

## penetration testing

[commissum - that which is entrusted]

**The commissum Penetration Testing service is an organisation specific assessment of vulnerability to a range of potential attacks. The service simulates the action of dedicated hackers, testing defences at the perimeter and within the enterprise as appropriate.**

### issues

It is now widely recognised that it is best practice for organisations to take penetration testing services from specialist external organisations.

The need to harden systems against attack is real; any organisation using modern Information Systems is at risk to some extent from threats that can originate internally or from the Internet.

Potential threats from system penetration include data theft, data corruption, or just vandalism; more sophisticated risks are also the use of facilities to mount email spamming, virus distribution and denial of service attacks.

It is also important not just to consider this from a perimeter perspective, but also to test the controls protecting the critical assets. This could be from an external attacker traversing your Internet Point of Presence, or a staff member or other trusted individual on local networks.

The **commissum** Penetration Testing service will assist you in assessing the effectiveness of the measures you have taken. An organisation specific, carefully scoped assessment of your vulnerability to a range of potential attacks provides guidance on improvements and alerts you to risks that you may not be aware of.

### approach

Many commercial penetration testing services provide an automated scan of your Internet presence. These tests can be useful in that they provide a very basic "snapshot" of your vulnerability to some known attacks. What they do not do is assess these in your business context and filter out the real risks from the many "false positives".

**commissum's** methodology is a consolidation of internally developed and proven practices, and industry best practice such as OSSTMM (the Open Source Security Testing Methodology Manual). Testing is scoped to each specific organisation's requirements, and is as intrusive or non-intrusive as required in each case.

The service can be either "Black Box" (limited prior knowledge) or "White Box" (full knowledge); frequently a combination of approaches is used to greatest effect.

Phases are, dependent on agreed scope:

- footprinting - check publicly available information about IT deployment that could be of use to a potential attacker
- enumeration – scanning and analysis using a variety of tools
- exploitation analysis – identify the systems and architectural features – analyse the potential for successful attacks and verify to agreed level
- impact analysis/reporting - correlate with known vulnerabilities examine findings, inform client and reach conclusions on business impacts

### customer benefits

**commissum** reports on the risks discovered and the impact to your business.

The report provides:

- a business focused executive summary
- a consolidated listing of identified and verified vulnerabilities
- the assessed risk to your business with relative priorities
- recommendations for corrective action
- recommendations for cost effective high value improvements

To supplement the report, **commissum** also provides follow-up presentations and interactive workshops. The aim is to collaboratively work with the organisation to assist in development of realistic, focused and prioritised plans of action to address recommendations.

**“Beautifully done”**

Sir Sidney Spencer (1891 - 1959)  
Thanking the nurse who had given him his  
nightly injection, just before he died.