Stealthnet.ai

// FIND WHAT ATTACKERS WOULD FIND. BEFORE THEY DO.

SOC 2 Penetration Testing Checklist

// AUDIT_PREP --FRAMEWORK=SOC2 --TYPE=PENTEST

Use this checklist to verify your penetration testing program satisfies SOC 2 Type II requirements. **Evidence of testing must map directly to the Trust Services Criteria (TSC).** Auditors will look for scope documentation, methodology, findings reports, and remediation tracking.

CC6 — LOGICAL ACCESS | CC7 — SYSTEM OPS | A1 — AVAILABILITY | CC9 — RISK MGMT

01 SCOPE & PLANNING

CC3.2 / CC9.1

- [ ] Define **in-scope systems**: production environment, APIs, cloud infrastructure, and any cardholder/PII data stores — CRITICAL
- [ ] Obtain **written authorization** (Rules of Engagement) signed by system owner before testing begins — CRITICAL
- [ ] Document **testing methodology** (OWASP, PTES, NIST SP 800-115, or equivalent) — HIGH
- [ ] Set testing window and notify operations/IR team to avoid false incident triggers — MEDIUM
- [ ] Confirm **tester qualifications**: OSCP, CEH, or equivalent credentials documented for auditor review — MEDIUM
- [ ] Verify testing covers **all system components** in the SOC 2 system description boundary — HIGH

02 NETWORK & INFRASTRUCTURE

CC6.6 / CC6.7

- [ ] Perform **external network scan** to enumerate exposed ports, services, and public-facing assets — CRITICAL
- [ ] Test **firewall and network segmentation**; validate DMZ, VPC boundaries, and inter-segment access controls — CRITICAL
- [ ] Assess **VPN / remote access** configuration, authentication strength, and split-tunneling risks — HIGH
- [ ] Identify **unpatched services** and CVEs ≥ 7.0 CVSS on internet-facing hosts — HIGH
- [ ] Validate **DNS security**: zone transfer restrictions, DNSSEC, dangling DNS records — MEDIUM
- [ ] Test cloud infrastructure misconfigurations — S3 buckets, security groups, IAM role assignments — HIGH

03 APPLICATION SECURITY

CC6.1 / CC6.6

- [ ] Test for **OWASP Top 10**: SQL injection, XSS, SSRF, XXE, insecure deserialization, IDOR — CRITICAL
- [ ] Assess **authentication mechanisms** including brute force resistance, MFA bypass, session fixation — CRITICAL
- [ ] Evaluate **API security**: authentication, rate limiting, excessive data exposure, BOLA/BFLA — HIGH
- [ ] Validate **authorization controls** including privilege escalation, horizontal and vertical access violations — CRITICAL
- [ ] Review **encryption in transit**: TLS version, cipher suites, certificate validity, HSTS enforcement — HIGH
- [ ] Test for **secrets exposure** such as API keys, credentials, tokens in source/headers/error messages — HIGH

04 ACCESS CONTROLS & IDENTITY

CC6.1 / CC6.2 / CC6.3

- [ ] Verify **least privilege enforcement** by testing ability to access data beyond assigned role scope — CRITICAL
- [ ] Attempt **credential stuffing / password spray** against login endpoints; verify lockout policies — HIGH
- [ ] Test **MFA implementation** for OTP reuse, bypass via account recovery flows, SIM-swap risk — HIGH
- [ ] Validate **session management**: token entropy, expiry enforcement, logout invalidation — HIGH
- [ ] Assess **privileged access**: admin console exposure, bastion host security, PAM controls — CRITICAL
- [ ] Review **SSO/IdP configuration** for SAML assertion manipulation, OAuth token leakage — MEDIUM

05 DATA PROTECTION & ENCRYPTION

CC6.7 / CC6.1

- [ ] Confirm **data at rest encryption**: database encryption, disk encryption on all systems in scope — CRITICAL
- [ ] Test for **PII/sensitive data leakage** in logs, error messages, API responses, and debug endpoints — CRITICAL
- [ ] Assess **key management** for hardcoded keys, insecure storage, key rotation enforcement — HIGH
- [ ] Verify **data backup security**: backup encryption, access controls, off-site storage protections — MEDIUM
- [ ] Check **third-party data sharing** via API integrations transmitting data to external services — MEDIUM

06 DETECTION & RESPONSE VALIDATION

CC7.2 / CC7.3 / CC7.4

- [ ] Verify **SIEM/logging coverage** by confirming attack activity generates alerts during test window — HIGH
- [ ] Confirm **IDS/IPS detection** by running known attack signatures to validate detection fidelity — HIGH
- [ ] Test **incident response trigger**; notify IR team post-test; confirm they observed activity — CRITICAL
- [ ] Validate **log retention**; confirm logs are immutable and retained per policy (≥90 days for SOC 2) — HIGH
- [ ] Assess **mean time to detect (MTTD)** and document detection gaps identified during engagement — MEDIUM

07 AUDITOR EVIDENCE & REPORT REQUIREMENTS

CC2.2 / CC4.1 / CC4.2

// SCOPE_DOC

- [ ] Signed Rules of Engagement
- [ ] System description boundary map
- [ ] Methodology statement
- [ ] Tester credentials on file

// FINDINGS_REPORT

- [ ] Executive summary for mgmt
- [ ] Technical findings w/ CVSS scores
- [ ] Proof-of-concept for each finding
- [ ] Risk-ranked remediation list

// REMEDIATION

- [ ] Findings tracked in issue system
- [ ] Owners assigned per finding
- [ ] SLA defined (Critical: 30d)
- [ ] Retest / validation performed

// ATTESTATION

- [ ] Annual cadence documented
- [ ] Significant change re-testing
- [ ] Report shared with auditor
- [ ] Management sign-off on risk acceptance