

Interrogate External

Features

- *Proactive risk and vulnerability assessment*
- *Manual analysis of all results by experienced consultants*
- *Comprehensive report, suitable for both technical and managerial levels*
- *Tests can be tailored to fall in line with planned changes to IT systems security infrastructure*

Benefits

- *Provides proactive assessments before any incidents occur*
- *Manual analysis provides thorough, accurate reports and reduced false positives*
- *No permanent harm or modification occurs*
- *Recommended remedial work is clearly identified*

"Conducting a proactive, 'human' analysis reduces overall risk."

Are your computers vulnerable to attackers?



Operating systems and applications can contain vulnerabilities or mis-configurations that allow an attacker to compromise Internet facing hosts, and possibly gain access to internal networks. An Integralis S3 proactive analysis identifies issues before they become security incidents.

INTRODUCTION

The Interrogate External is a manual scan, across the Internet, of specified hosts run as two options:

- a vulnerability assessment designed to identify, but not exploit, potential vulnerabilities
- a full penetration test to identify exploits and leverage them to determine further issues.

No permanent harm or modification occurs. Manual testing provides intelligent analysis not available when an automated scan is utilized.

SCOPE

Vulnerability Assessment is essential for critical web-facing systems such as routers, firewalls, web servers and email servers. It identifies:

- vulnerabilities that exist and may be exploited in order to gain unauthorised access to the internal network or key servers
- weaknesses present in commercially released operating systems or applications.

INTEGRALIS - LEADING CERTIFICATION

The Integralis S3 team holds leading testing status with CHECK Green Light status and the Payment Card Industry Approved Scanning Vendor certification.



BUSINESS BENEFITS

This service is an ideal starting point for providing an assessment of the effectiveness of deployed network security. Conducting a proactive analysis reduces overall risk and lowers the costs of responding to incidents. The use of human analysis, interpretation and attention to detail, minimises the risk of false positives and other erroneous information. It also highlights vulnerabilities that automated tools miss, ensuring results are accurate and comprehensive.

AUDIENCE

Security and infrastructure managers are able to ascertain the effective security of devices at their network perimeter. Recommended settings, patches and other remedial work are clearly identified for support staff.



BS7799: PART 2: 2002 - ISO 27001

Interrogate External

"Human interpretation ensures that our clients are provided with the best advice, presented in an easy to understand format."

DELIVERABLES

S3 consultants have extensive security industry experience and utilise a variety of tools. These are combined to carefully compare the results before completing a comprehensive report, suitable for both technical and managerial levels. Technical issues are prioritised, explained and remedial action or workarounds covered. Human interpretation ensures that a client is provided with the best advice, presented in an easy to understand format.

TECHNOLOGY

The Interrogate External service is based on manual testing, analysis and reporting, not just the running of proprietary system scanners followed by an automatically generated report.

The following list details some of the categories that are tested:

- **Information gathering possibilities**
- **Backdoors and misconfiguration**
- **HTTP and CGI abuses**
- **Firewall, filters and proxy vulnerabilities**
- **File Transfer Protocol abuses**
- **Authentication mechanism tests**
- **DNS and Bind checks**
- **Remote file access vulnerabilities**
- **Remote Procedure Call checks**
- **SMTP and Mail transfer vulnerabilities**
- **SNMP vulnerabilities**
- **Windows Service Pack and Hotfix checks**

PREREQUISITES

A client must provide the IP addresses and web URLs (if applicable) of the hosts that are to be tested. A contract must also be signed, authorising access to the client's site, information records and other relevant material. Permission must be granted from all persons, including third parties, such as the client's Internet Service Provider

PACKAGE

Interrogate External can be purchased as a one-off 'snapshot', or as an annual contract. The annual service provides 4 quarterly engagements per annum, although the precise timing of tests can be tailored to fall in line with planned changes to IT systems security infrastructure. As standard the service covers 8 IP addresses. More IP addresses can be tested if required.

Interrogate External can also include Denial of Service (DoS) attack vulnerability tests. However, these will only be performed with prior express approval because of the risk of service loss on live systems.

Two additional modules are available to complement Interrogate External:

● **Host Discovery Add-On**

Optionally, a 'Host Discovery' procedure can be invoked before an Interrogate External, during which an IP address range is scanned for active devices. This enables the identification of hosts prior to selection of these devices for input to the full Interrogate External process.

● **Web Application Testing Add-On**

Optionally, a Interrogate External can be supplemented with the S3 Web Application Testing Add-On service. More details are available in the Web Application Audit datasheet.



BS7799: PART 2: 2002 - ISO 27001