
# Penetration Testing Services

A Penetration Testing assessment is the first step any organisation should take to assess your current organisational readiness and defence against a cyber-attack.

JAW Consulting UK offers a comprehensive range of penetration testing services to discover vulnerabilities in your systems, performed by CREST Certified Penetration Testers.

How will your organisation's infrastructure hold up against a real cyber attack? Are you confident business systems are configured correctly, and the security operations teams will detect an malicous intrusion?

A Penetration Testing assessment is the first step any organisation should take to start managing information risks correctly.

Vulnerabilities and exposures in most environments are due to poor system management, patches not installed in a timely fashion, weak password policy, poor access control, etc. Therefore, the principal reason and objective behind security assurance testing should be to identify and correct the underlying systems management process failures that produced the vulnerability that was detected in the assessment. The most common of these systems management process failures exist in the following areas:

- System software configuration
- Applications software configuration
- Software maintenance
- User management and administration

Our Penetration Testing Services are based on the proven industry standard Security Testing Methodology (OSSTM) to minimise missing patches and any vulnerabilities.

Each engagement is followed by a debrief session to ensure the report on issues found is fully understood and the correct possible impacts have been agreed. After discussing the findings will clearly explain how the issue came to exist in the first place given the context you have provided, in order to prevent future management failure from causing

We provide nine Penetration Testing Services, assisting your business with identifying vulnerabilities across your businesses applications, infrastructure and employees.

Speak with us today
To speak to us today, about how we can help test your organisation's defences against cyber-attack, data theft and malicious compromise.

+44 (0) 207 222 3333
www.jawconsulting.co.uk
info@jawconsulting.co.uk

JAW. consultinguk
Cyber Security, Data Protection & Privacy

**Web Application Penetration Testing**
Web Applications present your business, brand and services to the outside world.

A compromise of a web application can allow a malicious threat actor to gain access to the internal network and/or database server hosting sensitive information such as username and password information, personal data and payment card data.

Our Web Application Penetration Test evaluates the security of a web application. This involves both manual and automated analysis common security flaws (OWASP Top 10) and more complex security weaknesses, technical flaws, or vulnerabilities, and underlying technology from the perspective of a malicious attacker.

**Infrastructure (Network) Penetration Testing**
Our Infrastructure (Network) Penetration Test service replicates how a skilled and determined attacker will scour the network in search of vulnerable components (from the network to the application level).

Excessive open ports, unnecessary services, missing patches and configuration not only increase the attack surface, but bring inherent security risk as they are unlikely to be managed operationally.

Infrastructure (Network) Penetration Testing is a vital means of ensuring your business is protected in a real world scenario and should form part of your business's overall Cyber Security Strategy, ensuring network based security controls and security operations are operating effectively.

**Wireless Network Penetration Testing**
The main security concern with wireless networks is the removal of physical barriers.

While highly convenience to users, an incorrectly configured wireless network can be attacked and connected to from distances ranging from hundreds of metres to even a number of miles, and may go completely undetected.

Our Wireless Network Penetration Test can cover one or more offices, seeking to access corporate resources both as a malicious attacker, guest, and corporate user.

This will also assess correct implementation of wireless security measures, intra-client wireless protection, Corporate separation with wireless networks and Guest/Corporate wireless network segregation, ensuring your wireless network is not the weak link.

**Build & Configuration Security Review**
Critical Business Applications and I.T environment are made up of numerous components such as servers, network devices and middleware accessed by your users and partners via desktops, laptops and mobile devices.

If configured incorrectly with default or 'out of the box' settings, any one component can introduce weaknesses in your companies overall security posture.

Default passwords, open ports and unnecessary services are only a few examples which make it easier for a malicious attacker to gain a foothold in your network, accessing sensitive data or disrupting critical business services.

Our Build & Configuration Security Review analyses each system component configuration in detail against security best-practice, enabling you to meet a'secure-by-default' approach.

