The 802.11 Honeypot

Our hero has been violated by TV Journalists and the free-to-do-anything brigade, he has had to suffer humiliation because his boss published the location of his secret exploits on the internet and then tried to claim it was his own work, but now the details of the honeypot are out.

1 What is it

HONEYPOT - Weird name for a security device, but the derivation is clear. How do you catch nuisance wasps or bees? – well you use an old jam-jar or **honeypot**, with a bit of jam at the bottom. Hence the name.

In security, a HONEYPOT is a device which "sole purpose is to be hacked". It is not used to trap anyone or prevent them going about their business , lawful or otherwise but to study their behaviour. This particular honeypot is designed to record the actions of Wireless hackers, war-drivers and war-chalkers. This will enable us to get an insight in the level and type of activity currently occurring in the UK – to add foundation or dispel the FUD FEAR DOUBT UNCERTAINTY.

2 Why is it

With the onset of 802.11, like every new technology of the last few decades, comes a raft of conflicting information regarding its safety. The suppliers extol the advantages whilst the security theorist whinge-on constantly about non-specific, unquantifiable attacks. Meanwhile, the rest of us are left to try to weigh-up the risks of using WLANS. Someone needed to determine what the risk of 802.11 was – KPMG took on the job.

The technical risk of using any technology(excluding business impact) is traditionally represented as a function of:

exposure of the technology multiplied by *the probability of you being attacked*

In short this can be paraphrased as, the vulnerability or hack-ability of the WLANS multiplied by the probability that a hacker will pick you.

Therefore, we needed to determine two factors:-

www.loud-fat-bloke.co.uk

1) the vulnerability or hack-ability of WLANS; and
2) the probability that a hacker will pick you.

We undertook a fairly extensive piece of work to determine the hackability of the a wireless LAN. We found that we could:

- Crack the encryption used;
- Defeat the authentication and filtering mechanism used; and
- Intercept and spoof most sessions.

The results of which can be summed as HELP!!!!.

But how do you estimate the second part of the equation, *the probability of your 802.11Wlan being attacked.- The answer was provided* by the *802.11 honeypot*

3 Details of the 802.11 honeypot

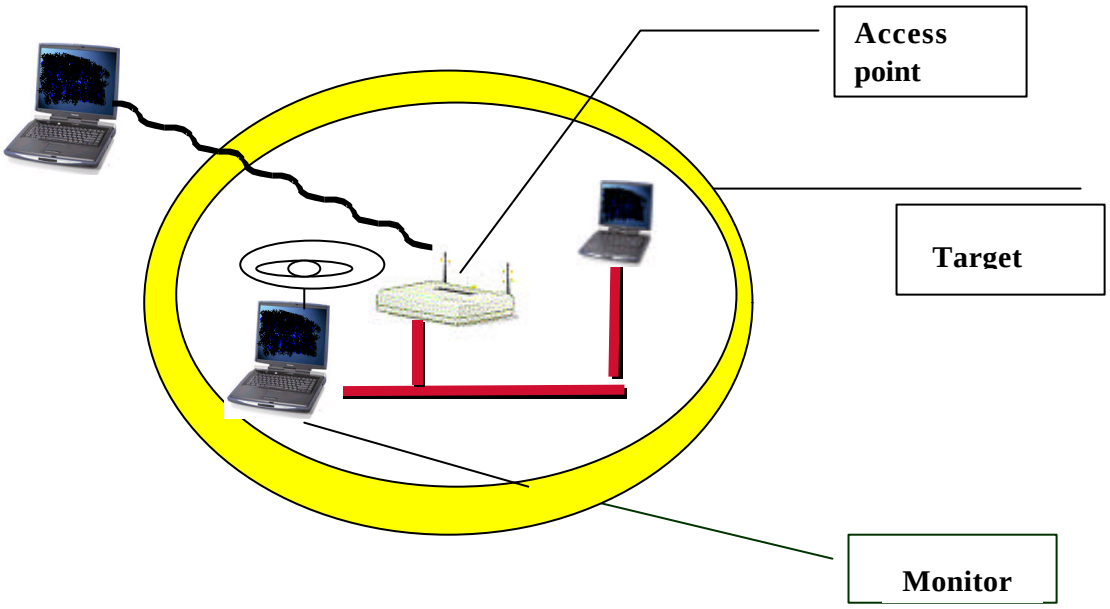
3.1 The Objective

This is a low user interaction honeypot – the commands that a hacker might use against a victim server are well documented and over publicized. The honeynet project do a fantastic job of researching this, a better job than we have time to do.

This honeypot is designed to research 802.11 activity. But research is the key word – this is a *research honeypot*, designed to be located in a number of different position, often in less than ideal circumstances. In such conditions we often find that things get unplugged or Cards removed. To this extend we have tried to ensure that a valid survey can be conducted if a service fails between manual checks – this means multiple data sources and physical precautions (see below).

www.loud-fat-bloke.co.uk

3.2 The technology



3.2.1 Monitor

Monitor is the key component to the honeypot. It performs two functions

1) It monitors raw Probe, Authentication and Association requests – this allows us to detect netstumbler, gtkskan and other network probes that occur at the data-link level.
2) It also monitors all IP traffic using snort. It does this in three ways:
   a) Records all in coming IP packets;

b) Produces a Vulnerability Alert for all well known attacks; and
c) Records all udp packets from the AP to the syslog server on the syslog port.

