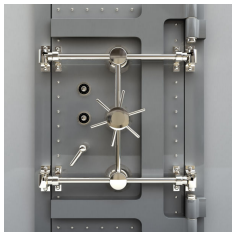
IDsec

Wireless LAN Security Testing



Wireless LANs offer a cost-effective, flexible extension to traditional cabled networks but access control and confidentiality are real concerns. Has the internal network gone external?

The Need

Unlike traditional networks protected by firewalls, Wireless LANs may allow anyone with a wireless access card to join and participate on the network. A company's strict security policy is ineffective with a rogue wireless LAN inside the building.

Our Service

We aim to find all the 802.11 wireless LANs operating in the immediate vicinity of a client's premises, gathering enough information in the field to determine whether a network belongs to the client. If so, it will be characterised, in terms of both physical location and networking properties, and the level of security determined.

To carry out this work, we use a portable scanning platform to find all wireless LANs operating at 2.4 GHz.

The authentication and association processes themselves give a considerable amount of information:

- unique identifiers for the network: MAC address, manufacturer, SSID and name
- authentication type and length of encryption key

Then, if the target network is using Open System Authentication – in other words, no key is needed to get access – it is quite likely that a DHCP exchange will take place, revealing higher level networking information such as:

- IP network address and mask
- DNS server and domain name

If access is gained but DHCP is not offered, a simple sniffing exercise will usually provide this information anyway.

Finally, a scan of the network using our Netwalk tool will give an inventory of the hosts present on the LAN.

The information gained so far may be enough to identify a given wireless LAN: for example, the name of the network or its hosts may well imply its function and location. In some cases, however, it is necessary to use direction-finding techniques to determine the physical location of the access point. To do this, we sample the signal strength at a number of points and use the data obtained to find its location by simple triangulation. (The recording of sampling points uses a mixture of GPS technology and traditional note-taking.)

Finally, if a suitable WEP-protected network has been found (and it is carrying enough traffic) we attempt to break the encryption key. We leave a wireless-enabled UNIX laptop in place for a day or so, letting it sniff enough traffic to break the key. (Whether the sniffing and cracking are carried out at the same time depends on the tools used.)

The primary tool used for mapping the networks is *Netstumbler* (www.netstumbler.org), running on an iPAQ with additional wireless networking and GPS devices. For further characterisation of found networks we use standard, wireless-enabled Linux laptops.

Assumptions and Caveats

Detailed security analysis of internal networks found in this way is assumed to be outside the scope of this work.

The work takes place outside client buildings, using public access areas.

We would expect site security staff to be aware of our presence, but the work would not be generally announced.

What You Get

Our report will show all the wireless LANs found, with:

- 802.11 network information: MAC address, manufacturer, SSID and name
- security properties: authentication type and length of encryption key, ability to force clients to fall back to plain text mode
- IP information: network address and mask, domain name, host summary
- physical location: co-ordinates and description, estimate of boundary
- assumed ownership: client or other
- any other information or comments

This will also be presented as a geographical map.

A summary will identify significant security vulnerabilities and giving general recommendations on their resolution. This can be made available in suitable electronic form if necessary.

Related Services

Internal Network Mapping	A full survey that gives a clear picture of the number and types of systems on the internal networks.
Network Penetration Testing	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

All prices exclude VAT and are subject to confirmation.
Copyright © 2011 IDsec Limited