WHY IS PENETRATION TESTING NECESSARY?

Penetration testing is a security assurance exercise. It provides independent validation that your security defences are sufficiently resilient. This is important for multiple reasons including:

Verifying that New Applications are Secure: When a new application is being deployed, regardless of the host, it is a good idea to carry out an assessment, especially if sensitive data will be stored within the application. Testing should be a key activity within your secure development lifecycle.

Understanding the Security Posture of your Organisation: Testing helps confirm your defences are sufficient and resilient. This will be important to your senior management and also to organisations you work with or hold data on behalf of.

Regulatory Compliance: Laws and regulations require good security assurance including testing. Article 32 of GDPR, for example, refers to data controllers implementing measures including "a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing"

Contractual Compliance: It is increasingly common for supplier contracts to mandate annual pen-testing of systems that are important to the services being provided by the supplier.

Improved Threat Awareness: Sometimes similar organisations are exposed to similar threats. Carrying out assessments using the same methods that perpetrators use to attack other companies in the same industry gives insight into how exposed the company is and how to prevent the organisation from being the next victim.

evalian

6 STAGES OF PEN TESTING

1 PRE-ENGAGEMENT INTERACTIONS

The tester will work with you to define:

- scope of the test
- any objectives
- strategies
- legal implications and/or constraints

2 RECONNAISSANCE OR OSINT

The tester will collate as much open-source intelligence as possible about the organisation

NOTE: Information will vary depending on the type of test being carried out,

3 VULNERABILITY IDENTIFICATION

The tester will use all the potential targets gathered in stage 2 and model the attack vectors which will be used on the target.

Vulnerability scanners and other manual or automated tools will be used on the target to discover any exploitable vulnerabilities.

4 EXPLOITATION

With all targets and vulnerabilities mapped, the tester will attempt to use exploits to gain entry to systems and/or networks.

NOTE: End goal is to see how far in the environment the attacker is able to get (within the defined scope).

5 ANALYSIS

The tester will document how the access was gained and provide remediations to avoid future exploitations.

The tester will sanitize the environment by reconfiguring any access obtained to penetrate the environment and cleaning up any traces of the attack.

6 REPORTING

A written report of the test is provided to the client, including recommendations to remediate vulnerabilities.

The company has the opportunity to review any findings with the tester during a debrief workshop.

evalian