Stealthnet.ai

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

CMMC Penetration Testing Checklist

// AUDIT_PREP --FRAMEWORK=CMMC2.0 --TYPE=PENTEST

Use this checklist to verify your penetration testing program satisfies **CMMC 2.0 Level 2 and Level 3 requirements** for defense contractors handling CUI and FCI. Testing must align to NIST SP 800-171 and 800-172 practice families; assessors will review scope, methodology, findings, and remediation evidence.

AC — ACCESS CONTROL | SI — SYSTEM INTEGRITY | CA — ASSESSMENT | IR — INCIDENT RESPONSE | IA — IDENTIFICATION & AUTH

01 SCOPE & AUTHORIZATION

CA.2.157 / CA.3.161

- [ ] Define **CUI boundary**: all systems, enclaves, and networks that store, process, or transmit Controlled Unclassified Information — CRITICAL
- [ ] Obtain **written Rules of Engagement** signed by the ISSO/FSO and prime contractor (if applicable) before testing begins — CRITICAL
- [ ] Confirm tester holds appropriate **clearance or citizenship requirements** per contract requirements (e.g. US Person, ITAR) — CRITICAL
- [ ] Document **testing methodology** referencing NIST SP 800-115, PTES, or equivalent — required for C3PAO review — HIGH
- [ ] Notify **ISSM and IR team** of test window to prevent false incident escalation to DCSA or prime contractor — HIGH
- [ ] Confirm coverage of **all system components** listed in the System Security Plan (SSP) and network boundary diagram — HIGH

02 NETWORK & ENCLAVE SECURITY

SC.3.177 / SC.3.180

- [ ] Test **CUI enclave isolation**: validate that non-CUI systems cannot reach CUI assets across segment boundaries — CRITICAL
- [ ] Perform **external perimeter scan** to enumerate internet-exposed ports, services, and unintended attack surface — CRITICAL
- [ ] Assess **remote access controls**: VPN authentication strength, split-tunnel risk, and managed device enforcement — HIGH
- [ ] Identify **unpatched systems** with CVEs scoring 7.0+ CVSS; CMMC requires timely patching under SI.2.216 — HIGH
- [ ] Validate **wireless network controls**: unauthorized AP detection, WPA3 enforcement, and rogue device exposure — MEDIUM
- [ ] Test **external-facing cloud services** for misconfigured storage buckets, public APIs, and IAM over-permissions — HIGH

03 ACCESS CONTROL & IDENTITY

AC.1.001 / AC.2.006 / IA.3.083

- [ ] Verify **least privilege enforcement**: attempt access to CUI assets beyond assigned role and document any violations — CRITICAL
- [ ] Test **multi-factor authentication** on all CUI-accessible systems; MFA is mandatory under IA.3.083 for Level 2+ — CRITICAL
- [ ] Attempt **privilege escalation** from standard user to admin on endpoints and servers within the CUI boundary — CRITICAL
- [ ] Run **credential attacks** (password spray, stuffing) against login portals; verify account lockout per IA.1.076 — HIGH
- [ ] Assess **shared/service account controls**: test for generic credentials, hardcoded passwords, and unrotated secrets — HIGH
- [ ] Validate **session termination**: confirm idle timeouts and forced re-authentication after inactivity per AC.2.013 — MEDIUM

04 SYSTEM & CONFIGURATION INTEGRITY

SI.1.210 / CM.2.061 / CM.2.062

- [ ] Test **endpoint hardening**: attempt exploitation of default configurations, unused services, and unnecessary open ports — CRITICAL
- [ ] Assess **anti-malware bypass**: use known evasion techniques to test EDR/AV coverage per SI.1.210 — HIGH
- [ ] Validate **software allowlisting**: attempt to execute unauthorized binaries on CUI workstations per CM.3.068 — HIGH
- [ ] Check for **unauthorized software** installed on in-scope systems; verify CM baseline enforcement and monitoring — MEDIUM
- [ ] Test **firmware and BIOS controls**: assess secure boot enforcement and physical access protection on CUI systems — MEDIUM
- [ ] Verify **patch status** across all in-scope assets; document any out-of-policy systems for POA&M tracking — HIGH

05 CUI DATA PROTECTION

MP.2.119 / SC.3.177 / SC.3.187

- [ ] Confirm **CUI encryption at rest**: FIPS 140-2/3 validated encryption on all storage media per SC.3.177 — CRITICAL
- [ ] Test **CUI in transit**: validate TLS 1.2+ on all data paths; flag any cleartext transmission of sensitive data — CRITICAL
- [ ] Identify **CUI sprawl**: test for uncontrolled copies of CUI in shares, desktops, email archives, or cloud sync folders — HIGH
- [ ] Assess **removable media controls**: test USB enforcement policies and DLP controls on CUI endpoints per MP.2.120 — HIGH
- [ ] Check **sanitization controls**: validate that decommissioned media containing CUI is properly wiped or destroyed — MEDIUM

06 DETECTION, AUDIT & INCIDENT RESPONSE

AU.2.041 / AU.3.045 / IR.2.092

- [ ] Verify **audit log coverage**: confirm all login attempts, privilege use, and CUI access events are captured per AU.2.041 — CRITICAL
- [ ] Validate **SIEM alerting**: confirm test attack activity triggered real-time alerts to the security operations team — HIGH
- [ ] Test **incident response capability**: verify IR team detected and documented test events per IR.2.092 requirements — CRITICAL
- [ ] Confirm **log integrity and retention**: logs must be tamper-resistant and retained per contract/DFARS requirements — HIGH
- [ ] Assess **DIBCAC/DCSA reporting readiness**: verify cyber incident reporting process meets 72-hour DFARS 252.204-7012 obligation — HIGH

07 C3PAO ASSESSMENT EVIDENCE & REPORT REQUIREMENTS

CA.2.157 / CA.3.161 / CA.3.162

// SCOPE_DOCS

- [ ] Signed Rules of Engagement
- [ ] SSP boundary / network diagram
- [ ] Tester qualifications on file
- [ ] CUI asset inventory tested

// FINDINGS_REPORT

- [ ] Executive summary for ISSO/FSO
- [ ] Technical findings w/ CVSS scores
- [ ] NIST 800-171 practice mapping
- [ ] Risk-ranked remediation list

// POAM_TRACKING

- [ ] Findings entered in POA&M
- [ ] Owner and due date per finding
- [ ] Remediation SLA: Critical 30d
- [ ] Retest / closure evidence

// ATTESTATION

- [ ] Annual cadence documented
- [ ] Significant change re-testing
- [ ] Report available for C3PAO review
- [ ] SPRS score updated post-remediation