Wireless 101

The basics to 802.11

Agenda

- Basic Wireless Definitions
- Wireless Attacker Kit
- Demonstration
- Defense Strategy Against Attacks
- Questions

Requires Wireless Definitions

- SSID
  - –BSSID
  - –MAC Address
- Encryption / Authentication
  - –WEP
  - –WPA
  - –802.11i
  - –802.1x
- Fade / Freznel Zone
- Channel
- Frequency

SSID

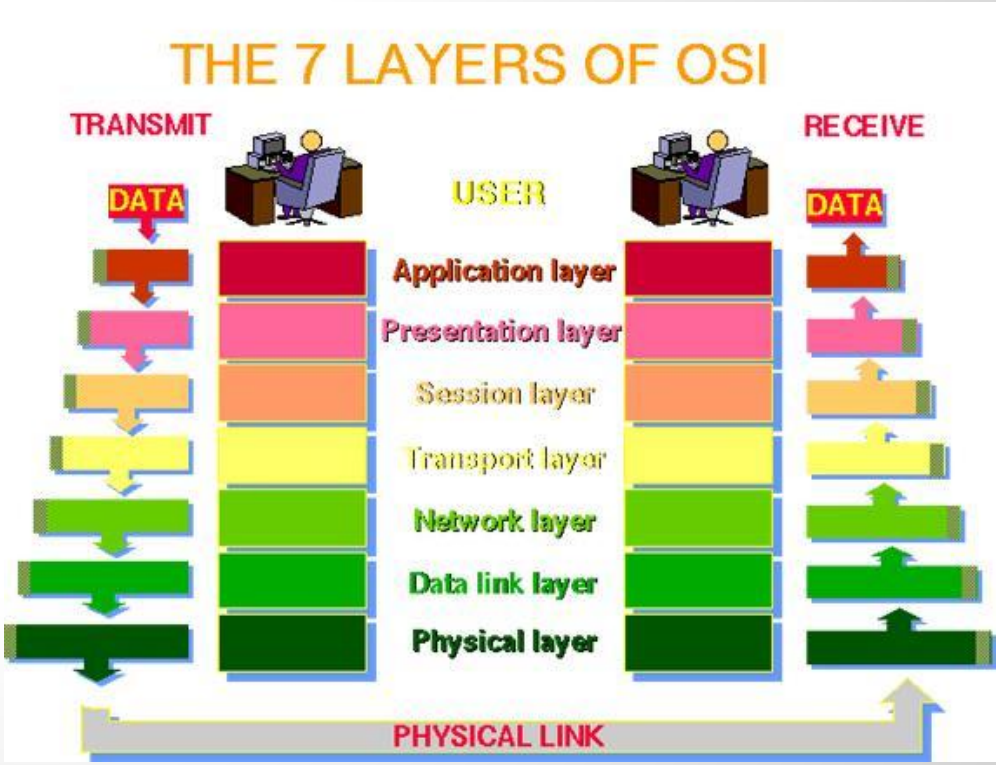
- “Service Set Identifier”
- Your “Wireless Network Name”
- Human Readable
- Can be disabled, but still discoverable

BSSID

- “Basic Service Set Identification”
- AP Identification by MAC Address
- (ESSID Share the same SSID & BSSID)

MAC Address
“Data Link” Layer

- Media Access Control
  - –Each device has one that is “unique”
  - –Example DE:AD:BE:EF:00:00
  - –Multiple MAC’s for WiFi
    - BSSID
    - Destination
    - Source



Encryption

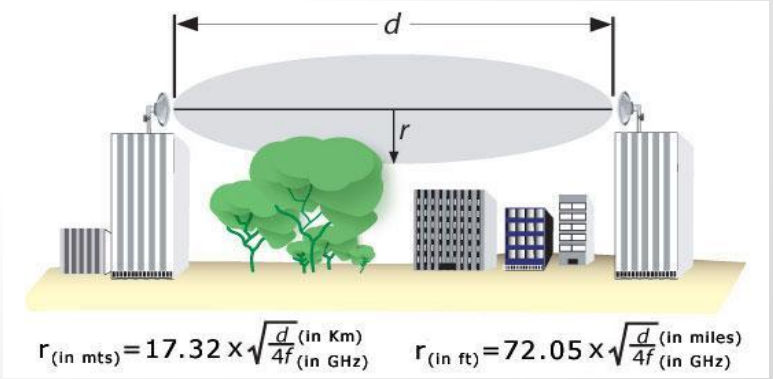
- WEP
  - –Though worthless for encryption, still useful as identifying a “private” network
- WPA
  - –PSK (typically version 1)
    - Broken using Rainbow tables (takes about ~10 minutes)
    - Can be made secure!
  - –Enterprise (typically version 2)
    - Uses dynamic key exchanges
    - Much stronger encryption (AES)

