

A vertical barcode is located on the left side of the red background.

Today's challenge on Wireless Networking

David Leung, CISM
Solution Consultant, Security
Datacraft China/Hong Kong Ltd.

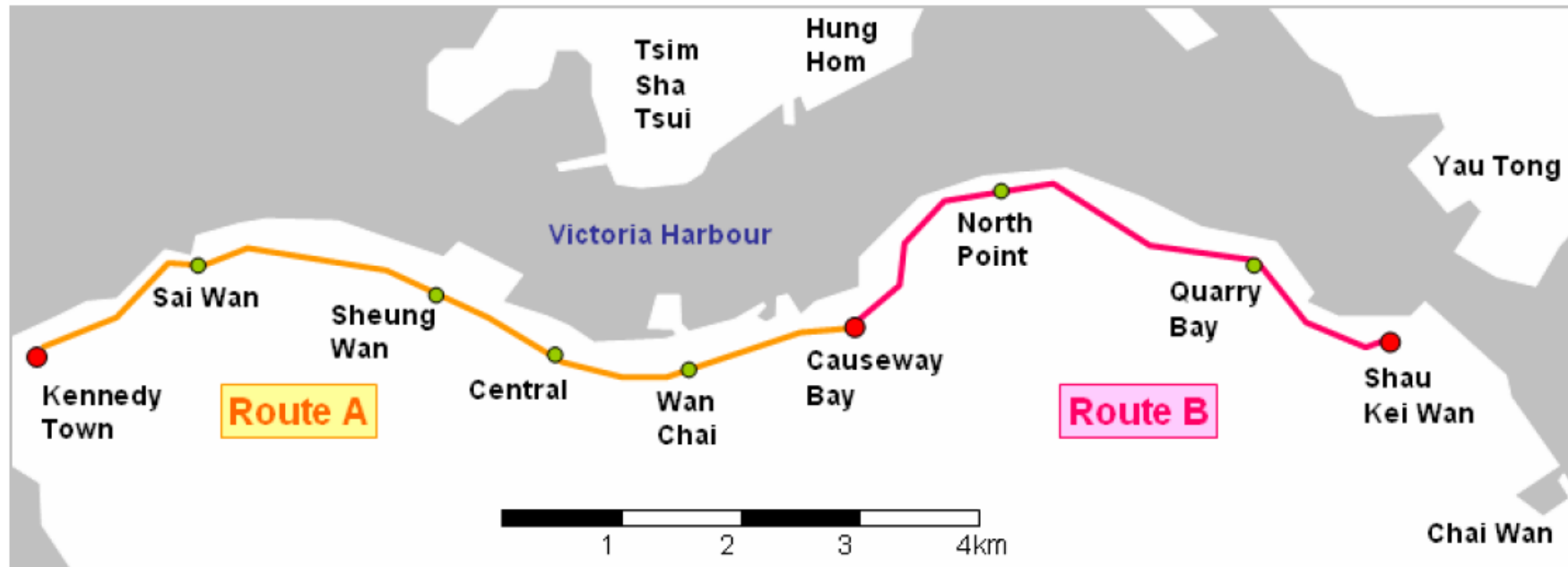
Agenda

- How Popular is Wireless Network?
- Threats Associated with Wireless Networking
- Wireless Security – the Revolution
- Layered Wireless Security Approach
- Maintaining Good Health - Wireless Assessment



How Popular is Wireless Network?

