



» SERVICES



THE QUEEN'S AWARDS
FOR ENTERPRISE:
INTERNATIONAL TRADE
2007



MAGAZINE
AWARDS
2008
EUROPE
WINNER

Category 'Best
Security Company'

Wireless
Security
Assessment (802.11)

Wireless Security Assessment (802.11)

The most common wireless technology deployed by far is that which is based upon 802.11 networks. However, with this popularity comes the danger of a large number of potential insecure configurations and specific security vulnerabilities. A malicious attacker could eavesdrop on wireless communications, steal sensitive data, gain access to sensitive systems and attack other users of a wireless network. Wireless network security assessments focus upon attempting to recreate the steps used by attackers to subvert wireless technologies.

» Methodology

The NGSSConsulting approach to service engagements is defined by a detailed and proven methodology. Our approach can be divided into a number of distinct phases:

» Stage 1 - Discovery

NGSSSoftware's consultants will begin an engagement with the discovery phase. Working closely with the client to keep any potential disruptions to an absolute minimum, this phase is conducted from within the client premises.

During this phase, NGSSConsulting will seek to discover the 802.11 capable wireless devices across all of the 802.11 sub-types including a,b,g and n (operating in the 2.4GHz and 5GHz frequency bands). This wireless sweep will provide an overview of the wireless footprint of the client, discovering access points, wireless clients (for example, laptops and printers) and any other 802.11 capable devices. This phase will highlight the information that is publicly visible to any potential attacker.

» Stage 2 - Profiling

Following the wireless discovery exercise, NGSSSoftware works closely with the client to review the results and to determine the architecture that is within the scope of the engagement. This phase will identify any rogue wireless devices which may exist.

Where rogue devices have been identified, NGSSSoftware's consultants will determine the strength of the wireless signal whilst moving around the test environment to help the client track down and physically locate the device.

» Stage 3 - Analysis

NGSSConsulting will passively monitor the wireless networks within the scope of the engagement whilst enumerating the technologies deployed. Where specific technologies are identified, NGSSSoftware's consultants will perform research to determine any applicable vulnerabilities. Before seeking to exploit any vulnerabilities discovered on a target network, 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 for enabling NGSSSoftware's consultants to mitigate risk during the exploitation phase (Stage 4).

This phase will also help to determine the protection mechanisms employed by the wireless network, identifying the authentication and encryption configuration (examples include WEP, WPA, TKIP/AES and LEAP).

» Stage 4 - Exploitation

Clients are immediately notified of any high-risk vulnerabilities discovered (together with the potential consequences which might arise from exploitation). Consultants will work with the clients' technical staff to identify a safe period in which to verify any potentially dangerous vulnerabilities.

Where weaknesses in the encryption solution have been identified, NGSSSoftware's consultants (with approval of the client) will attempt to exploit these weaknesses. This may include the use of de-authentication attacks, packet injection and replay attacks - all from the perspective of an unauthorised client.

When within the scope of the engagement, NGSSSoftware's consultants can also assess the risks posed by wireless clients that bridge wireless and internal networks. This involves coercing wireless clients into associating with a trojan access point, providing a vector for attacks against the client. In some cases, the trojan access point can be used to perform a "man-in-the-middle attack" between the wireless client and the access point.

» Stage 5 - Mitigation

NGSSSoftware's consultants will go the extra mile where necessary to ensure that appropriate procedures are in place to help mitigate against wireless attacks. This may involve reviews of device configurations, client patch levels, architecture hardening and wireless security policies to ensure that industry best practice are being adhered to.



» SERVICES



Wireless Security Assessment (802.11)

Wireless Security Assessment (802.11)

» Benefits

A Wireless Security Assessment from NGSSoftware provides a detailed overview of existing security vulnerabilities within a clients' Wireless deployment that could potentially be used in attacks and exploitation. Additionally, as a result of our globally recognised expertise in the field of vulnerability research, NGSSoftware's Consultants can also provide insight into developing threats and as yet undisclosed vulnerabilities. This assessment is conducted using a mix of NGSSoftware's proprietary tools, as well as our consultants' expert knowledge and significant depth of experience.

» Further Wireless Security Assessments from NGSSoftware

NGSSoftware provides an exhaustive range of Wireless Security Assessments. For further details of other Wireless Security Assessment Services, please refer to the following brochures:

- » Wireless Security Assessment (1) - For Bluetooth Network Testing, Wireless Input Device Testing, Wireless Handheld Security Testing, Wireless Transaction Device Testing and Cordless Communications Testing.
- » Wireless Security Assessment (2) - For Electromagnetic Radiation (EMR) Testing, RFID Security Testing and Microwave Radio Testing.
- » Wireless Security Assessment (3) - Wireless Surveillance Device Testing and Infrared Systems Testing.

» 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