CYBERSECURITY 101 · eBuilder Security

Penetration Testing

A penetration test is a controlled attack on your own systems, run to find the weaknesses a real attacker would use before they do. Here is what it covers and the one habit that makes it pay off.

WHAT IT IS

A penetration test, or pentest, is an authorised and controlled cyberattack. A skilled tester plays the attacker to find and safely exploit weaknesses in your networks, applications and people, then reports exactly what was reachable and how to fix it. It shows you your real gaps before criminals find them.

WHY IT MATTERS

21.3%

Share of EU intrusions ENISA traced to exploited vulnerabilities in 2024 to 2025, second only to phishing.

ENISA, 2025

147 million

People exposed when Equifax left one known web flaw unpatched in 2017.

US FTC, 2019

Every 12 months

Minimum internal and external penetration testing PCI DSS requires, plus after any major change.

PCI DSS v4.0.1

WHAT HAPPENED

In May 2021 ransomware shut down Colonial Pipeline, a major US fuel line, for about five days. Investigators traced the entry to a single leaked password on an old VPN account that was still enabled and had no multi-factor authentication. No advanced exploit was needed. An external test of remote access would have flagged that gap first. (US Congressional testimony, 2021)

RED FLAGS TO WATCH FOR

These are the gaps a good penetration test is built to find. If any sound familiar, you are overdue.

- Internet-facing systems that are behind on security patches.
- Remote access or admin logins without multi-factor authentication.
- Old or unused accounts that were never disabled.
- Web applications or APIs that have never been properly tested.
- Cloud storage and permissions that no one has reviewed.

THE ONE RULE THAT STOPS IT

Test your most exposed systems at least once a year and again after any major change, then fix what is found and retest to confirm it is closed.

THEN BUILD THE HABIT AROUND IT

- Agree the scope and rules of engagement in writing before any test.

- Use qualified testers who are independent of the team that built the systems.
- Pair periodic tests with continuous vulnerability scanning between them.
- Track findings to closure and require a retest, not just a resolved ticket.

MYTHS AND FACTS

MYTH

A vulnerability scan is the same as a penetration test.

FACT

A scan is automated and lists possible weaknesses. A pentest adds a human who proves which ones can actually be exploited.

MYTH

We passed our last test, so we are secure.

FACT

A test is a snapshot. New systems and newly disclosed flaws can reopen risk the day after the report is signed.

MYTH

Only large companies need testing.

FACT

Attackers scan the whole internet. Smaller organisations are often hit because their defences are thinner.

THE LEGAL DUTY

Regular testing is now a compliance duty. GDPR Article 32 requires regularly testing your security measures and PCI DSS requires annual penetration tests, while DORA mandates threat-led testing for significant financial firms. In Sweden this sits alongside Cybersäkerhetslagen, the NIS2 law in force since 15 January 2026.

GET HELP

eBuilder Security runs human-led penetration testing for organisations across Sweden and the EU, scoped to your real risk. Read the full guide at the link below.

Read the Full Article →