

# Penetration Testing: Vulnerability Assessment

## Detect the weaknesses that help attackers

Vulnerabilities within your systems, software and hardware make an attacker's job that much easier. Following the path of least resistance, attackers exploit the weaknesses to create inroads that will lead them further and deeper into your assets, enabling them to find and compromise the data, access and privileges that are the lifeblood of your organisation.

The Common Vulnerabilities and Exploits (CVE) database lists more than 11,000 exploitable vulnerabilities in commonly used systems and software. In light of the complex and extensive networks within your organisation, the likelihood that you are susceptible to multiple vulnerabilities is extremely high.

**Reliance acsn's Vulnerability Assessment service finds attack paths into your organisation and mitigates those that carry the most risk, across a plethora of different systems, software, and hardware.**

Automated, efficient, requiring no human input from your teams, it tracks issues across your infrastructure, and produces reporting that clearly prioritises remediation actions. This enables you to understand which risks should be tackled first – and how – in order to best protect your organisation's operations and revenues.

## What Vulnerability Assessment delivers

Reliance acsn's Vulnerability Assessment delivers indispensable insight both as a standalone service and as a critical element in your overall Penetration Testing strategy and the other services we offer to support it.

It does this through a powerful combination of approaches, processes and tooling, combined with human security expertise, including:

**Reconnaissance:** Port scanning, application identification, service enumeration.

**Detection:** Insecure file permissions, application-level bugs, backdoor and Trojan horse installations, vulnerable protocols, network services, and more

**Powerful framework tools:** Qualys, Nessus etc.

## How our approach benefits you

We understand that every customer's operating model and risk profile is different, so we first work with you to identify the greatest security threats to your organisation and prioritise the Vulnerability Assessment around them.

Then we take the pressure off your teams, premises and workflows by setting up and automating the assessment remotely, but using human security analysis expertise to examine the outputs, create a tailored view of your exposure, and walk you through clear next steps to address it.

### **1** We target one of the top attack vectors

An estimated 60% of breaches involve vulnerabilities.

### **2** We investigate comprehensively

This ensures we scan for all new and existing vulnerabilities.

### **3** We fit with your routine

Scheduling detection tools to run within or outside working hours, to maximise productivity and minimise disruption.

### **4** We deliver clear reporting & next steps

We help you through them, in jargon-free language from humans with security expertise and an understanding of your business priorities.

### **5** We can assess regularly

The vulnerability and threat landscape evolves daily. We can be on hand to always help you keep one step ahead of it.

### **6** We help free up your IT teams

So they can focus on business productivity, rather than spending time and money trying to second-guess security issues.

## About Reliance acsn

**Across five continents, enterprise and government clients depend on Reliance acsn to defend them against cyber threats like nobody else can.**

Our managed security and consultancy services support organisations throughout the challenges of assurance, awareness, detection, response and prevention, 24 x 7, and focus on business risk – securing not just assets and data, but revenues, too.

- Reliance acsn's history goes back to 2003, with the founding of global cyber security specialist ACSN.
- In 2016, a merger created Reliance acsn in London, UK, to deliver real-time Managed Detection and Response (MDR)
- We've helped scores of the world's top brands plan, deploy and manage robust security solutions, in banking, telecoms, retail, government and insurance.
- Our people are accredited across all the major standards in IT security – including PCI, ISO27001, G-Cloud, CISSP, CREST, and many more – and accredited to support virtually any technology you have in place or are planning to procure.