate expired | HIGH | –20 |
| Expires within 30 days | MEDIUM | –8 |
| Valid | INFO | 0 |
| Hostname mismatch / chain error | HIGH | –15 |
| Port 443 not reachable | HIGH | –15 |

Records: commonName, issuer, protocol version, cipher suite, days remaining.

## [3 / 17] TLS Protocol Versions

**Category:** TLS/SSL **Method:** ssl.SSLContext with pinned minimum/maximum_version

| Protocol | Classification | Deduction |
|---|---|---|
| TLSv1.0 | Weak (deprecated) | –10 |
| TLSv1.1 | Weak (deprecated) | –10 |
| TLSv1.2 | Strong | 0 |
| TLSv1.3 | Strong | 0 |

## [4 / 17] TLS Cipher Suites

**Category:** TLS/SSL – Ciphers **Method:** ssl module + custom SSLContext with set_ciphers()

### a) Forward Secrecy

Negotiates the default TLS handshake and examines the selected cipher suite. TLS 1.3 ciphers always guarantee forward secrecy. TLS 1.2 requires ECDHE or DHE. No forward secrecy → HIGH, deducts 10.

### b) Weak Cipher Acceptance

| Weak Suite | Severity | Deduction |
|---|---|---|
| RC4, 3DES, DES, NULL, EXPORT, aNULL | HIGH | up to –12 |

## [5 / 17] HTTP Security Headers

**Category:** HTTP Security **Method:** curl -sk -D - https://{hostname}/

| Header | Severity if Missing |
|---|---|
| Strict-Transport-Security | HIGH |

| Header | Severity if Missing |
|---|---|
| Content-Security-Policy | HIGH |
| X-Frame-Options | MEDIUM |
| X-Content-Type-Options | MEDIUM |
| Referrer-Policy | LOW |
| Permissions-Policy | LOW |

Deduction: 2 pts per missing header (capped at 12). Version disclosure in Server / X-Powered-By → LOW, –3.

## [6 / 17] HTTP→HTTPS Redirect

**Category:** HTTP Security **Method:** curl -sk --max-redirs 0 (port 80)

| Result | Severity | Deduction |
|---|---|---|
| First hop → https:// | INFO | PASS |
| Multi-hop chain → https:// | INFO | PASS |
| Chain never reaches HTTPS | MEDIUM | –5 |
| HTTP 200 with no redirect | HIGH | –8 |

## [7 / 17] CSP Quality Analysis

**Category:** CSP Analysis **Method:** curl -sk → Content-Security-Policy header

| Keyword / Condition | Context | Severity | Deduction |
|---|---|---|---|
| unsafe-inline | script-src / default-src | HIGH | –8 |
| unsafe-inline | style-src only | INFO | 0 (advisory) |
| unsafe-eval | script-src / default-src | HIGH | –6 |
| unsafe-hashes | any | MEDIUM | –4 |
| Wildcard * in script-src/default-src | | HIGH | –10 |
| object-src not none | | MEDIUM | –3 to –4 |
| No script-src / default-src | | HIGH | –8 |
| No upgrade-insecure-requests | | LOW | –2 |

## [8 / 17] Cookie Security

**Category:** Cookie Security **Method:** curl -sk -D - -A Mozilla/5.0 https://{hostname}/

| Missing Attribute | Severity | Deduction |
|---|---|---|
| Secure flag | HIGH | –8 |
| HttpOnly flag | MEDIUM | –5 |

| Missing Attribute | Severity | Deduction |
|---|---|---|
| SameSite attribute | MEDIUM | –4 |
| SameSite=None | MEDIUM | –3 |

No cookies set → INFO, no deduction.

## [9 / 17] CORS Misconfiguration

**Category:** CORS **Method:** curl -sk -H "Origin: https://evil.example.com" https://{hostname}/

| Result | Severity | Deduction |
|---|---|---|
| No ACAO header | INFO | 0 |
| ACAO: * (alone) | MEDIUM | –5 |
| ACAO: * + ACAC: true | CRITICAL | –20 |
| ACAO echoes hostile origin | HIGH | –15 |
| ACAO is specific trusted origin | INFO | 0 |

## [10 / 17] Email Security (SPF / DMARC / DKIM / MX)

**Category:** Email Security **Method:** nslookup / dig against 8.8.8.8

### SPF

| Policy | Status | Deduction |
|---|---|---|
| -all (hard fail) | PASS | 0 |
| ~all (soft fail) | WARN | –3 |
| ?all (neutral) | WARN | –6 |
| +all (allow all) | FAIL | –12 |
| Missing SPF | FAIL | –10 |
| Multiple SPF records | FAIL | –8 |

### DMARC

| Policy | Status | Deduction |
|---|---|---|
| p=reject | PASS | 0 |
| p=quarantine | WARN | –4 |
| p=none + strict align + reporting + sp=reject | WARN | –3 |
| p=none on non-email domain | WARN | –3 |
| p=none with no hardening | FAIL | –8 |
| Missing DMARC | FAIL | –10 |

### DKIM

Probes 10 common selectors: default, google, selector1, selector2, k1, dkim, mail, smtp, s1, s2. A valid key requires both p= and v=DKIM1. Active email domain with no key found → LOW, –2.

