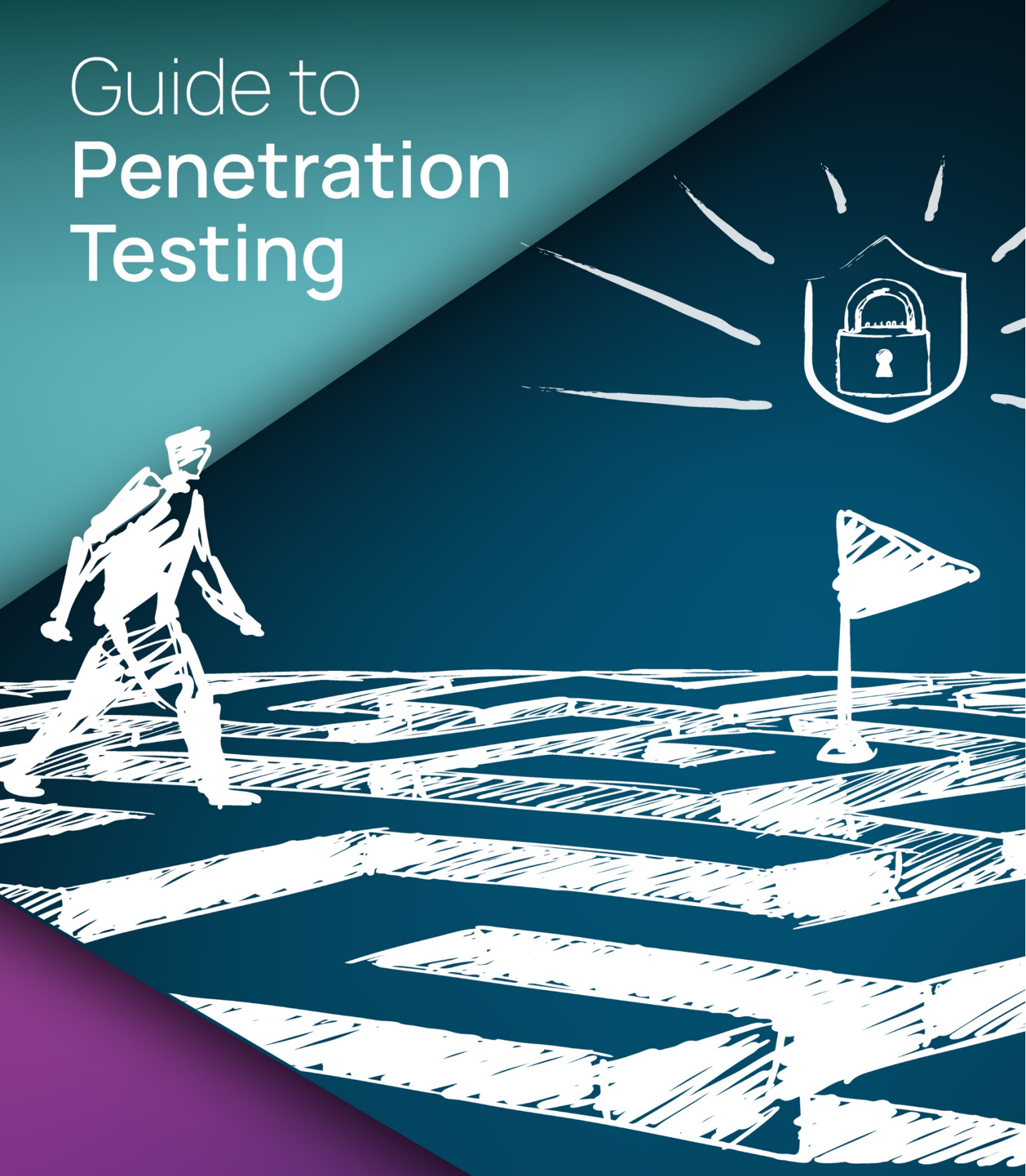
# Guide to **Penetration Testing**



evalian

*This extensive guide will give you a detailed overview of penetration testing. You can use the table of contents in the right hand side bar to navigate to different sections.*