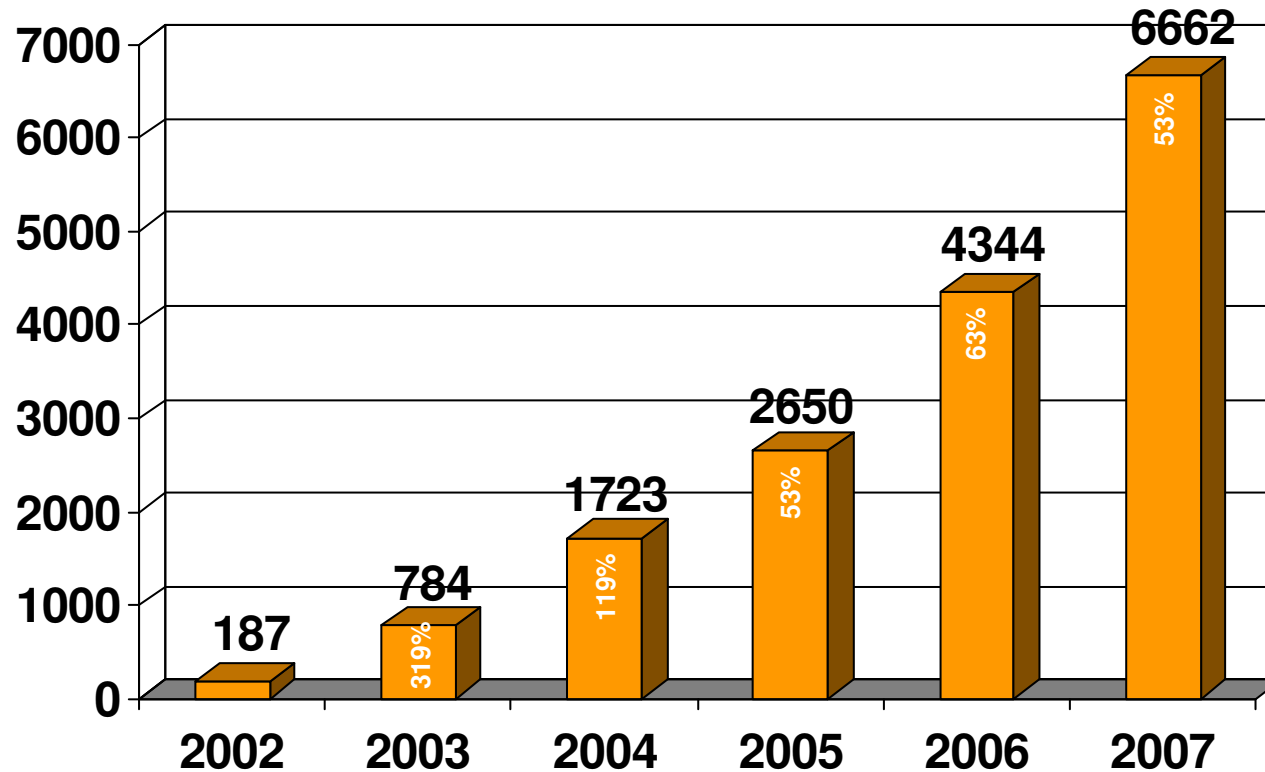
War Driving 2007 – PISA



War Driving Route

How Popular is Wireless Network?

