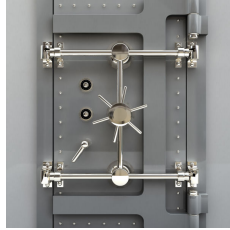


Internet Gateway Security Testing



External penetration testing puts us in much the same position as a potential intruder, trying to break into an Internet gateway and compromise the systems behind it.

The Need

The Internet is not getting any safer.

External testing of an Internet connection is necessary to make sure that there are no holes that intruders can exploit: even with the best security design there may be errors in configuration that would otherwise go unnoticed.

Our Service

IDsec consultants follow an established methodology, extracting as much information from a target as possible before looking for specific vulnerabilities.

So our first step is to find all the services that are offered to the world at large.

Some of these may be unnecessary and, perhaps, offer information that might be of use to an intruder. It is often possible to characterise the various hosts and produce a rough network map.

We then launch a wide range of probes to see if there is any vulnerability that could be exploited by an intruder. Vulnerabilities may arise from poor design, misconfiguration or the use of outdated software. We use our own *Netwalk* tool for network mapping and host characterisation. For finding specific vulnerabilities we use a number of tools, including Internet Scanner from ISS and the public domain tool Nessus.

This inevitably leads to some manual follow-up: in some cases the output of tools may imply a vulnerability that only a skilled analyst can confirm.

Unless requested by the client, we do not run any checks designed to cause a denial of service (that is, crash or otherwise seriously affect the remote system). This means that the impact on business is minimal.

The final, and most important, stage is to merge all the findings from various sources into a single view of the network and any threats to it. This involves consolidating the results given by the tools, eliminating any false positives, summarising the population of the network as found and then producing a set of conclusions, including specific recommendations for fixing vulnerabilities. Any serious holes in an exposed network are reported to client staff immediately.

What You Get

At the end of the review we issue a written report containing a summary of the systems found on the network, a set of detailed host-by-host results and a set of conclusions and recommendations.

IDsec reports are not simply the output of the tools used for scanning: we explain the significance of each vulnerability in plain terms and provide general guidance on closing any security holes found. In some cases our conclusions may relate to important non-security issues that we believe are impairing the general well being of the network (for example, misconfigured routing or name servers).

The Price

Prices start at around £2,700 for a small Internet gateway with up to 10 IP addresses.

Our Track Record

Since 1997 IDsec has been carrying out external audits for many blue-chip companies, in some cases carrying out repeat tests over several years.

For a major UK telecoms company we have carried out regular tests of its managed firewall service, using a high level of automation to cover a very large network range.

A large mobile phone operator has commissioned us to test a number of its on-line services just prior to going live.

At the other end of the scale we carry out a number of small-scale assessments for organisations setting up their first Internet presence and requiring more detailed interpretation of the results than more sophisticated players might need.

Related Services

On-Site Gateway Review	An on-site review of an Internet gateway that goes beyond a simple external scan and looks for strength in depth.
Superwalk: Automated Monitoring	Superwalk runs regular scans of an Internet gateway, and characterises all hosts that give any IP response. It also uses a number of tools to find specific vulnerabilities in the services offered.
Web Application Testing	Classic penetration testing at the network level has its place, but many new attacks are aimed at interactive web applications. A thorough external test can minimise these risks.

Feel Good About Your Network

IDsec is an independent company specialising in network security. We can assess your security and advise on long-term protection: as we have for a range of blue-chip clients since 1997.

IDsec

31-33 College Road, Harrow, Middlesex HA1 1EJ, United Kingdom
T: +44 20 8861 2001 F: +44 20 8861 3433 W: www.idsec.co.uk

All prices exclude VAT and are subject to confirmation.
Copyright © 2009 IDsec Limited

services/testing/gateway-testing.pdf 20091019 (5.09)