Penetration Testing

EISL

Elmdale IT Services Ltd

elmdaleit.co.uk

What is a Pen Test?

Penetration testing, also referred to as Pen Testing or ethical hacking is an authorised attack on a computer system, such as network, web/mobile application or a Wi-Fi network. Pen Testing simulates exactly what a hacker would do, which helps an organisation to understand any security weaknesses that could be exploited by an hacker.

By assessing if an IT System is susceptible to a cyber attack you will be able to plan, repair and strengthen your organisation's defences against such an attack. An internal Pen Test is undertaken within an organisation's network, searching for vulnerabilities from within. An external Pen Test is performed remotely, with an ethical hacker looking for security vulnerabilities in internet-facing assets such as FTP and mail servers.

Good security practise involves regular testing of your IT infrastructure for vulnerabilities and exploitable weaknesses.

Internal

A test to identify and exploit any weaknesses within your internal infrastructure.

External

A test to identify and exploit any weaknesses within your perimeter and public facing systems.

Vulnerability Assessments

An automated procedure using a range of scanners and tools to identify vulnerabilities.

Wi-Fi

A test to identify and exploit any weaknesses within your wireless network systems.

Web App

A test to identify and exploit any weaknesses within any software or website which is managed by you organisation.

Elmdale is a Crest certified provider of Penetration Testing services, providing you with assurance that our approach and methodology is approved at the highest level.

How it works

Intelligence Gathering

This phase of the engagement involves using a range of tools and techniques such as active scanning, open-source intelligence (OSINT.)

This involves using public sources such as websites or other data points to detect data leaks, accidental data exposure and software or hardware versions

Vulnerability Analysis

The vulnerability analysis aims to discover and identify security weaknesses that can be exploited by an attacker.

The flaws can be misconfigurations or insecure platforms. Techniques used vary from automated vulnerability scanners, metadata analysis, traffic monitoring, public research, common/default password databases

Pre-Exploitation

During this stage, the tester will use their experience and knowledge to plan how to exploit any vulnerabilities identified during the scanning phase.

Sometimes these will be well known vulnerabilities due to out-of-date patches or end of life systems, other times it may require some creativity and research. All engagements are different, the value that Elmdale IT testers bring to the table is their experience and knowledge, covering both infrastructure and applications. The good thing about all this planning is that if you want us to replicate the vulnerability, we can walk you through exactly what we did.

Exploitation

The exploitation phase of a penetration test focuses on gaining access to the system or resource using different methods depending on the intelligence gathered in previous steps.

This phase should be a well-planned and specific attack. Methods vary from, but are not limited to, initial access, execution, privilege escalation, lateral movement, and credential access.

How it works

E · I · S · L

Reporting

The final phase of the engagement is to produce a document that outlines any misconfigurations and vulnerabilities found with the supporting evidence cleanly and understandably.

The first of which is the executive summary which is aimed at those that oversee the security of the company. It will explain the goals of the engagement and any high level findings. Then there is the technical report that is aimed towards the remediators of any issues. It will provide more depth to the vulnerabilities found. For example, information, the attack path impact, and remediation suggestions.

1000+
Completed tests
We have delivered over 1000 penetration tests to our customers and partners.

How it works

E·I·S·L

Safeguard your digital frontier with **confidence.**

Ethical Hacking

Drop us an email or give us a call with any questions or to find out more.

sales@elmdaleit.co.uk

0118 982 1444

E·I·S·L

Elmdale
IT Services
Ltd

Leading The Way In
Digital Business Solutions

Contact Us

sales@elmdaleit.co.uk

0118 982 1444