Wireless LAN Security

Understanding and Preventing Network Attacks

Objectives

- Demonstrate how to recognize, perform, and prevent attacks
- Discuss the impact of these attacks on an organization

Topics

- Wireless LAN Auditing Tools
- Wardriving
- Freeway discovery applications NetStumbler, Kismet and KisMAC
- Wireless Zero Configuration
- Wireless Client Utilities
- Gathering information
- Conclusion

802.11 in a nutshell

- 802.11 Link-layer protocol, IEEE
- Wi-Fi and Wi-Fi Alliance
- Spectrum
- Ad-hoc mode (peer-to-peer), Infrastructure mode (with AP)
- Packets (source, destination, BSSID)
  - Data
  - Management (Beacons, Deauthentication)
  - Control (RTS, CTS)

Wireless LAN Auditing Tools

- Auditing is the act of verifying that the configuration of the network is in compliance with policies and provides adequate protection from attackers of both the malicious and unintentional natures.
- Auditing procedures include penetration testing, configuration verification and other device and system-specific measures.

Cont…

- Few examples of auditing tools are:
  - Wireless LAN Discovery Tools
  - Wireless Protocol Analyzers
  - Antennas and WLAN Equipment
  - Password Capture and Decrypt
  - Hijacking Tools
  - RF Jamming Tools
  - Etc..

Wardriving

- Wardriving is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle using a Wi-Fi-equipped computer, such as a laptop or a PDA.
- Software for wardriving is freely available on the Internet, notably, NetStumbler for Windows, Kismet for Linux, and KisMac for Macintosh.

Source : http://en.wikipedia.org/wiki/Wardriving

NetStumbler

- NetStumbler (also known as Network Stumbler),written by Marius Milner, is a tool for Windows that facilitates detection of Wireless LANs using the 802.11b, 802.11a and 802.11g WLAN standards.
- It runs on Microsoft Windows operating systems from Windows 98 on up to Windows Vista.
- More information about Netstumbler can be found at www.Netstumbler.com.
- A trimmed-down version called MiniStumbler is available for the handheld Windows CE operating system.

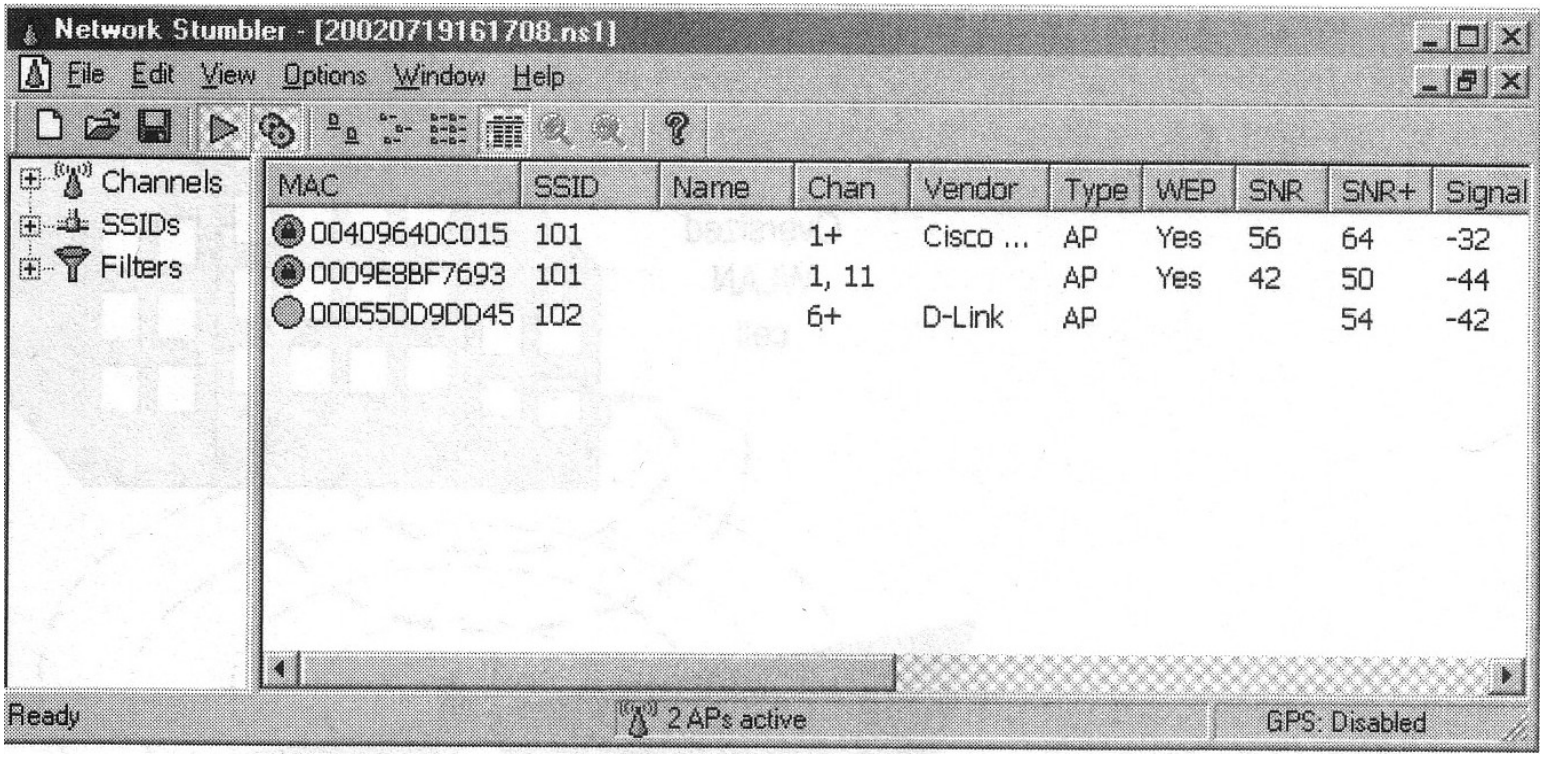
source: http://en.wikipedia.org/wiki/NetStumbler

