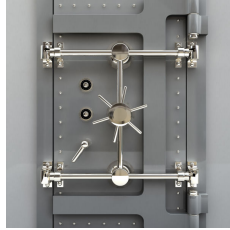


## Modem Detection and Audit



*Regular scanning of external phone numbers can help find uncontrolled dial-up connections and eliminate potential back-doors into the internal network.*

### The Need

A constant worry for many IT security managers is that an unofficial population of modems exists, outside any central registration or control.

These may have been installed by users with the best of intentions, but they can easily be found and abused by “war diallers” who systematically try all numbers in a direct-dial range.

Scanning may also reveal secondary dial tones that may be open to abuse – for example, in allowing a local outside caller to make an international call at the client’s expense.

### Our Service

IDsec uses the commercial PhoneSweep product from Sandstorm Enterprises to run automatic scans against the given target number sets. This allows us to categorise numbers as interesting (a modem), uninteresting (dead, unanswered, voice, voice-mail or FAX) or unknown (constantly busy). Note that automated re-dialling minimises the number in the last category.

PhoneSweep is then used, together with a manual examination of responses, to identify responding systems. Typical systems that we can detect in this way include pcANYWHERE, Microsoft RAS, Shiva LanRover, PPP, Citrix ICA WinFrame, NetWare CONNECT, cc:Mail, Cisco, Ascend, Bay Networks, PBX control ports and UNIX log-in.

If explicitly requested by the client, we will also use PhoneSweep and our own scripts to run automated attempts to break into systems by guessing likely username/password combinations.

We start by looking for systems that are not protected by password or other credential checking. In other cases there may be known security flaws that can be deduced from version data or other contextual information, including “factory default” passwords.

The bulk of the work, however, is in running brute force attacks – that is, automated ID/password guessing attempts – against susceptible systems. Note that we make some effort to tailor these password lists to the client’s circumstances, using company, departmental, product and geographical names as input.

It is inevitable that phone scanning may result in minor disturbance for the individuals within an organisation who answer calls made in this way, but we believe that the overall impact on the business is minimal.

#### What You Get

We produce a list of modems, faxes and dial tones found, including the type of system and (if appropriate) any security vulnerabilities.

Detailed reconciliation and follow-up work is outside the scope of the specific service described here, but we are always keen to work with clients on implementing any necessary changes that result from our findings.

#### The Price

The cost is based on the size of the phone number list to be scanned. As an example, a guide price for scanning an organisation with 1,000 numbers is £4,500: economies of scale mean that the price for a set of 10,000 numbers would only be £18,000.

We do assume that the targets represent normal office environments with, roughly, one modem being found for approximately every 100 numbers scanned.

These costings are also based on an assumption that scanning takes place during working hours, but other approaches can be discussed.

#### Our Track Record

Our experience of modem detection goes back to the earliest days of IDsec in 1997.

A well-known British merchant bank asked us to scan all of its external phone numbers. This included the direct-dial number range of its London and New York office and all the numbers of its overseas operations. This amounted to about 16,000 phone numbers.

We scanned all the direct-dial numbers allocated to a major UK telecoms operator, covering approximately 8,000 numbers.

IDsec has supplied the PhoneSweep product and related equipment to an energy utility so that they can carry out their own regular audits.

#### Related Services

<b>Internet Penetration Testing</b>	External penetration testing puts us in much the same position as a potential intruder, trying to break into the Internet gateway and systems behind it.
-------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------

#### **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](http://www.idsec.co.uk)

All prices exclude VAT and are subject to confirmation.  
Copyright © 2008 IDsec Limited

[services/testing/modem-detection.pdf](#) 20080715 (5.08)