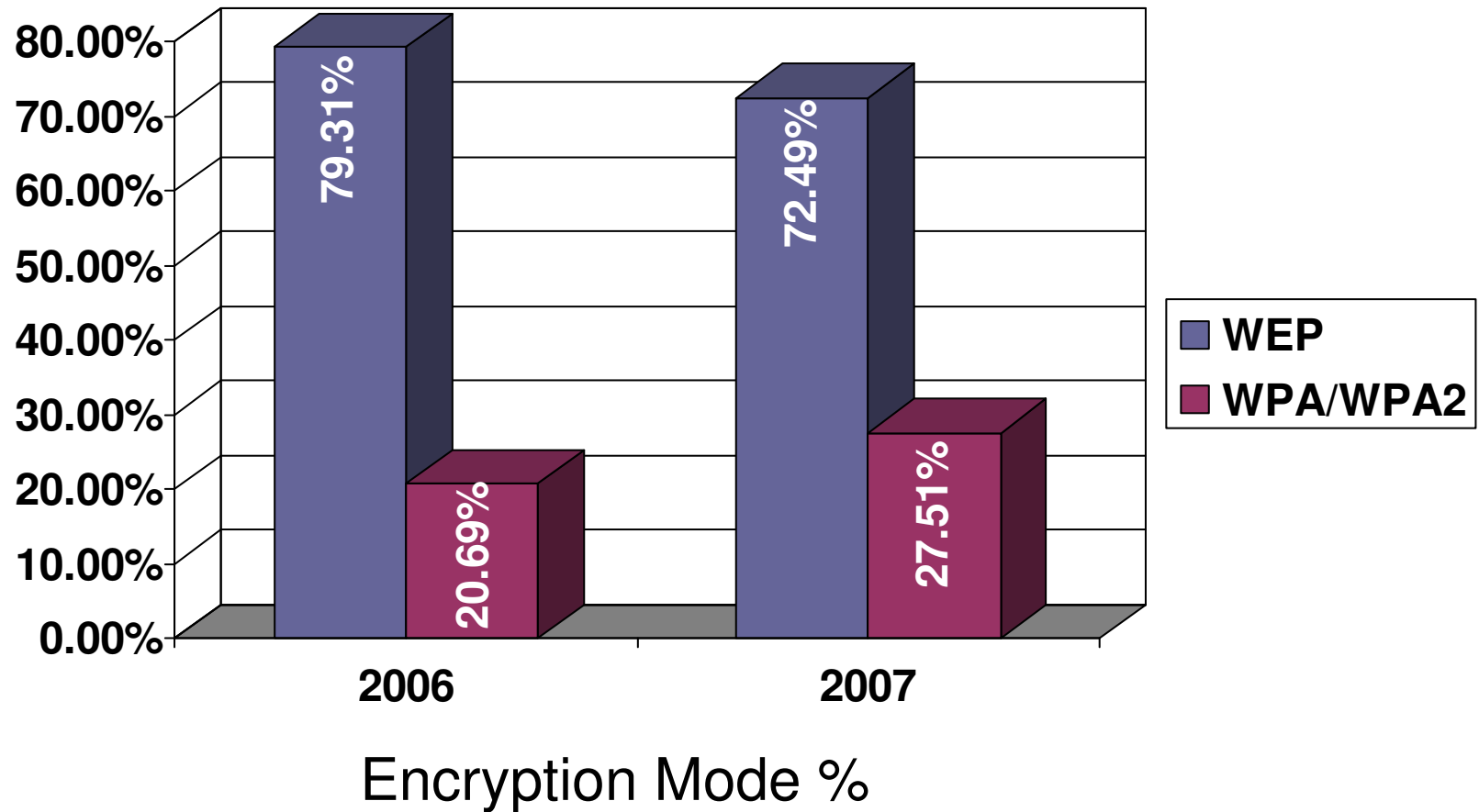
War Driving 2007 – PISA



No. of APs discovered

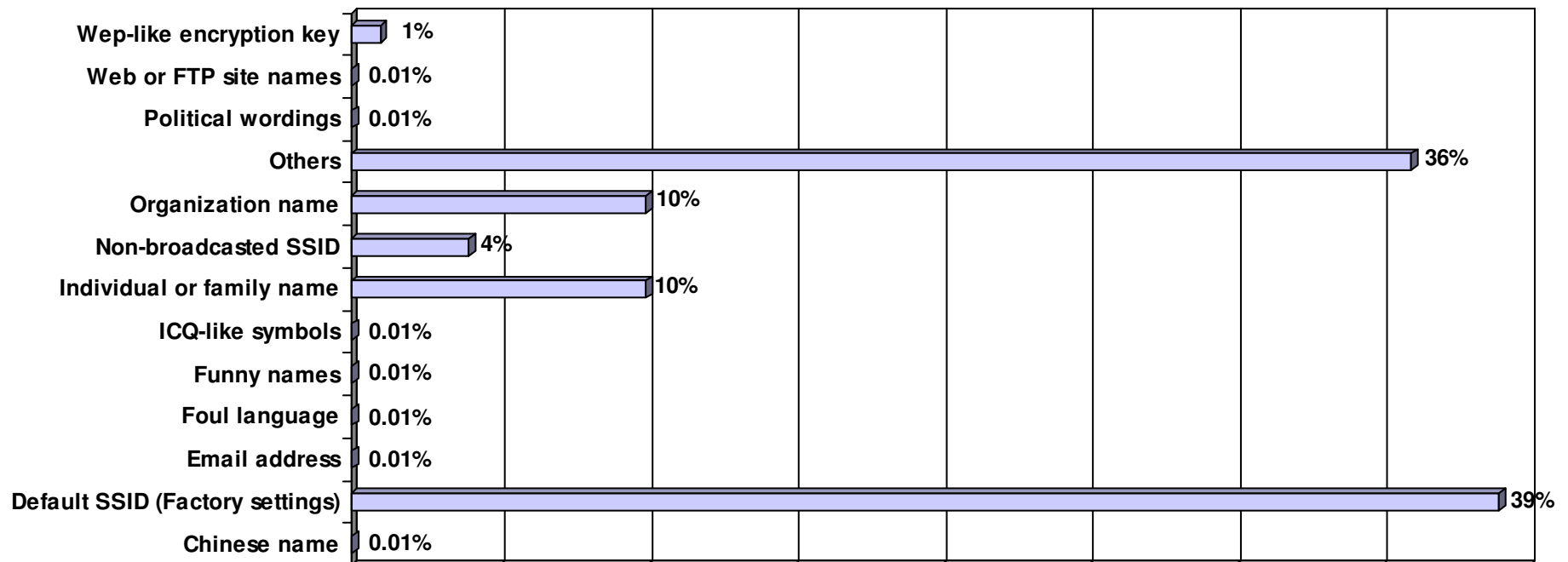
How Popular is Wireless Network?

War Driving 2007 – PISA



How Popular is Wireless Network?

War Driving 2007 – PISA



SSID Analysis

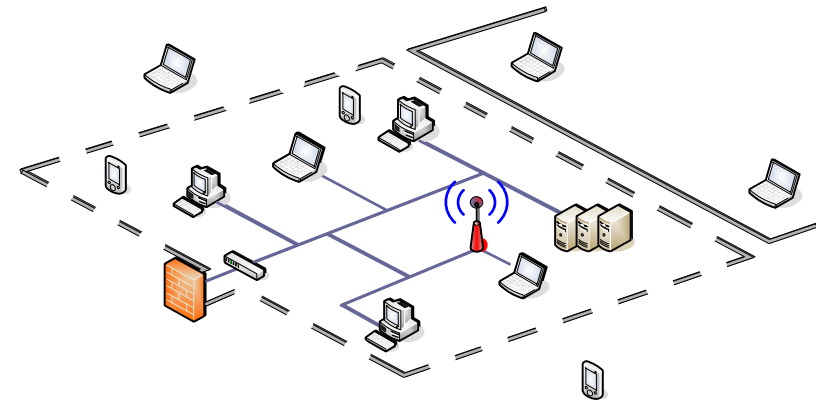
Traditional Network Environment

Protection focused on Network Entry Point (Outside-In)

- Firewall
- VPN
- 2-factor logon

Less worried on internal

