ZIMOZI SOLUTIONS

Zi

FREE RESOURCE

Penetration Testing Scope Guide

How to scope, run and buy a pen test with confidence

Zimozi Solutions Pte Ltd | Singapore | Custom software, web, mobile and AI for startups and SMEs | zimozi.sg

> A practical guide for IT and security leads who are planning their first penetration test. If your company is growing, handling customer data, or facing questions from clients, regulators, or insurers about your security, a pen test is one of the clearest ways to find and fix real weaknesses before someone else does. This guide walks you through what a pen test actually is, the main types, how to scope one properly, what to expect, and how to pick a vendor you can trust. No jargon, no scare tactics, just what you need to run a smart engagement.

What Penetration Testing Is

A penetration test, or pen test, is a controlled, authorized attempt to break into your systems the same way a real attacker would. Skilled testers use the same tools and techniques as criminals, but with your permission and a clear set of rules. The goal is simple. Find the weaknesses that matter, show how they could be exploited, and tell you how to fix them before they cause harm.

A pen test is different from a vulnerability scan. A scan is automated and gives you a long list of possible issues, many of which turn out to be low risk or false alarms. A pen test adds a human. A tester decides which findings are actually exploitable, chains small issues together into a real attack path, and tests the things automation cannot, like business logic and how your systems behave under pressure. That human judgment is what separates a useful report from a noisy one.

Most quality pen tests follow recognized methodologies so the work is consistent and thorough. The two you will hear about most are PTES, the Penetration Testing Execution Standard, which covers the full engagement from planning to reporting, and the OWASP Web Security Testing Guide, which is the reference for web application testing. You do not need to memorize these, but it helps to know your vendor should be able to name the standards they follow and explain how they apply them.

The 5 Types of Penetration Tests

Network penetration testing. This looks at your infrastructure, the servers, firewalls, routers, VPNs, and other systems that connect your environment together. Testers probe for misconfigurations, weak or default credentials, unpatched services, and ways to move from one system to another once inside. You need this when you run your own servers or cloud infrastructure, when you have remote access in place, or when you simply want a baseline picture of how exposed your network is from the outside and the inside.

Web application penetration testing. This focuses on the apps your customers and staff use through a browser, including your customer portal, dashboard, or any site that handles logins and data. Testers check for issues like broken authentication, injection flaws, access control gaps, and business logic that can be abused, guided by the OWASP testing guide. You need this if you build or run any web app that holds sensitive data or processes payments, and it is often the first test SaaS and mid-market companies should prioritize.

Mobile application penetration testing. This covers iOS and Android apps and the way they store data, talk to your servers, and protect what is on the device. Testers look at insecure local storage, weak encryption, exposed API calls, and ways the app can be reverse engineered or tampered with. You need this whenever you ship a mobile app to customers or employees, especially if it handles accounts, payments, or personal information.

Social engineering testing. This tests your people rather than your technology, usually through simulated phishing emails, phone calls, or other attempts to trick staff into sharing access or information. The point is not to catch people out but to measure how well your team and your processes hold up against realistic attempts, and to guide training. You need this when staff have access to sensitive systems, when you want to test your security awareness program, or when phishing is a known risk for your industry.

Wireless and cloud testing. Wireless testing examines your Wi-Fi networks for weak encryption, rogue access points, and gaps that let someone bypass your perimeter from the parking lot. Cloud testing examines your AWS, Azure, or Google Cloud setup for misconfigured storage, over-permissioned accounts, and exposed services. You need wireless testing if you run office networks that connect to sensitive systems, and cloud testing if a meaningful part of your infrastructure lives in the cloud, which for most modern companies it does.

How to Write a Scope Document

A good scope document is the single most important thing you produce before testing starts. It tells the testers exactly what they can touch, how, and when, and it protects both sides if anything goes wrong. Work through these steps and write each one down.