## Introduction

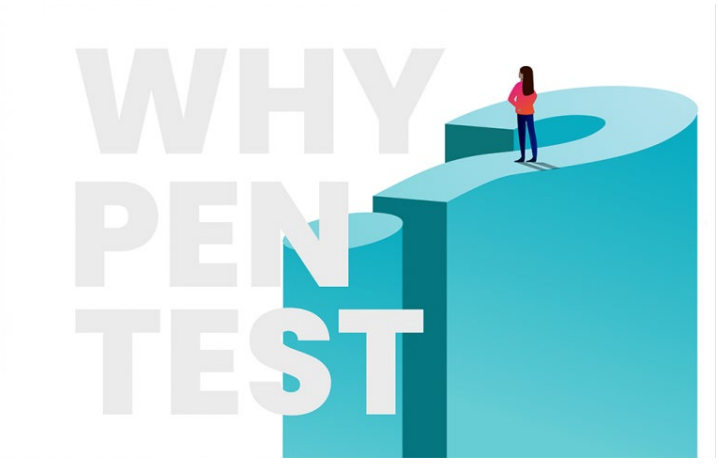
Penetration testing is a common way for companies to gain assurance and information about the security of their IT infrastructure. But for many, it's seen as a dark art, carried out by hoody-wearing geeks with confusing terminology and (excuse the pun) impenetrable reports that can be hard to interpret, let alone act on.

In truth, while pen testing can be a complex and highly technical field to work in, a good testing partner will guide you through the process and provide usable reports to help quickly improve a company's security posture. When carried out over a period of time, pen testing provides valuable input into tracking the maturity of your security programme.

In this article, we're going to break down the many different aspects of penetration testing and dispel the myths surrounding it.

## Why Pen Test?

Without getting too philosophical, computer systems are an inherently human construction. We design them, build them, and operate them. They're also ferociously complex, requiring years of training and experience to work with. No single person, however intelligent, understands every aspect of computers or their security.



As such, they are as flawed as their creators. Even the best IT architects, developers, and administrators work within their constraints, with misconfigurations, workarounds, changing requirements and differing feature sets making every IT system unique. Despite our best efforts, computer systems are hard to secure and constantly changing, and some people are out to take advantage of that fact.

Pen testing is the most widely recognised approach to carrying out in-depth reviews of computer systems and encompasses many different techniques and methods to assess their security. Pen tests can focus on individual applications and tools or look holistically at a wider system to identify security issues that present a risk to the business. This gives us the opportunity to fix those problems before a bad guy gets there first.

## Vulnerability Assessment or Penetration Test?

A common place to start gathering information about the security of a computer system is with a vulnerability assessment. Commercial, off-the-shelf tools are used to scan the network and gather information about vulnerabilities, misconfigurations, and missing updates on servers, computers and other devices on the network, all of which is collated into a report.

Activities can then be targeted to fix those vulnerabilities and make sure systems are updated and properly configured. This is a valuable exercise and one which should be carried out regularly, probably once a month for most companies.

Vulnerability Assessments are also a component of penetration testing, and commonly form one aspect of the final report. However, penetration testing goes a step further by focusing on those high-value vulnerabilities and misconfigurations that could be exploited by a criminal hacker and validating whether an attack could be successfully mounted against them.

Using real-world exploit techniques and bespoke tooling, a pen test uses benign payloads to validate whether an exploit will work and demonstrate the end result of such an attack. The subsequent report shows how an attack on one system or component can be turned into part of a larger, more complex attack, adding significant detail to a basic vulnerability assessment.

Our vulnerability assessment services

## Internal & External Infrastructure Testing

Most companies still take a traditional “walled garden” approach to securing their networks. The important servers, desktops and underlying IT infrastructure are placed behind a firewall protecting them from the wilds of the Internet, with a few small windows opened to allow necessary information to flow in and out of the network.

This Trusted vs Untrusted model presents a challenge to attackers, and means they have to be inventive in their attempts to access the company's crown jewels: an attacker starting with nothing needs to discover ways to get into the network.


Penetration testing of the external parts of a company's network helps to identify those systems and servers that are presented to the Internet, whether they be email servers, websites, application servers, file transfer tools or other publicly accessible resources, and discover the ways in which an attacker may try to subvert them.