- Bounded by Physical Protection
- Less likelihood on internal security incidents
- End point security for road runners
- Standardized H/W, O/S, applications



As Wireless Network Deployed The Network Becomes Boundaryless

Physical boundary have been removed

- No more walls to protect your NETWORK
- Radio signal leakage
- Insufficient planning
- Mis-configurations

Wireless Networking is Invisible!

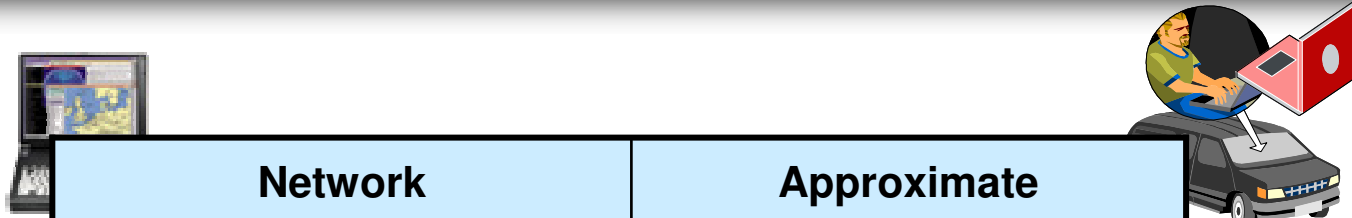
WiFi Encryptions – How secure they are?