Fade / Fresnel Zone

- Fade
  - –The area where the signal strength begins to degrade the link's performance

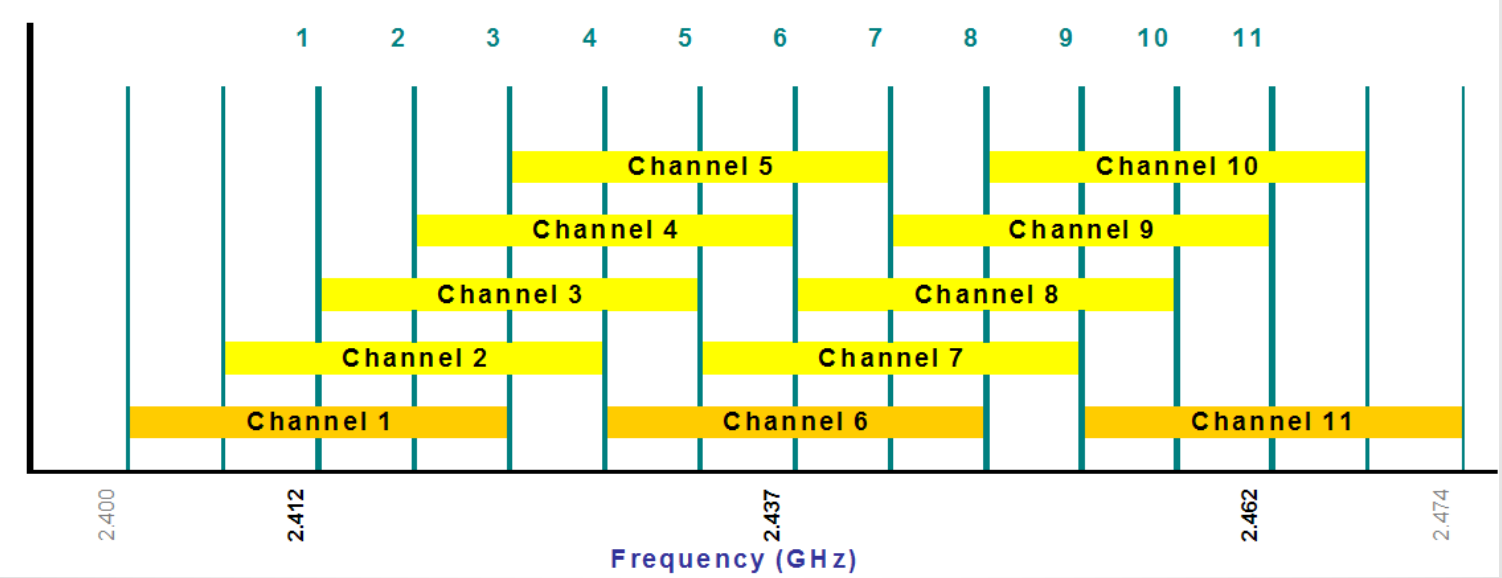
2. This photograph shows a typical microwave repeater station.

- Fresnel Zone
  - –the area around the visual line-of-sight that radio waves spread out into after they leave the



Channel

The frequency band allocated to a transmission



Wardriving

Warwalking

Warflying


Oceanside
Carlsbad
Valley Center
Jesmond Dene
San Pasqual
Ramona
Encinitas
Leucadia
Solana Beach
Del Mar Heights
La Jolla
Fernbrook
Eucalyptus Hills
Johnstown
Suncrest
Jamacha
Jamul
San Diego
Coronado
Palm City
San Ysidro
Imperial Beach Naval Air Station
Border Field State Park
Silver Strand State Beach
Cabrillo National Monument
Ft Rosecrans Military Reservation
Torrey Pines State Reserve
Cardiff State Beach
Mission Beach
Pacific Beach
Harmony Grove
Del Dios
Rincon Indian Reservation
San Pasqual Indian Reservation
Barona Ranch Indian Reservation
Brown Field Bombing Range
Jamul Mountain
Doghouse Junction
CRQ

