Flying Penguins

WaveLANs im Einsatz (Security)

4. Chemnitzer Linux-Tag

http://www.tu-chemnitz.de/linux/tag/

Michael Weisbach

linuxtag@tuts.nu

Agenda

- Können Pinguine überhaupt fliegen?
  - ja, sie können - mit folgenden Hilfsmitteln :)
    - (Hardware, kommt in Paul's Vortrag)
    - Software
- Haben Pinguine Angst vorm Fliegen? - Nö. Wieso auch?
  - Flugangst
  - Gefahren beim Fliegen allgemein
- Flugsicherung
  - Allgemeine Benutzungshinweise
  - Spezielle Hinweise für paranoide Pinguine

Grundlagen - Hardware

- PCMCIA-Karten
  - zahlreiche Hersteller, viele Karten - IEEE 802.11
  - oft Prism / Prism II basierend
  - Orinoco Silver / Gold, Elsa AirLancer MC-11, Compaq WL100, ...
- Access Points
  - ebenfalls diverse
- Add On's
  - Antennen
- Wie funktioniert das genau?
  - siehe Paul's Vortrag im Anschluss
  - http://grouper.ieee.org/groups/802/11/

Grundlagen - Software

- viele Karten, viele Treiber
  - siehe http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/
  - wvlan_cs.o - 1.0.7, discontinued
    - Wireless Extension, PCMCIA-CS
  - orinoco_cs.o - Version 0.10
    - Lucent/Cabletron IEEE 802.11 + Prism II
    - Wireless Extension, Kernel-PCMCIA 2.4
    - http://ozlabs.org/people/dgibson/dldwd/
  - prism2_cs.o - Version 0.1.13
    - Intersil Prism, Prism II
    - http://www.linux-wlan.com/linux-wlan/
- Wireless Tools (iwconfig, iwlist, iwspy, iwpriv, ...)
  - http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html
- WLAN-NG Tools (wlanctl-ng)
- don't panic - in den meisten Distrib's ist das bereits Plug&Pr^Hlay

Grundlagen - Betrieb

- Infrastructure Mode
  - 1 - n AccessPoints (AP's)
  - m Clients
  - "Gateway" (Bridge) ins normale Drahtnetz
- Ad-Hoc Mode
  - 2 - x Clients unterhalten sich direkt, d.h. ohne AP
- Host AP Mode
  - quasi eine spezielle Form von Infrastructure Mode

Flugangst und Gefahren

- Wireless LAN = Funknetz
  - Einfluss auf Gesundheit von Pinguinen & Umgebung
- Funk = unsichtbar, lautlos, ... - breitet sich nach allen Seiten aus
  - "oh, mein Nachbar kann mithören?"
  - Antwort vom Hersteller
    - "nein, wir haben WEP"
    - MAC-Address Filter
    - Hidden AP's
  - Antwort vom Hacker
    - "ja, lustig, oder?"

WEP ist sch*****

- Hardware mit Wired Equivalent Privacy (WEP)
  - "billig", einfach zu installieren, drahtlos, ...
- bedenkliche Entwicklungen und "Drive-by hacking"
  - Expo-Roboter
    http://www.heise.de/newsticker/data/ju-08.08.00-000/
  - Drive-by hacking
- Aufklärungsarbeit durch Aktivisten
  - http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
  - http://www.ccc.de/wlan/
  - https://wiki.ash.de/cgi-bin/wiki.pl?Wlan

Das Grauen hat viele Gesichter...

- AirSnort
  - http://freshmeat.net/projects/airsnort/
  - WEP aushebeln durch passives Mithören!
- Wireless-NG Tools
  - wlanctl-ng wlan0 lnxreq_wlansniff channel=N enable=true
- Kismet
  - http://freshmeat.net/projects/kismet/
  - benötigt WLAN-NG Treiber
  - Wireless Network Sniffer
  - GPS Integration :-)
- ...

... aber macht nichts!

- Flugsicherung - netter Versuch
  - "Funknetz-Verschlüsselung WEP wird ausgebessert" http://www.heise.de/newsticker/data/ea-08.02.02-000/
  - "Flicken für Sicherheitslöcher in Funk-LANs" http://www.heise.de/newsticker/data/ea-19.12.01-000/
  - jeder Hersteller versucht's auf seine Weise *seufz*
- Flugsicherung - Basic... das kann jeder!
  - IP Filter mit Netfilter, http://www.netfilter.org/
  - Port Tunneling mit OpenSSH, http://www.openssh.org/
- Flugsicherung - Advanced... ist leider aufwendiger
  - echtes VPN mit IPSEC, http://www.freeswan.org/

Tips und Hinweise

- Welche Karten sollte ich kaufen?
  - Geschwindigkeit 2MBit/s oder 11MBit/s?
    - 11 MBit/s
  - Silver/Gold, 40/128 bit WEP?
    - Silver bzw. 40 bit... mehr ist das Geld i.A. nicht wert
- Wireless sollte man nur einsetzen, wenn man sich im Klaren ist, was man tut!
  - mehr als 11MBit/s ist nicht drin (bzw. momentan kaum bezahlbar)
  - es ist und bleibt ein "offenes" Funknetz!!!
- Aufruf zur Aufklärung
  - Einsatz in Anwaltskanzleien, Steuerbüros und Krankenhäuser #-(

micha@vortrag # logoff <enter>

- Fragen?
- Antworten?!
- Diskussion!!!

Mehr Infos auch am SysAdmin-Demostand!