Cont…

- When NetStumbler finds an access point, it display the following information:
  - MAC Address
  - SSID
  - Access Point name
  - Channel
  - Vendor
  - Security (WEP on or off)
  - Signal Strength
  - GPS Coordinates (if GPS is attached)

Cont…

- Sample output from NetStumbler



Kismet

- Kismet, written by Mike Kershaw, is an 802.11 wireless packet analyzer.
- It runs on the Linux operating system and works with most wireless cards that are supported under Linux.
- kismetwireless.net is a large source of information about the use of Kismet and war driving.

Cont…

- Some features of Kismet are:
  - Multiple Packet sources
  - Channel hopping
  - IP block detection
  - Hidden SSID Decloaking
  - Manufatcurer Identification
  - Detection of Netstumbler clients
  - Runtime decoding of WEP packets.
  - etc

KisMAC

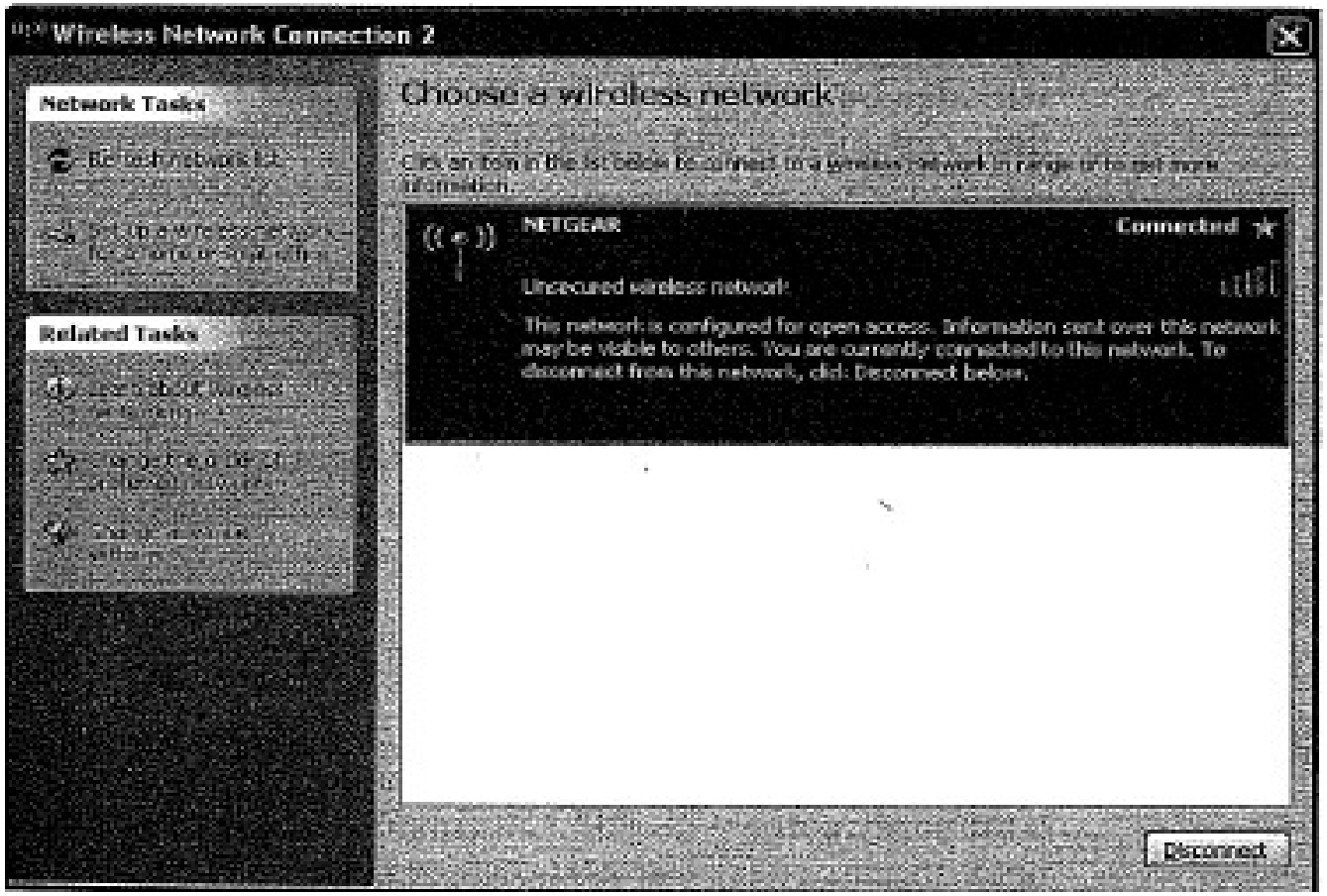
- KisMAC is a wireless network discovery tool for Mac OS.
- It has a wide range of features, similar to those of Kismet and it is more powerful than Kismet.
- More information can be found by searching for KisMAC at google.com

Wireless Zero Configuration

- Wireless Zero Configuration (WZC), also known as Wireless Auto Configuration, or WLAN AutoConfig.
- It is a service that dynamically selects a wireless network to connect to based on a user's preferences and various default settings.
- It is included with modern versions of Microsoft Windows.
- More information about WZC can be found at www.microsoft.com , search with the keyword wireless auto configuration.

Cont…

- WZC Available Networks



Wireless Client Utility Software

- Wireless Client Utility Software is used to perform site surveys and, in effect, network discovery.
- These software tools gives the information that include list of available networks, Security (WEP on or off) and the channels that are using.

Wireless Client Utility Hardware

- The most common tools used in wireless LAN discovery are:
  - Laptops and table PCs.
  - Handheld and PDAs.
  - Wi-Fi Finders.
  - Antennas and wireless LAN Equipment.

Gathering Information

- Auditors and attackers use various processes to gather information about a network.
- The various methods include:
- Social engineering
- Search Engines
- Public Records
- Garbage Collection

Social Engineering

- Some well-known targets for this type of attack are:
  - Help Desk
  - On-site contractors
  - Employees

Conclusions

- A Wireless network administrator or Auditor should understand how to secure his or her wireless devices over time withstanding new vulnerabilities and attacks.
- Explained some available Freeware discovery applications.