- WEP (Wired Equivalent Privacy)
 - Shared Key: 64 or 128-bit WEP Key (24-bit IV included)
 - Packet encrypted by RC4 streams
 - Security weakness
 - Short Key size (2^{20} RC4 keys)
 - IV collisions or altered packets
 - Can be cracked within hours
- WPA2 (WiFi Protected Access)
 - Created in response to serious weaknesses found in WEP
 - Personal
 - 8 to 63 character Pre-shared Key
 - Enterprise
 - 802.1X authentication / Radius (individual has their own password)
 - TKIP or AES encryption
 - Technically more secure

Identity Theft

- Spoofing – Mac Address, SSID etc.
- Breaking encryption
 - 50% successful rate with 40,000 packets
 - 95% successful rate with 85,000 packets
 - 104-bit WEP key can be break within 3 seconds with 40,000 packets
 - Hacking tools on wireless client WEP Cracking, not AP anymore
 - The Café Latte Attack
 - WepOff

Threats Associated with Wireless Networking



Network Configuration	Approximate Cracking time
Shared + DHCP	~ 6 minutes
Shared + Static IP	~ 6 minutes
Open + DHCP	~ 6 minutes
Open + Static IP	~ 6 minutes

Probing & Association with target victim

Send numerous ARP Requests to victim

Collect sufficient ARP Responses for WEP Cracking

Denial-of-Service Attacks

- Aim to prevent legitimate users from accessing network resources – loss of production
- DoS on perimeter of Network (e.g. F/W, Mailserver etc.)
 - Single point of attack, single point of protection
 - Most F/W and Anti-Spam can block malicious connections
- How about multiple point of attacks = multiple point of protection
 - Jamming Wireless Signal in a matter of seconds
 - Your internet connections still works.....but you users can't access it.
 - Heavy workload to IT Support
 - Again, No trace at all

How easy to crack WEP?

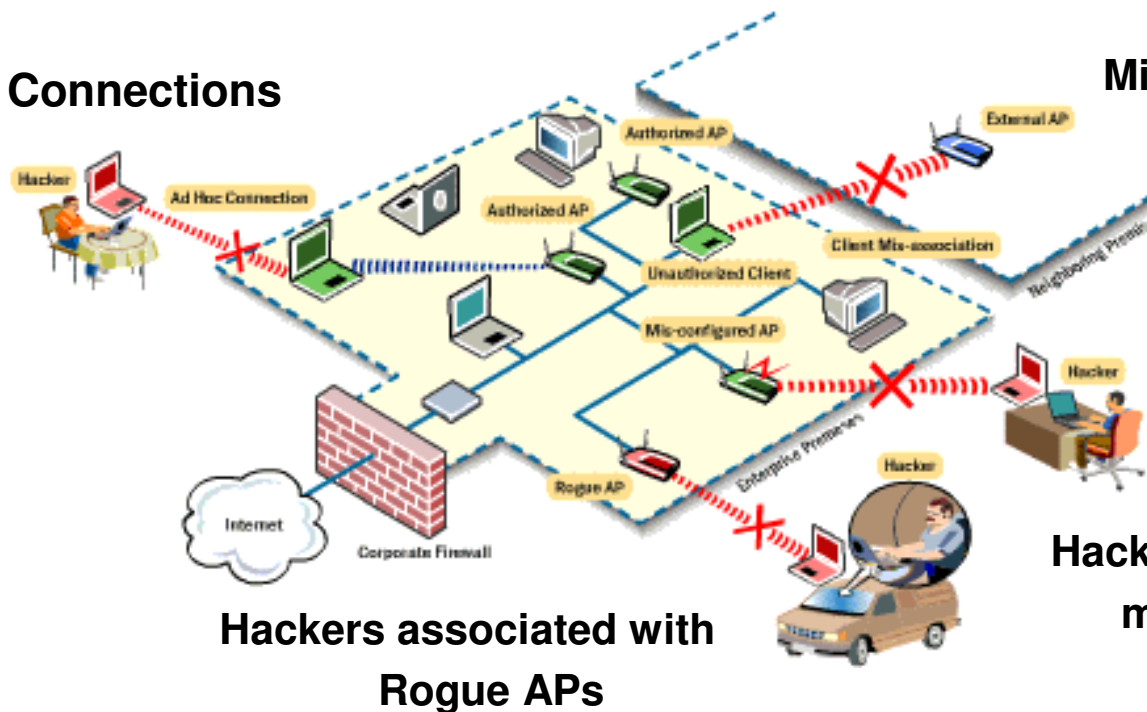
1. Setup equipment
 - a Computer
 - WiFi card that supports monitoring mode and packet injection
 - Market available tools e.g. Backtrack CD
2. Find the target (SSID)
 - Airdump-ng
 - Net Stumbler
3. Capture Data from Air
 - Airmon-ng
 - Airodump-ng
4. Wait.....or make the network busy
 - Aireplay-ng
 - Packetforge-ng
5. Crack WEP key with Captured Data
 - Aircrack-ng



