pentest
security assurance

Wireless Security Assessment and Penetration Testing Tools

By Mark Rowe

Overview

The security of 802.11 wireless LAN networks has been in the news a great deal over the last few months. Insecurities in the configuration of wireless access points and clients, especially default out of the box installations have been discussed as well as weaknesses the in the implementation of the 802.11b standard encryption called WEP (Wire Equivalent Privacy). The art of "war driving" (or "war walking, biking, boating, flying" depending on your mode of transport ;-)) has also seen a lot of press coverage. One positive thing all this exposure has achieved is to highlight how wireless security risks can impact the security of the standard networks they are attached to. Fortunately there are a number of actions that can be taken to minimise the wireless network security risk.

There are a number of very good resources on the Web that discuss in detail the wireless network vulnerabilities and that provide security analysis tools and solutions for them. There are also a number of companies including ourselves that offer wireless security solutions, tools and services. Part of the security solution is to discover and assess the security of your wireless access points and clients. To do this you will need a few tools. There are a number of commercial tools that can help you with this task, however, like war dialling there are also a number of free tools available on the Internet that do the job well. Because of the vast array of free software tools on offer, all of which have various software and hardware requirements, the freeware route can appear a little daunting at first.

This document intends to guide you through some of the hardware and software options you have to choose from. It is not intended to be a definitive guide to all the tools on offer or how to use them but as shopping list of items that you will need. Remember Christmas is approaching!

Note:- This is intended to be a series of articles. Other articles will discuss the techniques and methodologies that may be used when performing wireless security assessments and penetration tests.

The shopping list (some of these items are optional depending on the scope of your work):

Hardware

1x PC Laptop or Palm held. Toshiba Libretto or Compaq iPaq are good if you think small is beautiful. Dual boot (or VMware) MS Windows and Linux is even better putting a bigger choice of software at your disposal. We use dual boot with W2K and RedHat7.0.

1x 802.11b PCMCIA Wireless card based on the Hermes chipset. We use Lucent Orinoco Gold PCMCIA Cards. They have the advantage of having a connection for external antennas.

1x 2.4 GHz External omni directional antenna with Lucent Orinoco IEEE connector. This gives a much better reception than the in-built antenna and is good for walking or driving. We use the standard Lucent 5 dBi Indoor Range Extender antenna, however, there are others on the market including magmounts.

1x 2.4 Ghz Yagi 14dBi directional antenna (this is good for pointing at buildings to pickup signals from a distance or deep inside buildings. These are good for assessing how far the signal travels or to try and pin point where the signal is coming from. You will usually need a pigtail adaptor lead to convert from Lucent Orinoco IEEE to N-Type 50cm connector on the antenna. There are other high gain antennas on the market including grid antennas but be aware the use of this type of aerial isn't legal in all countries.

1x camera tripod or similar to attach the Yagi aerial to.

1x 802.11b PCMCIA Wireless card based on the PRISM2 chipset that is required by linux tools such as AirSnort. We use SMC EZ Connect Wireless PCMCIA card. Unfortunately this does not support external antennas.

1x GPS with a PC interface. This is used for logging signal strength/details against GPS co-ords etc. This can be useful if you have a large site and want to plot signal leakage especially when trying to decide on the best locations for access points. We use Garmin GPS II Plus GPS and data cable for connecting to the serial port.

Software

- Netstumbler- a good Windows tool for finding/identifying/plotting wireless LANS. Supports GPS logging. Works with Hermes chipset cards e.g. Lucent
- AirSnort- Linux based tool that gathers unmodified encrypted packets and then attempts to crack the WEP key. Works with Prism2 cards e.g. SMC card. Also requires Kernel source code, PCMCIA CS package source code, linux-wlan-ng (You must have version 0.18-pre13), wlan-monitor patch, AirSnort source. Alternatively you could just go and ask the administrator of the AP, although you may not want to do this if you are doing a penetration test.
- Ethereal with a "prismdump" patch to allow, "wireless sniffing".
- Wardrive from THC which is a Linux equivalent of NetStumbler. This also uses a wavelan card e.g. Lucent.
- THCRUT from THC. A useful suite of tools to aid penetrating into Wireless APs.
- LucentRegCracker used to decrypt WEP key stored in registry by Lucent Orinoco Client Manager.

This completes the toolkit. As we have said earlier you will find more tools out on the Net but the ones we have discussed will get you started. We have included below a few links to other resources that you may find useful. Some of which we have already mentioned. I have also listed other wireless cards that are known to work with the tools I have mentioned. We use these tools so feedback about these tools and others on offer is always welcome, please email Mark Rowe with any feedback.

Prism2 Chipset Cards

- Addtron AWP-100
- Compaq WL100
- D-Link DWL-650
- GemTek (Taiwan) WL-211
- Linksys WPC11
- Samsung SWL2000-N
- Z-Com XI300
- Zoom Telephonics ZoomAir 4100

Hermes Chipset Cards

- Lucent Technologies WaveLAN/IEEE (Orinoco)
- Dell TrueMobile 1150 Series (PCMCIA and mini-PCI)
- Toshiba Wireless LAN Card (PCMCIA and built-in)
- Compaq WL110
- Cabletron/Enterasys Roamabout
- Elsa Airlancer MC-11
- IBM High Rate Wireless LAN
- Buffalo Airstation (Melco) WLI-PCM-L11
- 1stWave 1ST-PC-DSS11IS, DSS11IG, DSS11ES, DSS11EG

Useful Websites

Description	URL
This is a good source	http://www.hyperlinktech.com/

for all things wireless, including antennas	
Airsnort can be found at	http://airsnort.sourceforge.net/
Netstumbler can be found at	http://www.netstumbler.com/
THC tools can be found at	http://www.thehackerschoice.com
A good site about Wardriving	http://www.bitshift.org/wardriving.shtml
Linux & Wireless LANs	http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/
Another good site about Wardriving	http://www.wardriving.com/
APTools is a utility that queries ARP Tables and Content-Addressable Memory (CAM) for MAC Address ranges associated with 802.11b Access Points. It will also utilize Cisco Discovery Protocol (CDP) if available. If a Cisco Aironet MAC Address is identified, the security configuration of the Access Point is audited via HTML parsing. APTools can be found at	http://aptools.sourceforge.net/

About Pentest

Established in 2001, Pentest Limited is a leading international provider of IT security, specialising in Web Application Security and Penetration Testing services. Pentest provides independent, practical advice to a wide range of clients across the UK, Europe, USA and Asia. For more information, or for further details about Pentest's services, please visit www.pentest.co.uk or call +44 (0) 161 233 0100.