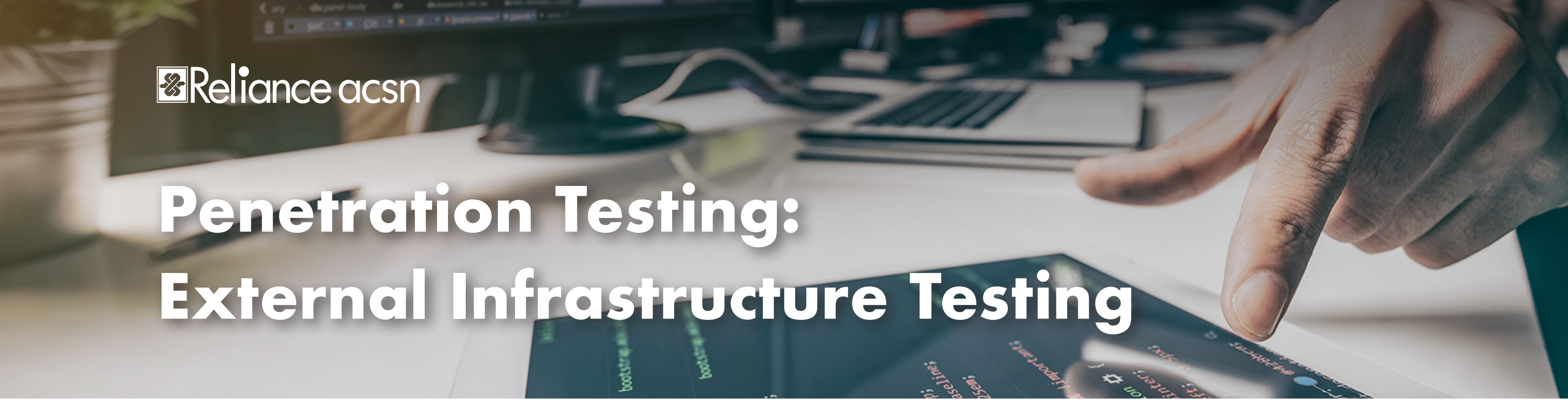

Reliance acsn

Penetration Testing: External Infrastructure Testing

Understand how attackers use your external infrastructure against you

Your external-facing IT assets - web servers, routers, firewalls and many others - are highly susceptible to attack and compromise. Industry sources suggest that 96% of testing identifies at least one vulnerability in these infrastructures, often resulting in the exposure of user credentials and other confidential information, and permitting unauthorised network authentication.

Clearly, many organisations' networks potentially contain significantly more than just a single vulnerability, multiplying attackers' opportunities to compromise those businesses' operations, their reputations, and their bottom line.

Reliance acsn's External Infrastructure testing assesses your internet-facing infrastructure for vulnerabilities that can then be addressed to reduce your organisation's attack surface. We simulate attacks to reveal weaknesses, prevent further penetration, and help you fulfil compliance-related testing requirements.

Our External Infrastructure Testing helps ensure that your internet-facing assets continue to deliver what your organisation, clients and supply chain most value – agility, productivity, accessibility – whilst preventing these benefits from being exploited to launch punishing attacks against you.

What External Infrastructure Testing delivers

Reliance acsn's External Infrastructure Testing delivers a robust investigation into the security of your external-facing assets, both as a standalone service and as part of a wider portfolio of Penetration Testing specialisms, using real-world attacker techniques.

We achieve this by combining extensive human security analysis expertise with powerful, specialist scanning tools, enabling us not only to comprehensively identify, but also thoroughly validate, the risks to your infrastructure.

Attacker-focused testing

We test from the internet, in real-world conditions, so we see your external infrastructure exactly as an attacker would.

Cutting-edge tools

Powerful, specialist tools including Nessus and Qualys deeply scan DNS, vhosts, TCP/UDP ports, service version enumeration and many more potential infrastructure weaknesses.

Additional human expertise

We extensively research publicly disclosed vulnerabilities and manually verify the scan findings to expertly interpret risks and impacts.

Comprehensive scope

Patching, configuration, encryption and secure protocols, data exposure, and third-party software vulnerabilities are all thoroughly investigated.

How our approach benefits you

At Reliance acsn, there is no 'one size fits all' approach to External Infrastructure Testing. Instead, we work closely with you and your teams to understand how potential vulnerabilities could be used by an attacker to capitalise on your organisation's specific business risks, so that we can focus the testing more effectively.

Then we take the pressure off your teams by setting up and executing the testing, expertly analysing the outputs, and creating a tailored report of your exposure, with clear indicators for next steps and how we can help you achieve them.

1 We identify the greatest risks first

Credential compromise and weak passwords, for example, are a problem for an estimated 42% of infrastructures tested.

2 We prove what we say

We test the identified vulnerabilities under controlled conditions to validate their risk.

3 We tailor our testing to you

We know every organisation is different, so we customise our testing around what your assets offer to an attacker – not anybody else's.

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 go again to keep you secure

We retest to prove the effectiveness of our recommendations, and we can test again to keep you constantly ahead of your attackers.

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.