Threats Associated with Wireless Networking

Scary enough!? What more is coming!

Ad Hoc Connections



Mis-association with external APs

Hackers associated with mis-configured APs

Hackers associated with Rogue APs



New Wireless Security Approach



3 Monitor for Security & Compliance

(Security. Policy. Enforcement. Operational Support)



1 Secure Wireless Devices (Laptops, Access Points, PDAs...)

2 Secure Communications (Encryption & Authentication)



New Wireless Security Approach



1) Securing Wireless Devices

- Reconfigure from default settings (SSID, Admin login, Password etc.)
- Establish set Channels of operations – off channel traffic as suspicious activity

2) Secure Communications

- MAC address filtering
- WPA-2 encryption.....and keep updates
- VPNs
- Personal Firewall
- End-point security

New Wireless Security Approach

Datacraft

The screenshot displays a software interface for wireless tracking. On the left, a floor plan of a building is shown with several green location markers. A red 'F' icon is also present on the plan. Labels for the markers include '192.168.1.1', '17F Middle', '17F MRoom 3', and '17F Left'. On the right, a 'Tracking Information' panel provides details for the selected device.

Tracking Information

Device: 192.168.1.1
Status: Located successfully
MAC: 00:03:9d:4f:2f:e5
Channel: 7
SSID: BenQ
Protocol: 802.11b
Last Seen: 15:12:49 PM Jan 23

Sensors:

17F Middle	-45 [dbm]
17F MRoom 3	-57 [dbm]
17F Left	-66 [dbm]

Stop Tracking

Common Mis-concepts

- I do not deploy wireless networking
- I do not allow my users to use wireless

How can you be sure?