Conversely, if an attacker successfully breaches the outer wall and gains a foothold *inside* the network, internal testing gives a view of what they might find once they're there. A vulnerability assessment typically isn't aware of every application bug, system, device or default password, and has no awareness of how they interact with one another. Internal testing helps to create that bigger picture and use an attacker's mindset to focus on the weak links.

This approach holds true for cloud-based assets as well. In order to use cloud-hosted systems, access must be provided for corporate users to build and configure them, and for customers and partners to use the resources once published. Assessing these systems is equally as important as for traditional networks, and ensures data is not exposed or left unprotected.

Our infrastructure testing services

## Web Application Testing

Earlier we touched on the public-facing resources a company may have earlier, and Web Applications make up a large proportion of those systems. These might include web-based email systems such as Outlook Web App, HR platforms, collaboration via SharePoint or an FTP tool, or other bespoke systems used by the company.

Increasingly these applications are moving into SaaS platforms – Software as a Service – where the software maker hosts it online on your behalf. However, it's still common for these systems to be built and hosted on company-managed infrastructure, with access to them made available via a web server accessible over the internet.

Regardless of the approach, these systems can hold highly sensitive information about the business or the people who work for it, making them valuable targets for hackers and are not immune to vulnerabilities or misconfigurations.

Web application testing is an aspect of penetration testing that focuses on these applications, testing the application itself for flaws that an attacker could use to compromise the app and the data it processes. SaaS tools don't get off lightly either, as a good web app test includes assessing apps and services hosted by third parties.

Our web app testing services

## Mobile Application Testing

In a similar vein to web app testing, mobile app testing looks at applications designed and built to run on mobile devices, such as phones as tablets. Modern mobile devices offer many security features for apps, such as Apple's Secure Enclave, sandboxing, app signing, encryption, data isolation, authentication and privacy features, and secure communications. However, these features are entirely optional, and a poorly designed app may fail to properly incorporate secure functionality.

Mobile app testing is a way to ensure the apps your company designs and uses work in a secure manner and protects the data they process and store. App testing, whether it be for mobile or traditional desktop applications, is commonly done throughout the development lifecycle. However, it's equally common to leave the *security* testing until the end of the development programme. For the highest levels of assurance, security testing should be.

Our mobile app testing services

## Other Testing Types

We've looked at the main elements of a penetration test, where the testers emulate the methods and tactics of a criminal hacker, but from a wider assurance perspective, there are many additional testing and assessment activities that can form part of a larger engagement.

Sticking with the more combative activities, simulated phishing can provide a valuable assessment of staff security awareness and identify weaknesses in processes or training. This can be expanded into related social engineering techniques such "vishing" (voice phishing) or physical pen tests – bypassing physical security measures to gain access to buildings or restricted areas.

Configuration assessment reviews can also provide assurance that underlying technical systems are configured to appropriate standards, including:

- Firewall configuration and rule sets
- Network segmentation and configuration
- Wireless network security
- Operating System configuration
- Virtualisation and data storage platforms
- Virtual desktop infrastructure
- Cloud and cloud app security
- API assessments
- Static code review

## Red Team Testing


So far we've focussed on well-defined, carefully planned activities where the testers are working to assess a particular system, app, tool or platform. This is often referred to as White Box testing, where the Pen Testers are working closely with internal technical teams to carry out controlled tests in a non-destructive manner.

This approach is excellent for providing a high level of all-round assurance that systems are well configured and tested to a particular standard or baseline. Many companies will stop there, content that their systems are well run and provide a generally good level of security.

However, this approach doesn't accurately reflect the real world, where an attacker could come from any angle at any time and exploit security weakness in unexpected ways. It doesn't test how people, processes and technologies work under stress and in the face of the unknown.

For a more accurate test of real-world resilience, we call on the Red Team.

The Red Team is still working *for* you – they're not out to deliberately cause damage to your systems – but they're not working *with* you. The Red Team acts like a bad guy and will typically have a loose goal, such as to gain access to a HR system or to extract a website's underlying database, but will be given free rein to do so however they can.