Wireless Attacker Kit - Hardware

At the least…

- Computer
- GPS
- Two 802.11 NICs
- Antenna

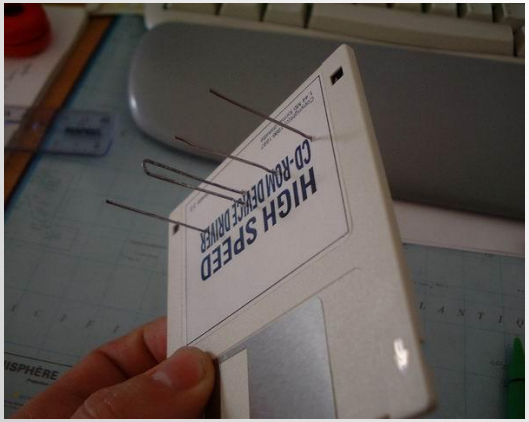
(Folding stock not included)

http://www.tomsnetworking.com/Sections-article106-page9.php

Antennas

Pringles Can

Coffee Can



Floppy Disk
Paper Clips

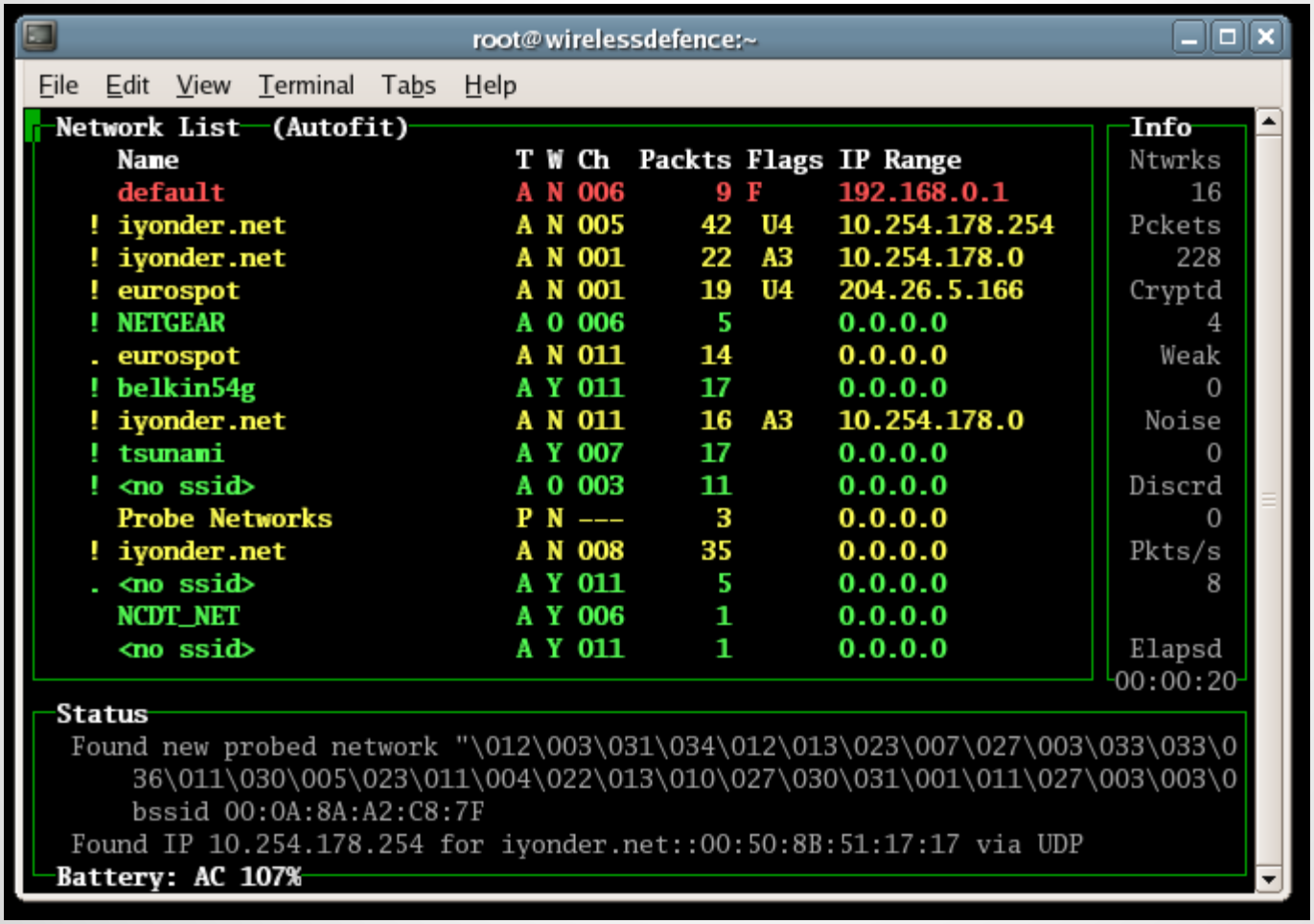
Discone

Wireless Attacker Kit - Software

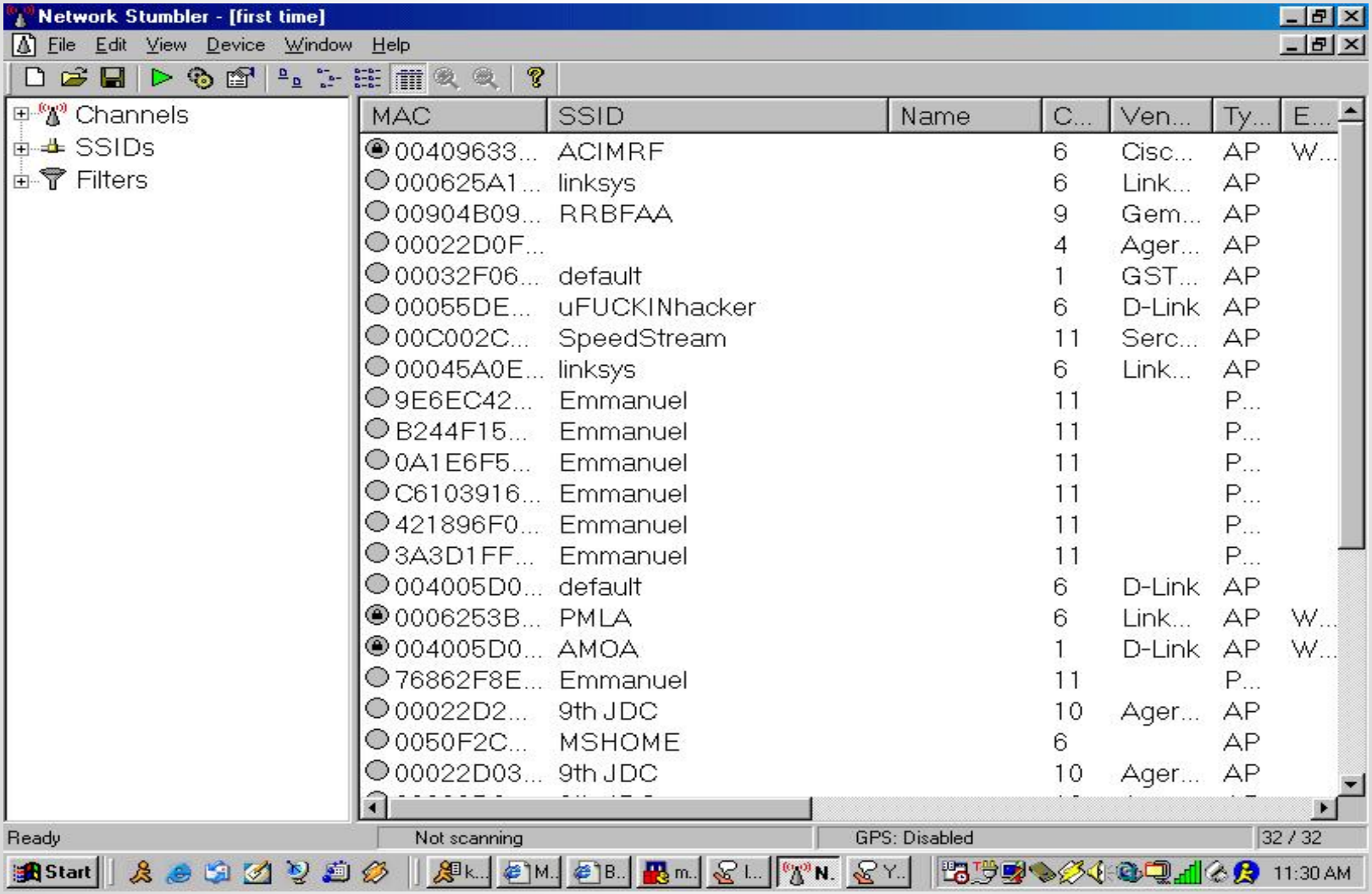
Kismet †	Backtrack†	FakeAP †
NetStumbler‡	Pentoo†	AiroPeek ‡
Wellenreiter † ‡	AirTraf†	WarLinux†

