



» SERVICES



THE QUEEN'S AWARDS
FOR ENTERPRISE:
INTERNATIONAL TRADE
2007



AWARDS
2008
EUROPE
WINNER

Category 'Best
Security Company'

Penetration
Testing

Penetration Testing

NGSConsulting offers clients a range of specialised Penetration Testing services. The Penetration Testing process makes use of NGSSoftware's proven methodology and provides a detailed evaluation of the current infrastructure and service security of the client organisation. NGSSoftware's consultants assess the architecture and configuration of the client operations, evaluating both legitimate and illegitimate points of access, and identifying any potential security vulnerabilities.

The NGSConsulting Penetration Testing process allows clients to evaluate the likelihood of potential attack - enabling them to secure their vital Internet visible infrastructure. The detailed technical and management reports provided by NGSConsulting allows client organisations to objectively assess the security of their information assets. As well as exposing risks during the Penetration Testing process, NGSConsulting helps to equip clients with the information necessary to remedy any security vulnerabilities through both detailed technical explanations and skills transfer activities.

The application of our world-leading penetration testing skills combined with our research and development facilities, has helped ensure our services to the worlds top commercial organisations & important government agencies are second to none.

» Methodology

NGSConsulting's approach to service engagements is defined by a detailed and proven methodology. Our approach can be separated into six distinct phases. These are:

- » **Passive Information Gathering** - NGSSoftware's Consultants gather detailed and relevant information from a variety of publicly available sources. The information gathering stage is defined as 'passive' as it does not interfere with normal client infrastructure operations and can be conducted in a variety of methods that are typically undetectable.
- » **Target Identification** - During this phase of an engagement, NGSSoftware's Consultants identify target networks, servers, and workstations within a clients' infrastructure. The target identification phase allows Consultants to build a detailed overview of security threats using such techniques as network mapping. This phase identifies potential avenues of exploitation and attack against the target that could potentially be exploited by malicious users and intruders.
- » **Target Enumeration** - This stage of the engagement is used by NGSSoftware's Consultants to fully identify the target resource. Consultants will identify the topology of clients network, specific systems and servers in place, security and applied patch levels, as well as communication infrastructures (e.g. open and closed ports on target systems, banner grabbing etc.).
- » **Vulnerability Identification** - Based upon the results of the Target Enumeration process, NGSSoftware's Consultants will identify vulnerabilities of a target during this phase. These vulnerabilities may be the result of improper security practices, system specific faults and unresolved hardware and software issues. During this phase, Consultants will assess the targets using best-of-breed applications, NGSSoftware's own tools, bespoke scripts and a detailed practical knowledge of security vulnerabilities.
- » **Vulnerability Analysis** - Before seeking to exploit any vulnerabilities discovered on a target host, NGSSoftware's Consultants will collate and carefully analyse the data recovered. Consultants scrupulously assess the potential hazards caused by exploiting any vulnerabilities found. The vulnerabilities discovered and the initial information gathered about targets is considered in tandem to enabling Consultants to mitigate risk during the exploitation phase.
- » **Vulnerability Exploitation** - Clients will be immediately notified of any high-risk vulnerabilities and the consequences of exploitation. NGSSoftware's Consultants will work with the clients' technical staff to identify a safe period to verify potentially dangerous vulnerabilities through exploitation. This process is often critical in the removal of false positive results. This allows consultants to fully assess the security flaws within a client infrastructure, and provides the basis of the reporting process.

» Benefits

Selecting NGSConsulting as suppliers of penetration testing services has a number of key benefits. These are:

- » An NGSConsulting penetration test provides a detailed overview of existing security vulnerabilities within a clients' infrastructure that could potentially be used in attacks and exploitation. Additionally, as a result of our globally recognised expertise in the field of application vulnerability research, NGSSoftware's Consultants can provide insight into developing threats and as yet undisclosed vulnerabilities.
- » A penetration test by NGSConsulting enables clients to assess their levels of security risk exposure. Consultants can subsequently employ this knowledge to assist clients to secure their infrastructures and mitigate risk.
- » The penetration testing process assesses the current security infrastructure of clients' existing security safeguards and control mechanisms. This assessment is conducted using proprietary software developed by NGSSoftware, as well as our consultants' expert knowledge and significant depth of experience.



» SERVICES



THE QUEEN'S AWARDS
FOR ENTERPRISE:
INTERNATIONAL TRADE
2007



AWARDS
2008
EUROPE
WINNER

Category 'Best
Security Company'

Penetration Testing

» Deliverables

During the Penetration Testing Assessment process, NGSSoftware's Consultants are available to discuss any results that may have been formulated, as well as outlining the processes involved.

The key deliverables throughout the assessment consist of:

- » Immediate notification to our clients of any high-risk vulnerabilities as and when they are discovered.
- » Delivery of interim reports detailing testing completed and findings at the end of each working day.
- » Scheduled conferences at the beginning of each day to discuss issues identified in previous daily reporting.
- » Consultants will be available at any point during the assessment process to discuss any issues that may arise.
- » A Final Report encompassing all activities and findings during the course of the assessment. This report is split into several key sections:
 - » A Management Summary listing areas of weakness and their respective business impacts.
 - » An Assessment Overview detailing the scope and objectives of the project undertaken, and the methodology utilised by the Consultants.
 - » Technical Findings detailing any security vulnerabilities discovered during the testing process, and providing detailed explanations of all the security implications. Comprehensive remediation information will be supplied including alternatives should the preferable solution be impractical.
 - » Conclusions detailing managerial and technical recommendations to the client, with a view to mitigating short term risks, as well as long term strategic solutions.
 - » Exploit Code - Where applicable NGSConsulting will provide the unique service of providing clients with demonstration exploit code.
 - » Additional Recommendations - Where the client is unable to patch any affected products, or the costs of doing so is prohibitive, NGSConsulting will provide a range of recommendations to mitigate any vulnerabilities discovered during the testing process.
- » A presentation to technical or management staff follows the delivery of the final report.

» Assessment Offer

If you feel that you are not receiving an adequate service from your existing security supplier, NGSConsulting would like to extend the opportunity of a no cost, no obligation 'mini-audit', provided under an NDA.

This allows our consultants to demonstrate their technical abilities and also allows future clients to assess the strengths and weaknesses of their existing suppliers.

For further details of this offer, contact info@ngsconsulting.com

» Contact Details

Web: www.ngssoftware.com

Support: support@ngssoftware.com

Sales: sales@ngssoftware.com

UK Head Office (London)
Next Generation Security Software Ltd
52 Throwley Way
Sutton
Surrey, SM1 4BF
United Kingdom

Australian Office (Sydney)
Next Generation Security Software Pty Ltd
Level 19, 2 Market Street
Sydney, NSW, 2000
Australia
ABN: 83 119804803
Regional Web: www.ngssoftware.com/au
Regional Sales: australiasales@ngssoftware.com

Tel: +44 (0)208 401 0070
Fax: +44 (0)208 401 0076

Tel: +61 (0) 448 692 022