AMERICAN
TECHNOLOGY
SERVICES

VAPT Setup Checklist

What to Expect When Launching a Penetration Test with ATS

Your Step-by-Step Prep for Testing, Reporting, and Real Results

A good penetration test does not begin with someone scanning your firewall. It begins with coordination. The best results come when your team and ours are aligned on scope, depth, approval, and next steps. This checklist explains what to expect from Day Zero to report delivery. It is not complicated, but it is deliberate.

Phase 1: Scope + Define

Lock in what's being tested and why.

- ☐ **Identify the systems, environments, and assets to test.**
  Cloud, on premises, hybrid, legacy, or SaaS. You choose what is in scope, and we can help map it if it is not clear.

- ☐ **Determine testing types: Black Box, White Box, or both.**
  We will recommend a strategy, but your approval determines how much access we simulate, from total outsider to partial insider.

- ☐ **Clarify compliance and reporting goals.**
  Are we doing this to meet regulatory requirements? Internal policy? Insurance renewal? Let's make sure the test aligns with what you need to prove.

- ☐ **Define timing and windows of acceptable testing.**
  Some tests hit live systems. If there are sensitive hours, operational blackouts, or specific constraints, this is when we map them.

- ☐ **Assign internal stakeholders for sign-off and follow-up.**
  Who authorizes the scope? Who gets the final report? Who needs to act on the findings? No confusion = a smoother process.

Phase 2: Testing + Execution

Here's what happens once we're cleared to proceed.

- ☐ **Reconnaissance and enumeration begin.**
  We start by identifying targets, services, domains, subnets, endpoints, and potential exposure, just as a real attacker would.

- ☐ **We observe a zero impact policy unless otherwise scoped.**
  No system disruption, no data alteration, no production interference unless we receive explicit authorization for stress testing or live exploit testing.

- ☐ **Zero-impact policy is observed unless otherwise scoped.**
  No system disruption, no data alteration, no production interference—unless explicitly authorized for stress or live-exploit testing.

☐ **Ongoing communication channel is established.**
We'll keep you posted if we uncover high-severity issues in real time, so you're not blindsided.

Phase 3: Delivery + Debrief

The part that makes all of it worth it

☐ **You receive the VAPT report, detailed, prioritized, and actionable.**
This is not just a PDF of problems. It is a strategic playbook that outlines what to fix, why it matters, and in what order.

☐ **We meet to walk through every major finding.**
One of our cybersecurity leads will guide your team through the report—explaining severity, impact, and recommendations.

☐ **You get clear, prioritized remediation guidance.**
We break down every critical finding with precise, environment-aware recommendations—so your team can act confidently, or you can loop us in to handle remediation as a service. Either way, you move fast and fix what matters.

What This Means

You're not just buying a test. You're launching a partnership designed to find what matters and help you fix it fast. The more prepared you are at kickoff, the more powerful your outcome will be.

Ready to get started?

We'll help define your scope and walk you through next steps.

info@networkats.com