What is a Penetration Test and Why Do I Need It?

Hacking through a company's security protections used to require a lot of time and skill. However, today's technological advances make it easier than ever for bad actors to find an organisation's most vulnerable points. The purpose of penetration testing is to help businesses find out where they are most likely to face an attack and proactively shore up those weaknesses before exploitation by hackers.

Get the security and technical expertise needed to conduct successful penetration testing by partnering with Defence Logic. Our security professionals have years of experience helping organisations protect their information through ethical hacking.

What Is Penetration Testing?

Organisations can define penetration testing by what it is meant to assess. That includes all networks, applications, devices, and physical security components. It mimics the actions of malicious actors. Experienced cybersecurity experts leverage penetration testing to improve a company's security posture and remove any vulnerabilities that open it to attack.

When appropriately done, penetration testing goes beyond merely stopping criminals from unauthorised access to a company's systems. It creates real-world scenarios that show businesses how well their current defences would fare when confronted with a full-scale cyber-attack.

Why Do I Need a Penetration Test?

Penetration testing is an everyday part of our job description at Defence Logic. In fact, it's our speciality. Something else we deal with almost daily, though, is answering the question: "What is a penetration test, and why do I need it?"

Penetration tests let companies evaluate the overall security of their IT infrastructure. A company may have robust security protocols in one area but be lacking in another. The high cost of a successful cyber attack means no company should wait for a real-world scenario to play out before going on offence. Using penetration testing tools to expose holes in a business's security layer allows security experts and Pen Testers to address any shortcomings before they become critical liabilities.

+ Test Security Controls — Gain insights into the overall health of your application, network, and physical security layers.
+ Find Real-World Vulnerabilities — Expose endpoints in your computer systems most susceptible to attacks from adversaries.
+ Ensure Compliance — Companies can maintain information security compliance with industry standards for penetration testing.
+ Reinforce Security Posture — Penetration testing assists businesses in prioritising and addressing their vulnerability with a security program.

What Are the Benefits of Penetration Testing?

When it comes to who typically performs a penetration test, it is entities that are responsible for protecting private citizens' information. Even the best IT department may not have the objectivity needed to find security flaws that could expose an organisation to hackers. When it comes to who typically performs these functions, it's best to have a penetration tester conduct black-box, white-box testing, and other security assessments from the outside.

Having someone separate from the business conduct intrusion tests can provide value in the following ways:

Determine the feasibility of security holding up under different kinds of cyberattacks.

+ Show how the exploitation of low-risk vulnerabilities could lead to much damage at higher levels.
+ Detect harder-to-find risks through automated network and application scanning
+ Assess and quantify the potential impacts on operational and business functions
+ Judge how successfully network defences perform when faced with an attack
+ Quantify the need for more significant investment in security technology and personnel.
+ Help thwart future attacks by implementing and validating updated security controls.

Equipping your organisation with smart, actionable security measures after our penetration testing services is critical. Pen testing shouldn't be limited to a one-time effort. It should be part of a system of ongoing vigilance to keep organisations safe through various types of security testing. Updates to security patches or new components used in a company website could expose new risks that open the door to hackers. That's why companies should schedule regular penetration testing to help uncover any new security weaknesses and prevent any opportunity to exploit vulnerabilities.

What Are the Different Types of Penetration Testing?

Network vulnerabilities typically fall into three categories: hardware, software, and human. Let's look at different testing types to understand more about what a pen test consists of and what types of potential vulnerabilities your business is facing;

Web Application Pen Testing

Web App Penetration tests search out places in an application open to exploitation by a hacker. Installing a new third-party component that allows viewing sensitive data on a company website could provide an opening into company systems. Security consultants carry out attack simulations designed to:

+ Find application security flaws.
+ Summarise the risks they present to a company.
+ Provide insights into how to address the flaws.

Defence Logic uses experts who come from an application development background. The use of that experience to zero in on issues common to web development and to develop actionable remediation strategies to address web application vulnerabilities like:

+ Cross-Site Request Forgery
+ Injection Flaws
+ Weak Session Management
+ Cross-Site Scripting
+ Insecure Direct Object References

Network Security Pen Testing

When it comes to network security, experts use network penetration tests to find places a hacker might exploit in various systems, networks, network devices (think routers, switches), and hosts. They look for ways a hacker might find real-world opportunities to compromise a company, gain access, or unauthorised access to sensitive data. Many also try to take over the company's systems for malicious purposes.

Defence Logic uses focused network infrastructure penetration testing to identify system-level and network flaws like:

+ Misconfigurations
+ Product-specific Vulnerabilities
+ Wireless Network Vulnerabilities
+ Rogue Services
+ Weak Passwords
+ Inadequate, Inconsistent or Non-Existent Password Protocols

It helps to have security experts with a background in supporting systems, networks, and hosts. That experience allows penetration testers to come up with intrusion tests that ultimately improve an organisation's security posture.

