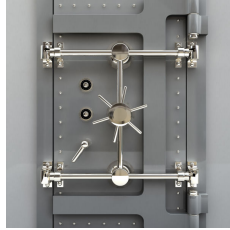


# Internal Network Mapping



*Many large organisations have no clear picture of the number and types of systems on their internal networks. A comprehensive network map is a vital precursor to vulnerability testing.*

## Purpose

We carry out a survey of all reachable TCP/IP networks to list all active hosts, identify types of system, show the services being offered and uncover routes to the outside world. The work needs to take place on site but should be non-intrusive, as it does not involve logging into systems or exploiting any security flaws.

## Our Service

Given a list of your internal networks, we try to contact and identify the hosts on them, using our own scanning PCs on your premises. Any further network topology information (typically SNMP and routing tables) provided by these hosts is analysed to see if there are additional networks that themselves need to be scanned – assuming that they can be identified as being within the scope of the mapping exercise. Depending on network topology, this exercise may be repeated using different access points on the internal network.

For practical and logistical reasons it is useful for us to have a general idea of the extent of the internal network, but we do not necessarily need a detailed network map before starting: in fact, we create one for ourselves as the work progresses.

We use our own Netwalk tool for network mapping and host characterisation.

## What You Get

At the end of the review we issue a report containing a summary of the systems found on the network, a set of detailed host-by-host results and a set of conclusions and recommendations.

To provide an overview, we summarise the population of the network, showing information such as the structure of subnets, the number of hosts found, the number actually offering services and the number of key servers by type of service – the latter will include software versions as appropriate. (In the case of a large internal network this summary is broken down into manageable parts relating to operational or geographical areas for convenience.)

The detailed results are presented as a table listing all hosts that show any IP response, but eliminating obvious network or broadcast responses.

For large networks these results represent a lot of information that is not easily managed in paper form. We therefore supply the detailed results as a browsable PDF document that can be printed but is also of use as a reference item.

#### Price

The total cost of the work will depend largely on the number and size of the networks involved and the number of active hosts found, plus expenses charged at cost. (There are no licensing fees associated with this service.) For example, to map a network of 10,000 addresses containing 3,000 active hosts, using a single pass, would require 8 days' consultancy effort plus travel costs depending on site location.

#### Assumptions and Caveats

You supply a direct connection to your internal network, with a fixed IP address for us to use for our scanning PC. To start the exercise, we need an initial list of known active networks. We need a technical contact who can decide whether any additional networks that we find are in scope. We expect to be notified of all appropriate SNMP community names.

There is no guarantee that we can determine the nature of all active hosts. In particular, it may not be possible for us to identify systems offering few, if any, services. In normal office environments, however, our success rate exceeds 95%. This survey does not identify or report on security vulnerabilities. There is a small but finite chance that this type of scanning can have an adverse effect on some hosts.

#### Our Track Record

Internal network mapping projects that we have carried out include:

We carried out an inventory and security vulnerability assessment for a UK mobile phone operator. This covered the entire internal network and resulted in mapping more than 7,000 hosts in a space covering 22,500 addresses over 50 networks. With the help of client staff we split the report according to areas of responsibility, to make it easier for the relevant administrators to act on our recommendations.

In another sector, we carried out an internal network review for a London-based foreign bank, covering approximately 1,000 hosts in an extremely mixed environment.

#### Related Services

<b>Network 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.
<b>On-Site Gateway Review</b>	An on-site review of an Internet gateway that goes beyond a simple external scan and looks for strength in depth.

#### **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 © 2009 IDsec Limited

[services/testing/internal-mapping.pdf](#) 20091019 (5.09)