penetration testing

7safe
information security

Penetration testing (or "Ethical Hacking") is often misunderstood, but can prove invaluable to any organisation with or without an Internet connection. In today's complex networked environments, the potential for unanticipated exposure to risk is growing and information security is an ongoing challenge.

Risks

Of particular significance are the following concerns when considering the effects of a malicious attack:

- Financial impact
- Damage to reputation
- Risk exposure of the business (downtime, media attention, effort etc.)
- Legal issues
- Loss of Internet presence of a service (in many cases business may cease)

Attacks are growing at an alarming rate and no longer are well known organisations such as banks and government agencies the only targets. With the advent of sophisticated, automated exploitation tools and "point-and-click" hacking, anyone with a network connection (internet, corporate, internal etc.) is potentially vulnerable. However, there are steps that can be taken to mitigate and anticipate this risk for organisations both large and small.

Our service

Engage 7Safe to scope and test your network & application services. We use sophisticated penetration testing software combined with our methodology – a blend of best practice and proprietary process. This includes the use of automated tools and manual testing techniques to discover vulnerabilities and any compromised systems. Even a suit of armour can have chinks. We assist our clients by helping them identify weaknesses from the "attacker's" perspective, in a controlled manner. Our penetration testing service comprises an in-depth investigation of systems from an external or internal perspective:

External testing usually takes place across the Internet to ensure that we see client systems through the eyes of a potential attacker from a similar environment.

Internal testing involves a visit to your site location and connecting to your internal network on the appropriate segment/s from a "behind the perimeter" perspective.

7safe

The process

7Safe's testing is designed to ensure that your systems are operating as expected and that there are no undiscovered security-related issues. The testing process is detailed and extensive, and typically involves the following stages:

- **Scoping** – assessing the appropriate targets & test types for testing
- **Discovery** – building information about a network & its services
- **Vulnerability Analysis** – testing systems & services for known vulnerabilities
- **Penetration** – exploiting weaknesses and escalating privileges
- **Analysis & Reporting** – detailed findings & recommendations

Scheduling penetration tests on a regular basis is recommended. However, we can perform one-off assessments where appropriate. Our reporting delivers a high-level summary for management purposes, together with the technical details that are organised according to perceived risk level. Within each section are recommendations for resolving any vulnerability found, combined with an overall summary that details any additional recommended actions, if required.

Price

Pricing is determined on a per-project basis and charged at our daily consulting rates.
We assist with determining the scope of the testing in order to provide accurate estimates.

Visit www.7safe.com or contact us on +44 (0)870 600 1667 to learn more.