CYBERLOGIC

INTERNAL VS EXTERNAL PENETRATION TESTING AT A GLANCE

	INTERNAL PENETRATION TESTING	EXTERNAL PENETRATION TESTING
Scope and target environment	Focuses on the organisation's internal networks, systems, and assets.	Evaluates external-facing assets, such as websites, servers, and applications.
Perspective	Assesses vulnerabilities from the viewpoint of an insider, simulating employee actions to identify weaknesses exploitable by insiders.	Emulates the actions of an external attacker, aiming to breach external defences and uncover vulnerabilities accessible from the internet.
Access levels and authorisation	Requires authorisation and coordination with internal teams, as it involves testing within the organisation's own network.	Typically conducted without prior knowledge or access to internal systems, replicating an attacker's approach from outside the organisation.
Objectives	Aims to uncover vulnerabilities associated with insider threats, assess internal security controls, evaluate employee training, and test incident response capabilities.	Identifies vulnerabilities in public-facing assets, aiming to prevent data breaches, unauthorised access, and service disruptions caused by external threats.
Testing techniques	Uses methods like privilege escalation, lateral movement, and data exfiltration to simulate insider threats as well as social engineering tactics.	Utilises scanning tools, vulnerability scanners, and ethical hacking techniques to probe external-facing systems for weaknesses.
Security focus	Concentrates on strengthening internal security measures and addressing employee-related vulnerabilities.	Focuses on bolstering perimeter security, securing public-facing systems, and guarding against external attacks.
Risk assessment	Helps evaluate the risks from within the organisation.	Evaluate risks that could lead to data breaches, service disruptions, or unauthorised access by external attackers from outside the organisation.
Compliance	Assists in meeting compliance requirements related to internal threats and the protection of sensitive data.	Supports compliance by ensuring that external systems and data are adequately protected against external threats, aligning with regulatory standards.