Penetration Testing Fact Sheet

What is Penetration Testing?

Penetration Testing, often referred to as ethical hacking or security/vulnerability testing, involves the simulation of real world cyber attacks on a system, network, or application, to identify any vulnerabilities and weaknesses using the same tools and techniques that a malicious actor may deploy.

Why should we conduct Penetration Testing?

A Penetration Test should be thought of as being like a financial audit. A finance team maintains and monitors expenditures and income day to day. A Penetration Test ensures that your systems, tools, and processes are sufficient to adequately secure your business and its assets.

How it works

Identification of vulnerabilities in systems, networks, and applications that may be exploited by attackers. This proactive approach allows your business to address potential security risks before they can be exploited.

Real World Simulation of attack scenarios to provide a more realistic assessment of your current security posture. This will give a clear insight into how well the perimeter defences stand up under pressure.

Verification of your security controls confirms the effectiveness of any controls and technologies that are currently deployed. Are these controls sufficient to detect and prevent unauthorised access, data breaches, and any other security incidents?

What you are left with after a Penetration Test

Risk Mitigation forms a key part of a penetration test outcome report. By helping your business to reduce the risk of security breaches and the potential impact on operational delivery, financial standing, or brand degradation.

Strategic/Budgetary Decision Support will form part of the outcome report delivered as part of a penetration test. These valuable insights will inform strategic decision-making regarding any cybersecurity investments, allocation of resources, and overall risk management.

Penetration testing is a critical component of a comprehensive cybersecurity program, offering proactive risk management, compliance adherence, and continuous improvement in the face of evolving cyber threats.

Xperience

Get in touch...
enquiries@xperience-group.com