1. **Define your assets and targets.** List the specific things to be tested. For network work, that means IP ranges and host names. For applications, that means exact URLs, app names, and API endpoints. Be precise. Our website is not a target. The address app.yourcompany.com and its login API is.
2. **Describe the environment.** State whether testing runs against production or a staging copy. Note any systems that are fragile, shared with third parties, or business critical. If you use a staging environment, confirm it genuinely matches production, or the results will not reflect real risk.
3. **Set the rules of engagement.** This is the heart of the document. Decide which techniques are allowed and which are off limits. Common questions include whether denial of service testing is permitted, whether social engineering is in scope, and how far testers may go once they gain access. Write down who the authorized contacts are and how testers should report a critical finding immediately if they discover one mid test.
4. **Agree the timing.** Define the testing window, including start and end dates and the hours of day testing may run. Some organizations prefer off hours to limit any impact on live users. Make sure your own team knows the test is happening so alerts from your monitoring tools are not mistaken for a real attack.

5. **List the exclusions.** State clearly what is out of scope. This might include third party services you do not own, specific production systems that cannot tolerate any disruption, or certain attack types. Anything not listed as in scope should be treated as out of scope by default.
6. **Set the success criteria.** Define what a good outcome looks like. Are you testing for compliance with a specific standard, validating a fix from a previous test, or getting a broad first assessment. Clear goals help the testers focus and help you judge whether the engagement delivered.

Once the document is written, both you and the vendor should review and sign it before any work begins. An authorized person on your side must give written approval. If a vendor wants to start testing without a signed scope, treat that as a warning sign.

What to Expect During and After a Test

Timeline. Most pen tests for small and mid sized companies run from one to three weeks of active testing, depending on scope, followed by time to produce the report. Your vendor should give you a clear schedule up front, including a firm date for the final report.

What the testers do. A typical engagement follows recognized phases. It starts with planning and reconnaissance, where testers gather information about your targets. Then comes scanning and analysis to map weaknesses, followed by exploitation, where they safely attempt to take advantage of those weaknesses. Throughout, professional testers work carefully to avoid disruption and stay within the agreed rules. If they find something serious, like a path to sensitive data, a good team will pause and alert you right away rather than waiting for the report.

The deliverable report. The main product of a pen test is the report. A strong one includes an executive summary written in plain language for leadership, a detailed technical section for your team, and for each finding a clear description, a risk rating, evidence of how it was exploited, and specific, actionable remediation advice. The findings should be prioritized so you know what to fix first. If a report is just a printout of automated scanner output, it is not a real pen test.

Remediation and retest. Finding issues is only useful if you fix them. After you receive the report, your team works through the prioritized findings. A good vendor offers a retest, where they verify that your fixes actually closed the gaps and did not introduce new ones. Many engagements include one round of retesting, and you should confirm whether yours does. Plan time and budget for remediation, because that is where the real security improvement happens.

Red Flags When Selecting a Vendor

Choosing the right vendor matters as much as the test itself. Watch for these warning signs.

1. **A flat quote with no questions asked.** A vendor who gives you a price without asking detailed questions about your environment is probably underscoping the work, which means critical assets may be missed. Proper scoping always comes before a real quote.

2. **Vague methodology.** Phrases like industry standard testing with no specifics are a red flag. A credible vendor can name the standards they follow, such as PTES or OWASP, and explain how they apply to your systems.
3. **Automated scans dressed up as a pen test.** Some firms run a scanner and hand you the output as if it were a manual test. Ask directly how much of the work is manual. A genuine pen test involves skilled people making decisions, chaining findings, and testing business logic that tools cannot reach.
4. **No relevant certifications.** Ask about the lead tester's qualifications. Recognized certifications like OSCP, GPEN, or GWAPT signal real hands on skill. If the people doing the work hold none of these, be cautious.
5. **Unwillingness to define scope in writing.** A vendor who will not clearly agree what is in and out of scope, in a signed document, is setting up disputes later. Push for a written scope both sides sign before testing starts.
6. **Vague timelines and a weak sample report.** Good vendors commit to a report delivery date and can show you a redacted sample so you know what you are buying. If they dodge questions about timing or refuse to share a sample, keep looking. The report is what you are paying for.

Request a Pen Test Quote

Ready to get a clear, honest picture of where your security stands? Zimozi Solutions runs penetration tests scoped to your environment, with manual testing led by certified professionals, plain language reporting, and a retest to confirm your fixes worked. We will start by understanding your systems, then give you an accurate quote, never a guess.

Book a call with our security team or reach out through zimozi.sg to request your penetration testing quote. Let us help you find the gaps that matter and close them with confidence.