†For Unix/Linux Platforms
‡For Windows Platforms

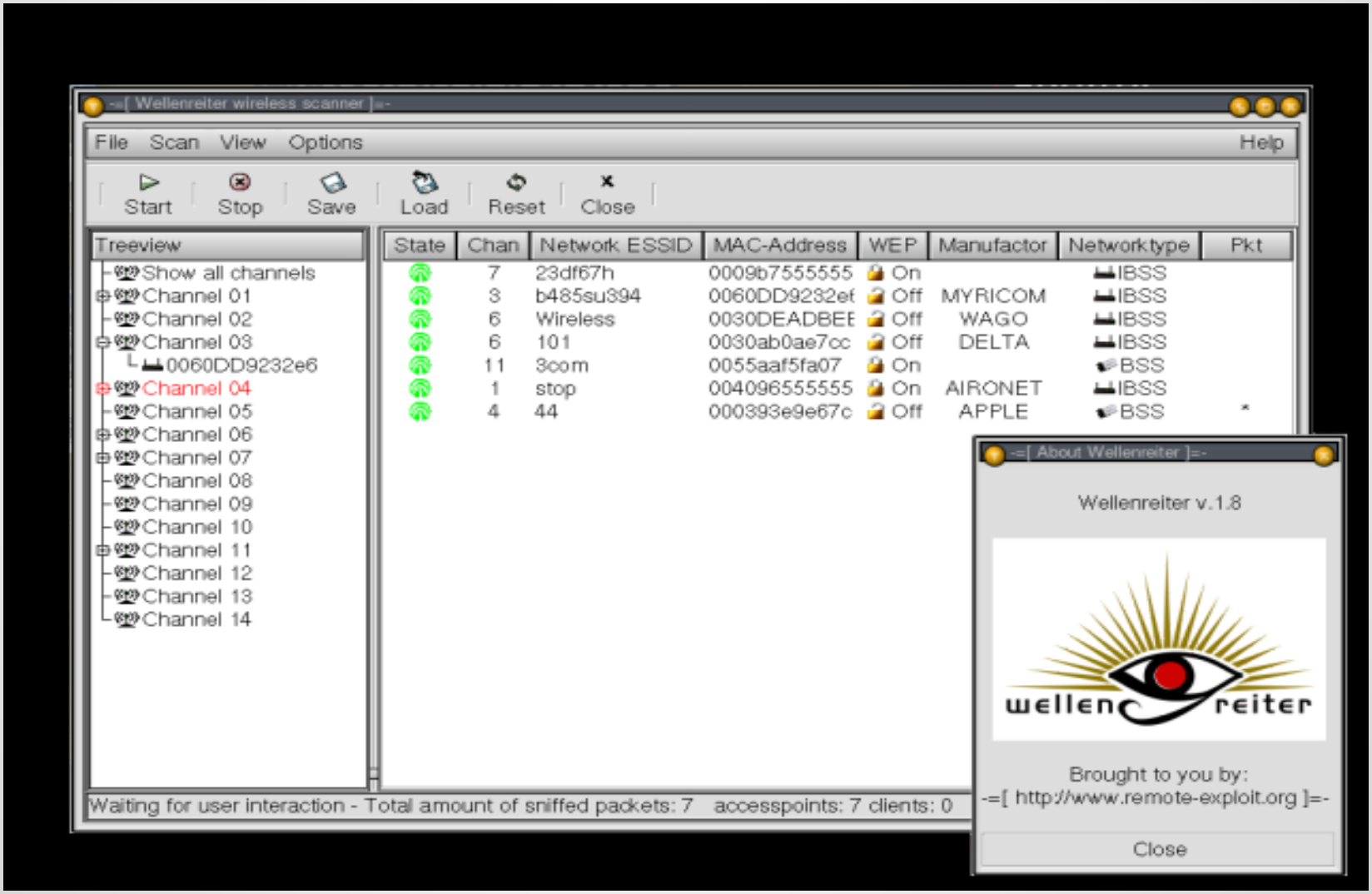
Kismet


root@wirelessdefence:~
File Edit View Terminal Tabs Help
Network List (Autofit)
Name T W Ch Packts Flags IP Range
default A N 006 9 F 192.168.0.1
! iyonder.net A N 005 42 U4 10.254.178.254
! iyonder.net A N 001 22 A3 10.254.178.0
! eurospot A N 001 19 U4 204.26.5.166
! NETGEAR A O 006 5 0.0.0.0
. eurospot A N 011 14 0.0.0.0
! belkin54g A Y 011 17 0.0.0.0
! iyonder.net A N 011 16 A3 10.254.178.0
! tsunami A Y 007 17 0.0.0.0
! <no ssid> A O 003 11 0.0.0.0
Probe Networks P N --- 3 0.0.0.0
! iyonder.net A N 008 35 0.0.0.0
. <no ssid> A Y 011 5 0.0.0.0
NCDT_NET A Y 006 1 0.0.0.0
<no ssid> A Y 011 1 0.0.0.0
Info
Ntwrks 16
Pckets 228
Cryptd 4
Weak 0
Noise 0
Discrd 0
Pkts/s 8
Elapsd 00:00:20
Status
Found new probed network "\012\003\031\034\012\013\023\007\027\003\033\033\036\011\030\005\023\011\004\022\013\010\027\030\031\001\011\027\003\003\0
bssid 00:0A:8A:A2:C8:7F
Found IP 10.254.178.254 for iyonder.net::00:50:8B:51:17:17 via UDP
Battery: AC 107%

NetStumbler



Wellenreiter



Pentoo


Analyzer
Bluetooth
Cracker / Bruter
Database
Exploit
Footprint
Forging
Fuzzers
Misc
MITM
Proxy
RCE & Forensics
Scanner
SIP / VoIP
Wireless
Fusil
Bed
Bss
Fuzzer-server
Httpfuzz
Ohrwurm
Peach
Smtpfuzz
Smudge
Taof
Fusil-clamav
Fusil-firefox
Fusil-gettext
Fusil-gstreamer
Fusil-imagemagick
Fusil-libc-printf
Fusil-mplayer
Fusil-ogg123
Fusil-php
Fusil-poppler
Fusil-python
Fusil-vlc
