

802.11 b

Security Top Tips 0 Thru C (Hex!!!!!!)

OR

David the accountant doesn't like the numbers

12/8/02



www.loud-fat-bloke.co.uk

Tip0

Session key based crypto

Products with 128 bit WEP and static shared keys are not
ENOUGH

- Use 802.1 + EAP-like protocols (Leap, EAP-TLS); or
 - Use IPSEC VPNs at layer 3
- > This is an essential protective control – there are tools to retrieve static WEP keys which are freely available and easy to run (for the patient).

12/8/02



www.loud-fat-bloke.co.uk

TIP 1

Strong Authentication

WLANs are external, insecure networks where the authentication system is a common attack target. Login credentials should be strong enough to resist guessing and brute force attacks, both in respect of system entry and wide-spread DOS by account lock-out.

- > This is an essential protective control – the authentication system should be fully integrated with the system ensuring that prolonged access is only allowed after login which must be enforced on entry to the system.

12/8/02



www.loud-fat-bloke.co.uk

TIP 2

Harden Laptops

WLANs are external, potentially public networks – laptops exposed to them should be equipped with

- A current OS build
- Desk-top firewall; and
- Anti-virus software.

- > This is an essential protective control.

12/8/02



www.loud-fat-bloke.co.uk

TIP 3

Harden Access Points

Change any WLAN equipment default passwords and Essids. Other common-sense precautions would include, for instance:

- ensuring that SNMP settings are appropriate (I.e. community strings not guessable, MD5 authentication or address-lists)
 - prevent access to the internal Ethernet interface from the un-wired subnet.
- > This is an essential protective control – the access point is a primary target for abuse –should it be compromised, it would permit further entry to the core networks.

12/8/02



www.loud-fat-bloke.co.uk

TIP 4

Address Authentication is poor

In the 802.11b environment, MAC addresses and IP addresses are so easily spoofed that only marginal protection is gained by its use in authentication I.e ACLs.

MAC addresses protective or detective controls (IDS) will be easily defeated after a few mouse clicks when using site definable MAC address options on many devices

It is nice to segregate WLANs and internal (wired) networks with firewalls – Especially if you only allow a subset of traffic. But if general access to all internal systems from the wireless client is needed, what would the rules look like? The firewall may not provide any tangible protective control – only improved logging. The client address is not a valid form of authentication.

- > This is an essential protective control

12/8/02



www.loud-fat-bloke.co.uk

TIP 5

Disable ESSID Beaconing

By default 802.11 Access points broadcasts the name of the wireless network at a regular configurable time interval. This should be disabled as it can attract an attacker to the site.

- > This is an obfuscation technique – it will deter casual wardrivers
 - But the ESSID isn't a password – it is available, along with network nickname, in clear to anyone that can use a wireless packet sniffer.

12/8/02



www.loud-fat-bloke.co.uk

TIP 6

Use ESSIDs that do not Entice

The ESSID is a network name – it can be retrieved by the determined hacker. Descriptive names like *Bank_treasury_1* will provide an *incentive* to the *hacker*

- > This is an obfuscation technique – it will deter casual wardrivers

12/8/02



www.loud-fat-bloke.co.uk

TIP 7

Null ESSID connects

By default 802.11 clients can detect Access points by broadcasting a *probe packet* containing no or a *Null ESSID*. Some Aps provide even more inadvisable flexibility.

Obviously, this is for convenience – A legitimate internal user will have a machine pre-configured with this name or they can ask the help desk.

War-drivers and hackers can't – they will use this feature to compromise the network. DON'T USE IT

- > This is an obfuscation technique – it will deter casual wardrivers

12/8/02



www.loud-fat-bloke.co.uk

TIP 8

Wireless IDS and Monitoring

Many attacks occur at the 802.11 management level – these are not understood by standard IDS or network monitoring tools.

Store AP Logs and use 802.11 IDS or other security tools.

- > This is a detective control .

12/8/02



www.loud-fat-bloke.co.uk

TIP 9

Avoiding signal leaks

RF Signal shaping – Avoiding unnecessary signal leaks with a pre-install site surveys, which is necessary to determine equipment placement and optimum Wireless coverage. Use directional antenna to completely eradicate leaks .

- > Ensure adequate planning and design takes place.

12/8/02



www.loud-fat-bloke.co.uk

TIP A

Regular scans and assessments

Wireless lan equipment is readily available and therefore prone to unsanctioned installation. Regular scans and assessment insure your equipment is secure and limit unauthorised installs

- > This is an essential detective control .

12/8/02



www.loud-fat-bloke.co.uk

TIP B

Have a wired Backup

Wireless lan are still vulnerable to RF interference (blocking) and certain DOS attacks –so Have a wired Backup for mission critical systems

- > This is an essential Recovery control .

12/8/02



www.loud-fat-bloke.co.uk

TIP C

Only Closed systems

Most APS allow the following options:

- *Closed* – a system secured in a number of ways
- *Open* – a system unsecured
- *Both* – a system where either is accepted

Only closed is acceptable

- > This is an essential protective control .

12/8/02



www.loud-fat-bloke.co.uk



www.loud-fat-bloke.co.uk

12/8/02



www.loud-fat-bloke.co.uk