10 Steps on Wireless Assessment:

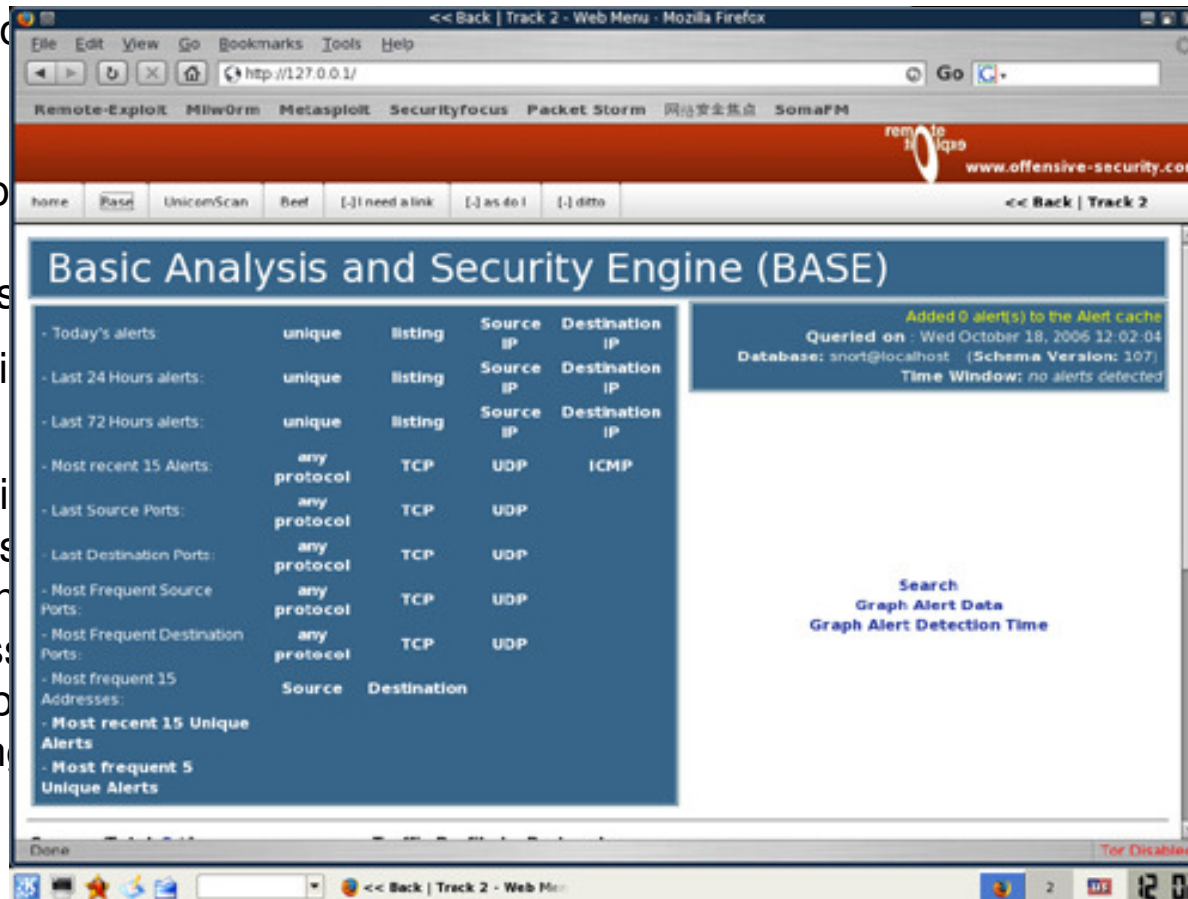
- 1) Review existing security policies
- 2) Review the system architecture and configurations.
- 3) Review operational support tools and procedures
- 4) Interview users
- 5) Verify configurations of wireless devices
- 6) Investigate physical installations of access points
- 7) Identify rogue access points
- 8) Perform penetration tests
- 9) Analyze security gaps
- 10) Recommend improvements

Maintain Good Health – Wireless Assessment

BackTrak

- Free suite of tools
 - Snort
 - ntop
 - db_auto
 - kismet
 - unicorns
- No Installation
- What it can do
 - Foot-printing
 - Analysis
 - Scanning
 - Wireless
 - Brute-force
 - Cracking

App Vulnerability Scanner, Site Policy Engine



PISA War Driving 2007

<http://www.pisa.org.hk/event/war-driving-2007.htm>

Network Stumbler

<http://www.netstumbler.com/>

The Café Latte Attack

<http://www.airtightnetworks.net/knowledgecenter/ppt/Toorcon.ppt>

AirDefense Network

<http://www.airdefense.net>

AirDefense Network

<http://www.airdefense.net>

The background of the slide is a solid red color. On the left side, there is a vertical white barcode-like pattern. In the center, the text "End of Presentation" is written in a bold, white, sans-serif font. There are also some faint, light red curved lines and shapes in the background, possibly representing a stylized 'D' or abstract shapes.