Physical Penetration Testing

Physical penetration testing measures the strength of a company's existing security controls. It looks for any weaknesses vulnerable to discovery and manipulation by hackers. They may compromise physical barriers like sensors, cameras, and locks to gain physical access to sensitive business areas. That could lead to data breaches through compromising systems and networks.

Some of the industries most concerned about these kinds of attacks include:

+ Banking Institutions
+ Technology Firms

- Healthcare Institutions
- Government Services
- Hospitality Services
- Retail Services
- Armoured Transport Services

Leveraging physical penetration testing helps organisations stop unauthorised access into secure environments. It also provides invaluable insights into remedial guidance and ways to correct critical issues.

Cloud Security Penetration Testing

Cloud security pen tests are essential in helping companies invested in cloud technology protect vulnerable assets. The flexibility and autonomy offered by solutions like Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) technology also expose organisations to new security threats.

With Defence Logic and our testing methodology, companies get experts who understand the risks associated with using cloud technology. They look for potential exposures from an organisation's application, network, and configuration in a business's cloud set up that could give hackers access to:

- Company Credentials
- Internal Systems
- Sensitive Data

Companies receive feedback on any identified security gaps and steps they should take to fix the vulnerabilities before outside threats discover them.

IoT Security Penetration Testing

IoT security pen tests focus on exposing any hardware and software flaws that could allow bad actors to access a business's sensitive data or take over company systems. They examine the different components in IoT devices for vulnerabilities like:

- Weak Passwords
- Insecure Protocols
- Insecure APIs
- Insecure Communication Channels
- Misconfigurations
- Product-specific Vulnerabilities

Defence Logic experts apply a layered methodology to help spot weaknesses before a hacker finds them.

What Are the Different Stages of Penetration Testing?

Information Gathering

Penetration testers and stakeholders make sure they are in sync with the expected outcomes of each test. Security experts do surveillance on the target, gathering the information needed to scope and execute each test properly. The information gathering can be active (allowing the tester direct contact with the target) or passive (the tester collects information while remaining undetected by the target).

The information-gathering stage also involves:

- Deciding what tests to run.
- Determining who will be responsible for monitoring tests.
- Designating the information testers have when starting each test.

Threat Modelling

During this phase, the security team maps out threats that could attack or harm a company. They use the insights obtained during the information-gathering phase to inform the activities to execute during various penetration tests and develop risk rankings for different vulnerabilities. The team also identifies and categorises different assets for testing. Questions that penetration testers should ask during this stage include:

- What are the primary and secondary assets to consider?
- Who or what are the most prominent threats or threat communities to the organisation?
- How does each of those threat communities relate to different assets?

Vulnerability Analysis

Based on the information gathered in previous stages, the company and the security team decide which assets to eliminate. They confirm systems, devices, networks, systems, and other components that present the most risk through research, testing, and validation.

Exploitation

The security team relies on the groundwork put in place during earlier stages to begin penetration testing. They do everything possible when it comes to abusing, abusing, and exploiting systems deemed vulnerable. Defence Logic penetration testers cover all networks, devices, physical controls, and human interactions while documenting any potential holes that present a risk to a company's security posture.

Post-Exploitation

During the post-exploitation phase, pen testers look at the extent of the damage that a hacker could potentially cause by compromising a weakness found in a component. They examine the value of any compromised sensitive data and how a hacker could gain control of company systems. The post-exploitation phase also explores what it would take for a company to recover from malicious actors' breaches.

Reporting

Defence Logic creates reports outlining the steps taken during the entire penetration testing process. They highlight successful attempts to compromise company security, where they found openings for possible exploitation and other relevant information. Clients receive recommendations on ways of mitigating the risks associated with each security weakness.

How Often Should You Do Penetration Testing?

Companies should plan on conducting regular penetration testing. Regularly scheduled penetration testing allows businesses to locate and mitigate security risks. Businesses should also call in experts like Defence Logic for penetration testing whenever the following changes occur:

- Adding network infrastructure
- Applying security patches
- Performing upgrades to applications or other Infrastructure
- Modifications to end-user policies
- Establishment of new office locations
- What Should You Do After a Penetration Testing?

Use the opportunity presented by penetration testing to go over plans about how to strengthen your overall security posture. They offer organisations a chance to go over the results with all stakeholders and assess what must happen to improve company security.

Businesses should turn the outcomes presented to them by penetration testers into actionable insights. Decision-makers within the company can use that information to spur any needed changes to current security protocols. They can also go forward with any needed technology changes that address the risks uncovered during intrusion testing.

How is Penetration Testing Done?

Defence Logic uses various automation processes and tools to execute penetration testing and expose vulnerabilities. Pen testing tools and automated tools look for issues like weak data encryption and hard-coded values within application code like passwords. They help companies find out how well their organisation complies with the current security policy. It's also an excellent way of measuring employee security awareness at all levels of the organisation.

Pen testers typically execute within defined parameters. Limiting the scope of where they operate keeps the focus on different elements of a company's systems, networks, applications, and physical structures.