



## » SERVICES



THE QUEEN'S AWARDS  
FOR ENTERPRISE:  
INTERNATIONAL TRADE  
2007



AWARDS  
2008  
EUROPE  
WINNER

Category 'Best  
Security Company'

War Dialling  
and Remote  
Access Discovery

## War Dialling and Remote Access Discovery

In a world of leased lines, VPNs and wireless communications, the ubiquitous computer modem lies largely forgotten in the corporate security-testing programme. Now, more than ever, rogue and unauthorised modems or ISDN terminals represent a very real and direct threat to network security with their ability to 'bridge' the best perimeter defences on the market.

A poorly configured or unauthorised modem will present an attacker with direct access to your internal network. Whether they came built-in to the latest network server or multifunction printer, or have been legitimately installed or not, the War Dialling and Remote Access Discovery service from NGSConsulting is specifically designed to discover all PSTN and ISDN listening devices within a client's environment. Using a mix of methodologies and discovery tools, consultants can rapidly enumerate all devices and subsequently evaluate any threats that they may represent to the organisation.

### » Methodology

The NGSConsulting approach to service engagements is defined by a detailed and proven methodology. Our approach can be divided into six distinct phases which include:

- » Stage 1: External Discovery Phase - Using either a list of numbers supplied by the client or a known range of DDI numbers, NGSSoftware's consultants will begin an engagement with a discovery phase. Working with the client to keep any potential business disruptions to an absolute minimum, this phase can be conducted outside of normal business hours and use a non-sequential dialling range (to prevent all sequential numbers within a single office all ringing at the same time). During this phase, NGSConsulting will seek to discover all electronic devices capable of accepting a digital or analogue connection. NGSConsulting normally recommends to their clients that this phase of testing be repeated multiple times over a one-week period (at different times of the day) so that devices that are available intermittently can be detected (e.g. devices only turned on over the weekend or early evening).
- » Stage 2: Internal Discovery Phase - In cases where any external dialling would cause an unacceptable interruption to the business, or when the ranges of telephone numbers or DDI's are simply unknown by the client, NGSConsulting is able to conduct a specialist internal discovery process. This phase is designed to utilise network mapping and interrogation techniques to identify devices that have, are likely to have, or have previously had installed, a digital or analogue modem. Relying on custom-developed tools and finely tuned automated scripts that make use of appropriate administrator-level privileges, consultants can rapidly discover potentially vulnerable hosts and devices. This is often more comprehensive than standard remote war-dialling of an entire DDI telephone range, as modems may only be switched on at particular times of the day.
- » Stage 3: Enumeration - Having discovered which PSTN or ISDN lines have listening devices together with any "time windows" in which they may operate, consultants would then focus upon enumerating the exact nature of the device. Each discovered connection is checked to see if it accepts digital or analogue data streams, and which type of service may be operating. This enumeration phase will identify Fax servers from voice mail services, bulletin boards from remote administration ports, and any other commercial remote access solution.
- » Stage 4: Vulnerability Identification - Based upon the results of the Enumeration process, consultants will identify vulnerabilities of the target during this phase. These vulnerabilities may be the result of improper security practices, specific faults or unresolved hardware or software issues. During this phase consultants will assess the listening service using the most appropriate client connection and vulnerability assessment tools. If appropriate, consultants can conduct restricted or brute-force guessing attacks to identify weak access controls. This phase takes enumeration a step further by attempting to identify computer systems to which a modem is attached and then trying to gain access to that system.
- » Stage 5: Vulnerability Analysis - Before seeking to exploit any vulnerabilities discovered on a target host, 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 NGSSoftware's consultants to mitigate risk during the exploitation phase.
- » Stage 6: Vulnerability Exploitation - Clients are immediately notified of any high-risk vulnerabilities and the consequences to them of exploitation. 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 forms the basis of the reporting.

### » Benefits

Like it or loathe it, almost every organisation has remotely connectable PSTN or ISDN devices scattered throughout their offices. Based upon NGSSoftware's experience, typically 1-2% of corporate telephone numbers have a modem attached to the end of them. The NGSConsulting War Dialling and Remote Access Discovery service has the following benefits:

- » Any operating services associated with a listening device can be enumerated, allowing technical staff to fully understand the nature of the device and evaluate whether its existence presents a security issue.



## » SERVICES



THE QUEEN'S AWARDS  
FOR ENTERPRISE:  
INTERNATIONAL TRADE  
2007



AWARDS  
2008  
EUROPE  
WINNER

Category 'Best  
Security Company'

War Dialling  
and Remote  
Access Discovery

## War Dialling and Remote Access Discovery

### » Benefits

- » Any PSTN or ISDN device lying within the telephone number range supplied to NGSConsulting will be detected. This information is typically collated and correlated with a list of known or authorised corporate devices, and any discrepancies found can be treated as hostile - representing a possible backdoor into the network.
- » When combined with a penetration testing exercise, clients can evaluate the full extent of their perimeter defences and whether their current dial-up PSTN or ISDN access controls are efficient in preventing attacks.
- » It provides a detailed overview of existing security vulnerabilities within a clients' dial-up 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 an insight into developing threats and as yet undisclosed vulnerabilities.

### » Deliverables

During the War Dialling and Remote Access Discovery 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 fix any affected elements, 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.

### » Contact Details

Web: [www.ngssoftware.com](http://www.ngssoftware.com)

Support: [support@ngssoftware.com](mailto:support@ngssoftware.com)

Sales: [sales@ngssoftware.com](mailto: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](http://www.ngssoftware.com/au)  
Regional Sales: [austaliasales@ngssoftware.com](mailto:austaliasales@ngssoftware.com)

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

Tel: +61 (0) 448 692 022