Fusil-wizzard
Fusil-zzuf
Main
Pentoo
Applications
Files
Run Command
Desktop
Windows
Lost Windows
Enlightenment
Settings
System

Wireless IDS

- Some cases, still a very young technology
- Can be evaded
- Watches a small world
  - –802.11a (5.2 GHz and 5.8 GHz)
  - –802.11b/g (2.4 GHz, but different spectrum management)
  - –802.11j / Public Safety (4.7 - 4.9 GHz)
  - –Bluetooth!!! (yes, they have AP's too)

Reconnaissance

- Wigle.net
- Google.com
- Local message boards
- Use your IMAGINATION

Deployment

- Use the right antenna for the right job
- Use the right amount of power
- Pay attention to your surroundings
  - Public roads, parks, etc
- Policies
  - Warning banners, private network messages, etc

Wireless Forensics Challenges

- Few solutions out there
  - –Solutions are generally not “court certified” (yet)
- Building is an option
  - –Must use FCC Certified components and be in operating compliance
- Procedure and expertise
  - –Wifi is “Layer 1” and up
  - –Radio and Network Engineer
- Physical environment presents their own challenges

Wireless Forensics - Antennas

Grid / Dish

Omni

Yagi

Panel

http://www.l-com.com

Wireless Forensics Kit

- A very fast computer with lots of disk space
- Two GPSs (one for backup)
- Multiple 802.11 NICs
  - Fourteen for 802.11 b/g
  - Eighteen for 802.11 a
- Antennas
- Kismet (Don't be Evil / 9th Circuit)
- Camera

Questions


WHAMOND 12-9
MUST HAVE SOMETHING TO DO WITH WIRELESS TECHNOLOGY...
© 2000 UFS, Inc.