**Mobile Device Security Review**
Both corporate and employee-owned mobile devices, are increasingly adopted by businesses for access to corporate resources such as email, corporate application and sensitive data.

With attacks previously targeting desktops and laptops now targeting mobile operating systems, and increased risk of device loss/theft, it is critical adequate security controls are in place to ensure the security of corporate data.

Our Mobile Device Security Review first attempts to access the mobile device without credentials, such as if found or stolen.

Following this, our consultant performs a comprehensive build review providing assurance that security best practice and a 'security-by-default' is achieved for the mobile deployment.

**Firewall Security Assessment**
Our Firewall Security Assessment service is designed to ensure that the firewall configuration and rule set meets the business and compliance requirements of the company.

Firewall technology continues to play a key role in businesses of all sizes, establishing boundaries of trust and security within your organisation and the internet, and providing connectivity to employees and partners.

With the increasing complexity and functionality availability of next-generation firewalls and 'virtual' firewalls, it is especially important to ensure these are configured and managed correctly.

A full review of the ruleset will be investigated in line with the security architecture and the business supporting services after understanding gained from the operational use of the security device.

**Email Phishing Testing**
With 90% of data breaches seen by Verizon's data breach investigation team containing an email phishing or social engineering component to them, targeted and non-targeted attacks typically start with a well-crafted but malicious email, send to one of your employees.

Our Email Phishing Testing service determines your organisation's current susceptibility to this type of attack, identifying the groups of users most at risk.

Our security consultants construct a range of Email Phishing scenarios based on Open Source Intelligence of your organisation, utilising social networks, websites, and other public information, with or without organisational knowledge.

With results of this testing, your business can take any necessary steps to increase staff awareness and reduce public-facing information which may prove useful to an attacker for future targeted attacks.

**Secure Code Review**
The cost of resolving a security bug found at coding stage of the development cycle provides a significant cost saving to those found later during the testing or maintenance stage.

Our Secure Code Review service utilises a combination of both manual analysis and advanced automated code review tools, performed by certified Application Security Consultants, with experience of end to end Secure SDLC.

Whether following an Agile or Waterfall based development methodology, our Secure Code Review service enables your software development team to identify and resolve security issues early, saving rework and costly future exploits.

**Mobile Application Penetration Test**
With an increased risk of loss/theft, ease of physical device access and requirement for personal use, the threat profile to Mobile Applications and data require particular consideration.

Our Mobile Application Penetration Testing service considers a range of both malicious and accidental threat scenarios, utilising manual and automated tools to fully validate the security of your mobile application.

Validation includes mitigation against common vulnerabilities such as OWASP Mobile Security Top 10, correct use of OS Security API's and defence against more complex exploitation typically missed when using automated tools alone.

Whether developing a consumer or business focused Mobile Application, our Mobile Application Penetration Testing service provides your business with the necessary assurance of security.

---

**About JAW Consulting UK - Cyber Security, Data Protection & Privacy**

Established in 2008, JAW Consulting UK is a leading provider of Cyber Security, Data Protection & Privacy Consultancy and Resourcing services.

We offer a range of services including Penetration Testing, Cyber Security Risk Assessment, Cyber Security Strategy & Architecture, PCI DSS, ISO27001, EU GDPR, UK DPB and other internationally recognised standards.

CYBER ESSENTIALS Certified

Using a unique set of methodologies, we aim to embed security and technology as part of the standard business process, ensuring the value of data is recognised and protected throughout its life-cycle.

JAW is proud to have a wide client base, covering all major industry verticals including but not limited to FTSE100, financial services, insurance, retail, local & central government, healthcare and utilities.

Security, in Simplicity™

JAW. consultinguk
Cyber Security, Data Protection & Privacy

JAW Consulting UK Ltd.
20 Eastbourne Terrace
Paddington, London, W2 6LG

To find out more about JAW Consulting UK, call +44 (0) 207 222 3333 or send an email to info@jawconsulting.co.uk