To make life harder for them, the Red Team will often start with very little information beyond knowing the given target, making this a "Black Box" test. This forces the Red Team to act in the same way an attacker would, gathering information about the systems they're targeting and identifying the weaknesses they can exploit, simulating a real-world attack.

They have the remit to try and achieve this goal using all the tools, techniques and tactics at their disposal. You won't know when the simulated attack will start, which systems they will target, or what methods they will use to achieve their goal.

A Red Team test is designed not only to prove how easy or difficult it might be for the attacker, but also to assess the defensive response to the attack. The defenders, or Blue Team, are typically made up of your IT team, security team, and maybe an MSP or MSSP, plus all their security tools and controls. The Blue Team's ability to detect and thwart the Red Team is an equally valuable outcome of the activity.

A Red Team test is an excellent way to assess the effectiveness of defences and the capabilities of detection tools such as SIEM, Antimalware, firewalls, IPS/IDS/FIM etc. More importantly, it helps to identify if the necessary systems and processes are in place and fully working to enable the company to successfully prevent a targeted cyber-attack.

## When Should You Pen Test?

Pen testing covers such a range of activities that it can be used as an assurance tool in many ways and at different times.

Most commonly, a standard pen test is carried out annually in support of certification activities for one of the many security standards, such as Cyber Essentials, ISO 27001, PCI-DSS or NIST 800-53.

Alternatively, a programme of testing activities could be spread throughout the year, focussing on different systems each time, coinciding with the release of new apps or to test substantial system changes. Similarly, these activities could vary in approach from a static code analysis one month, to a Red Team activity the next or testing app security against one of the many methodologies such as OWASP or OSSTM.

## Benefits of Penetration Testing

Most business decisions are ultimately based on the management of risk, whether it be threats from cyber attackers or the opportunities presented by new products or services. Pen Testing provides the technical foundation for assessing risk across IT systems and gives assurance to customers, investors and partners across the supply chain.

There are many good reasons to carry out penetration testing, including:

**Identifying and fixing security problems** – if your systems or applications have vulnerabilities, you want to know what they are, what is affected and how to fix them. You also want to know the risk - does it need fixing today, or can it wait a little longer, especially if the fix means system downtime?

**Ensuring compliance** - this is increasingly important with the introduction of legislation such as NIS and GDPR which set specific security obligations. GDPR, for example, requires “a process for regularly testing, assessing and evaluating the effectiveness of technical […] measures for ensuring the security of the processing". Likewise, if you are subject to PCI DSS it’s mandatory to pen test your cardholder data environment at least annually.

**Supply chain and contractual obligations** - buying organisations are starting to set minimum security standards in contracts with their supply chain. These commonly mandate specific controls or compliance with standards such as NIST 800-53, which defines pen testing as a core technical control, and ISO 27001 which focusses on regular vulnerability assessment and evaluating exposure, usually achieved by pen testing.

**Secure development** - even with security testing being carried out earlier during

development as part of a DevSecOps culture, there is still a need to test code regularly and ideally before major releases of internet facing applications to ensure that vulnerabilities, such as the OWASP Top 10, are not present. Pen testing therefore forms a key part of your secure software development life cycle.

**Assurance** – ultimately you want peace of mind by knowing that your security posture is strong, that there are no obvious gaps in your IT systems or application that an attacker could exploit, and your data is protected. No organisation wants to suffer a data breach and have to deal with the reputational and financial fall-out that follows. Pen testing doesn't guarantee you won't be hacked, but it will help ensure your systems are resilient to an attack.

Building a programme of testing in a repeatable cycle develops security practices and helps to baseline improvements over time.

## Contact us

**Telephone**

03330 500 111

**Email**

hello@evalian.co.uk

**Head Office**

West Lodge, Leylands Business Park, Colden Common, Hampshire, SO21 1TH

**London Office**

10 Fitzroy Square, London W1T 5HP

**Manchester Office**

Jactin House, 24 Hood Street, Ancoats, Manchester, M4 6WX

**Dublin Office**

69 Main Street, Blackrock, Dublin, Ireland, A94 N6D0

## Visit

**www.evalian.co.uk**