## [11 / 17] DNSSEC

**Category:** DNSSEC **Method:** dnspython (preferred) or dig (fallback)

| Result | Severity | Deduction |
|---|---|---|
| DNSKEY / RRSIG found | INFO | PASS |
| No DNSSEC records found | MEDIUM | –5 |

## [12 / 17] Port Scan

**Category:** Network **Method:** Concurrent socket.create_connection(), 1.5s timeout, 30 threads

Scans 21 common ports: 21 (FTP), 22 (SSH), 23 (Telnet), 25 (SMTP), 53 (DNS), 80 (HTTP), 110 (POP3), 143 (IMAP), 443 (HTTPS), 445 (SMB), 1433 (MSSQL), 1521 (Oracle), 2222 (Alt-SSH), 3306 (MySQL), 3389 (RDP), 5432 (PostgreSQL), 5900 (VNC), 6379 (Redis), 8080 (HTTP-Alt), 8443 (HTTPS-Alt), 27017 (MongoDB).

| Result | Severity | Deduction |
|---|---|---|
| Telnet (23) open | HIGH | –15 |
| High-risk ports open (RDP/SMB/VNC/Redis/Mongo/etc) | HIGH | –10 |
| Non-standard port open (not 22/80/443) | MEDIUM | –4 |
| Only expected ports open | INFO | 0 |

## [13 / 17] robots.txt

**Category:** Web **Method:** curl -skL https://{hostname}/robots.txt

Fetches robots.txt following HTTP redirects. A valid file must contain User-agent. Missing or empty → LOW, –1.

## [14 / 17] VirusTotal Domain Reputation

**Category:** Threat Intelligence **Method:** VirusTotal API v3 — /api/v3/domains/{hostname}

| Result | Severity | Deduction |
|---|---|---|
| ≥ 5 vendors flag malicious | CRITICAL | –25 |
| 1–4 vendors flag malicious | HIGH | –10 |
| ≥ 3 vendors suspicious | MEDIUM | –5 |
| Clean | INFO | 0 |
| Reputation score < –10 | HIGH | –5 |

Requires VIRUSTOTAL_API_KEY in .env. Queries the domain-level reputation endpoint.

## [15 / 17] URLhaus Malware Distribution

**Category:** Threat Intelligence **Method:** URLhaus API v1 — /v1/host/

| Result | Severity | Deduction |
|---|---|---|
| Live malware URLs active | CRITICAL | –25 |
| Historical URLs (now offline) | MEDIUM | –5 |
| Not found in database | INFO | PASS |

Requires URLHAUS_AUTH_KEY in .env.

### [16–17 / 17] SSH Algorithm Analysis + Auth Methods

**Category:** SSH **Method:** Raw TCP socket on configurable SSH port (default 22)

Both checks are skippable with --skip-ssh and can be isolated with --ssh-only.

#### Check 16 — SSH Algorithms

| Check | Weak Algorithms | Severity | Deduction |
|---|---|---|---|
| Protocol version | SSHv1 | HIGH | –20 |
| OpenSSH version | < 8.0 | MEDIUM | –8 |
| KEX algorithms | dh-group1-sha1, group14-sha1, etc. | HIGH | –10 |
| Encryption ciphers | 3des-cbc, arcfour, aes*-cbc, etc. | HIGH | –10 |
| MAC algorithms | hmac-md5, hmac-sha1, etc. | MEDIUM | –5 |
| Host key types | ssh-dss (DSA) | HIGH | –8 |

#### Check 17 — SSH Auth Methods

| Result | Severity | Deduction |
|---|---|---|
| Password authentication enabled | MEDIUM | –6 |
| Key-only authentication | INFO | 0 |

## Output Formats

| Format | Flag | Content |
|---|---|---|
| Terminal (colored) | `default` | Rich/ANSI with per-finding icons |
| JSON | `--json FILE` | Full structured data: findings, score, timestamp |
| HTML | `--html FILE` | Self-contained dark-theme report with score breakdown |

## Scan Profiles (GUI)

| Profile | Flags |
|---|---|
| Full Scan | All 17 checks |
| External Only | `--skip-ssh` (15 checks) |
| SSH Only | `--ssh-only` (2 checks) |
| Quick | `--skip-ssh` + no VirusTotal/URLhaus |

## API Key Configuration

Place a `.env` file alongside the executable or `spat_cli.py`:

```
VIRUSTOTAL_API_KEY=your_vt_key_here
URLHAUS_AUTH_KEY=your_urlhaus_key_here
```

Free API keys:

• VirusTotal: https://www.virustotal.com/gui/join-us

• URLhaus: https://auth.abuse.ch/