This Compaq m700 laptop was equipped with a built-in 10bt and a pcmcia DWL650 or ZoomAir 4100 card but did not have an IP addresses on either interface.

Because we had heard so much about it, we used the prism2 driver from the wlan-ng project. These did not have a particularly happy marriage with my favored Linux distribution, Mandrake. This resulted in some (shody) customisation of the kernel to make it all perform.

3.2.2 Target

This has an address of 10.0.0.1 and is a semi-hardened Win 2000 server, running a DHCP, IIS and ftp server.

- The DHCP server which will allocate addresses from the rest of the b class i.e. (10.0.0.3-10.6.6.5, 10.6.6.7-10.255.255.254) with an indefinite lease. This will enables us to link an IP address to a MAC address.
- The IIS server has one page – this is a dummy login page that records the user and password entered;
- The ftp server that just records all login attempts; and
- A syslog server.

The Target also has a packet sniffer running full time, logging its data into a compressed folder.

3.2.3 Access point

This is an Access point which provides the main connectivity – it has an address of 10.6.6.6. It has a fairly unremarkable configuration except that it logs association requests to the syslog.

3.3 Disaster-recovery

As described above, these devices are positioned in places that have poor physical environmentals –access controls and general hygiene. The study period

is 9 days, which is a long time to throw away because someone has unplugged your kettle lead. So we have defined a number of data sources to reduce single-point of failure

Description	Primary Data Source	Secondary Data Source
802Probe request	Monitor – wireless card	None
802association request	Monitor – wireless card	Target – syslog or Monitor – snort trace
Initial IP connection	Monitor – snort trace	Target – DHCP
Network research – scanning and discovery	Monitor – snort trace	Target – sniffer
user unsuccessful or successful	Monitor – snort trace	Target – IIS logs and FTP logs

3.3.1 Other high-tech design features

This ROFDCI factor of this project is very high. ROFDCI = Risk Of Failure Due to Cleaner Intervention. One thing we noticed is they like popping out the wireless card. We devised a technique to prevent this.

That's right!!! – we secured the card in with GAFFA tape.

www.loud-fat-bloke.co.uk

3.4 Traffic Classifications

Having spent ten years performing pentests and IDS maintenance, I have found other peoples interpretation of network attacks quite unspecific. We have borrowed snort traffic classification and augmented it to include 802.11. This results in a quantifiable traffic classification.

Classification	Short Desc	Long Desc	Priority
STD Snort classification	attempted-user	Attempted User Privilege Gain	1
STD Snort classification	unsuccessful-user	Unsuccessful User Privilege Gain	1
STD Snort classification	successful-user	Successful User Privilege Gain	1
STD Snort classification	attempted-admin	Attempted Administrator Privilege Gain	1
STD Snort classification	successful-admin	Successful Administrator Privilege Gain	1
STD Snort classification	shellcode-detect	Executable code was detected	1
STD Snort classification	trojan-activity	A Network Trojan was detected	1
STD Snort classification	web-application-attack	Web Application Attack	1
STD Snort classification	kickass-porn	SCORE! Get the lotion!	1
STD Snort classification	policy-violation	Potential Corporate Privacy Violation	1
STD Snort classification	bad-unknown	Potentially Bad Traffic	2
STD Snort classification	attempted-recon	Attempted Information Leak	2
STD Snort classification	successful-recon-limited	Information Leak	2
STD Snort classification	successful-recon-largescale	Large Scale Information Leak	2
STD Snort classification	attempted-dos	Attempted Denial of Service	2
STD Snort classification	successful-dos	Denial of Service	2
STD Snort classification	rpc-portmap-decode	Decode of an RPC Query	2
STD Snort classification	suspicious-filename-detect	A suspicious filename was detected	2
STD Snort classification	suspicious-login	An attempted login using a suspicious username was detected	2
STD Snort classification	system-call-detect	A system call was detected	2
STD Snort classification	unusual-client-port-connection	A client was using an unusual port	2
STD Snort classification	denial-of-service	Detection of a Denial of Service Attack	2
STD Snort classification	non-standard-protocol	Detection of a non-standard protocol or event	2
STD Snort classification	web-application-	access to a potentially vulnerable web	2

www.loud-fat-bloke.co.uk

Classification	Short Desc	Long Desc	Priority
	activity	application	
STD Snort classification	misc-attack	Misc Attack	2
STD Snort classification	not-suspicious	Not Suspicious Traffic	3
STD Snort classification	unknown	Unknown Traffic	3
STD Snort classification	string-detect	A suspicious string was detected	3
STD Snort classification	network-scan	Detection of a Network Scan	3
STD Snort classification	protocol-command-decode	Generic Protocol Command Decode	3
STD Snort classification	misc-activity	Misc activity	3
STD Snort classification	icmp-event	Generic ICMP event	3
STD Snort classification	tcp-connection	A TCP connection was detected	4
KPMG classification	802association req	Unauthorised 802 association request	4
KPMG classification	802Probe req	Unauthorised 802 probe	5

3.5 The Deployment Plan

The *802.11 honeypot* is a dummy portable wireless LAN that can be positioned in any office that has power supply. The deployment and the results are the subject of another document,

---