

EXTERNAL & INTERNAL NETWORK PENETRATION TESTING

Avalon attacks your network like a real adversary from outside, then from an internal foothold to prove which weaknesses are actually exploitable.

THE PROBLEM WE ADDRESS

Most assessment work confirms controls are documented — not that they hold up under a real attack.

CA-8 and RMF/FISMA require exploitation-based testing for higher-impact systems — skip it, and it's an audit finding, not just a security gap.

WHAT WE DO

- Recon and enumeration of the real internet-facing attack surface
- Unauthenticated, OSINT-driven discovery of exposed assets
- Authenticated internal enumeration from an assumed foothold
- Post-exploitation and lateral movement (where scoped)
- Controlled exploitation that proves impact, without disrupting production
- Detection-and-response observation — do your defenses even notice?
- Findings report with evidence, severity, and CA-8/RA-5 control mapping
- Remediation matrix ranked by exploitability × mission impact

HOW WE DO IT

1 SCOPING & ACCESS

Rules of Engagement, authorization letters, and access/credentials confirmed before testing starts.

DELIVERABLE

Signed ROE

3 INTERNAL TESTING

Foothold-based lateral movement, privilege escalation, and access-to-data proof.

DELIVERABLE

Validated internal findings

2 EXTERNAL TESTING

Recon, enumeration, and controlled exploitation of internet-facing assets.

DELIVERABLE

Validated external findings

4 REPORTING & RETEST

Control-mapped findings, executive out-brief, and an optional retest once you've remediated.

HANDOVER

Final report + retest option

VALUE DELIVERED

- › **Exploitability proof, not just a scan list.** Every finding has been shown to be genuinely reachable — no time spent chasing theoretical risk.
- › **Audit-ready evidence.** Findings map to NIST 800-53 CA-8/RA-5, feeding your RMF Assess step and FISMA package directly.
- › **A detection check most scans skip.** Internal testing shows whether monitoring would actually catch a real intrusion.
- › **A fix list your team can execute.** Remediation is prioritized by exploitability × mission impact.

THE ONE THING TO REMEMBER

The named expert on the proposal is the one testing your network.

COMMONLY PROCURED AS

Network penetration testing / IT security assessment support

AT A GLANCE

Model	Fixed-price or T&M, scoped per engagement
Typical	2–4 wks active testing; 6–10 wks ROE to final report
NAICS	541512, 541511, 541519, 541611, 541690
UEI	Y9MXMMHY3HA1
CAGE	242T0
Standards	NIST SP 800-115, MITRE ATT&CK, PTES, NIST SP 800-53 (CA-8)

WHO WE WORK WITH

- › Capture manager scoping a security-testing subcontract line
- › ISSO / system owner preparing for an RMF Assess or annual FISMA cycle
- › CISO / IT security lead validating defenses before a real incident does

COMMITMENT TO QUALITY

Avalon is led directly by a PMP-certified founder with a decade of enterprise engineering experience where every engagement gets senior-level attention, never a subcontracted bench. Delivery follows NIST SP 800-53, RMF, and FISMA, evidence-backed and control-mapped by design. ISO 9001/27001 is on the roadmap as the pipeline scales.

Status: Small business federal contractor based in Los Angeles, CA

NIST SP 800-115

PTES

MITRE ATT&CK

NIST 800-53