Basic
Wireless Audits & Penetration Tests

ISACA
Serving IT Governance Professionals
San Francisco Chapter

Jeff Camiel

- Director, Technology Risk Management
- Jefferson Wells
- 18 years in security, 20 years in technology
- CISSP, CIPP
- Been there, Done that

Rob Tillman

- Professional, Technology Risk Management
- Jefferson Wells
- 12 years in security and information systems
- RCT,RCE,RHCE, MSCE 2003, MCP 2000
- Been there, done that, doing that

Index

- A Little Fun
- Threats, Risks & Controls
- Audit Program
  - Vulnerability Assessment
  - Penetration Testing

The Plant

Leroy is your worst nightmare!

- Easily placed
- Not Noticed
- Opens your network
- Skill Level - Nerve Only

The Lab

- The Access Point
- The Client (Victim Box)
- The Attacker
  - Two nic cards
- Antennas

A Little Fun

- One big antenna
- One tripod
- One laptop
- Open source software
- A projector

One priceless education!!

History of Interception

- Messengers with documents - Mugging
  - Solution: Encryption:Seals
  - Point-to-Point
- Hardwire - Wiretap
  - Solution: Fiber optics: Encryption
  - Point-to-Point
- Wireless - Carrier Interception
  - Solution: Authorization: Encryption
  - Broadcast
- Voice - Overhearing
  - Solution: The Cone Of Silence

Wireless Defined

Any broadcast technology that enables connection to a device that does not require physical cables

80211.x

Bluetooth

IR

etc

Risk, Vulnerabilities & Attacks

Risk

Communication Interception

Unauthorized Access

Vulnerabilities

Removal of Physical Security

Poor Configuration

Poor Encryption

Network Connection Cross-Over

Attacks

Against Non-Secured Access Point

Attacks against WEP, WPA

Attacks against VPNs

Audit Programs

Vulnerability Assessment

And

Penetration Testing

Audit Program - Vulnerability Assessment

- Vulnerability Assessment
  - Governance
    - Policies, Standards, Procedures & Controls
  - Process
    - Access Control
    - Event Monitoring
    - Rogue Access Monitoring
  - Technology
    - Architecture Review
    - Configuration Review

Audit Program - Penetration Testing

- Objective Set
- Access Point Identification
- Authorized Access Point Validation
- Access Point Configuration Testing
- Encryption Cracking
- Client Attack
- Target Acquisition

Audit Program - Penetration Testing

- Un-secured access points
- WEP
  - Weak IV
  - Statistical Attacks
  - Dictionary Attacks
- WPA-PSK
  - Dictionary Attacks

Audit Program - The Details

Vulnerability Assessment

Audit Policies, Corollaries, Standards

- Expected Results
  - Policy
    - Wireless access points may only stay connected to the organization's network while complying with all wireless access corollaries and standards.
  - Corollary
    - Only authorized wireless access points are permitted to be connected to the organizations network.
    - Only authorized systems are permitted to connect to the organization's wireless access points.
    - All wireless access point will be monitored for security related events.
    - All physical sites will be audited on a bi-annual basis for non-compliant wireless access points.
    - All physical sites will be monitored for rogue access points on a monthly basis.

Lets get a bit technical

- SSID - Service Set Identifier - code attached to all packets on a wireless network that identifies each packet as part of the network. Categories:
  - Ad-hoc:
    - IBSS - Independent Basic Service Set Identifier - used by client machines without an access point
  - Infrastructure:
    - BSS ID - Basic Service Set Identifier
    - ESS ID - Extended Service Set Identifier
- MAC: 48-bit Media Access Code: address of the access point
- Channel Number - Changed to minimize wireless interference
- Encryption - WEP (40,128), WPA-PSK,
- SNR - Signal-to-Noise ratio
- Signal - Current RF noise level in dBm

Audit Policies, Corollaries, Standards

- Expected Results
  - Standards
    - All access point configurations tested and certified prior to connected.
    - All authorized access points will be listed in the system of record.
    - Unauthorized access points are detected and removed.
    - SSID: random-generated name 10 characters long
    - SSID: Hidden
    - Encryption WPA-PSK or Enterprise
    - VPN (e.g. Aventail) access only
    - Network Authorization: Radius, AD, etc

Audit Process Controls

- Account Management
  - Expected Results
    - All individuals with access to the AP are current employees (FTE, PTE).
      - Knowledge of how wireless access is granted and removed.
    - Removal of AP access is at time of employee termination.
      - Access to IP address

Audit Process Controls

- Security Event Monitoring
  - Expected Results
    - Events are logged or alerts are sent.
    - Events/Alerts are recorded in the system-of-record
    - Events evaluated and action or no-action documented.
    - Reports are submitted to senior management on a periodic basis.

Audit Process Controls

- Rogue Access Point Monitoring
  - Expected Results
    - Monitoring approach is adequate.
    - Monitoring results are logged.
    - Results are recorded in system-of-record.
    - Results evaluated and action or no-action documented.
    - Reports are submitted to senior management on a periodic basis.

Audit Technology Controls

- Access Point Configuration
  - Expected Results
    - Sample or All APs
    - Certification records exist.
    - Current configuration matches standards (screen prints).
    - Network and resource authorization and architecture configuration matches.
    - Firmware is current.
    - Reports are submitted to senior management on a periodic basis.

The Audit Program - Details

Penetration Testing

The Plan

- Pre-Test Planning
- Tool Selection
- Physical Site Assessment
- External Scanning
- Encryption Attack
- Client Attack
- Internal Scanning

Pre-Planning

- Rules of Engagement
  - Penetration test authorization
    - "Get-Out-Of-Jail" CARD
  - "Windows of Opportunity"
  - Liaison
  - Obvious or Stealth
  - Set the objective(s)
    - Obtain IP address
    - Internal NMAP
    - Map share drives
- # of physical sites
- Location of physical sites
- Number of floors per physical sites

Tool Selection

- Tool Sets
  - Commercial Hardware and Software
    - AirDefense
    - AirMagnet
  - Open Source Scanning Software
    - Insecure.org's short list
      - Kismet
      - NetStumbler
      - Aircrack
      - Airsnort
      - KisMac (for the Mac in all ofus) wireless
      - BackTrack - (collection of tools)
    - coWPAtty
    - Church of Wifi: Uber CoWPatty lookup tables
    - Nmap or nessus

Tool Selection

- Chipsets
  - Herms
  - Prism
  - Atheros
- Cards (x2) - External antenna connector
  - Lucent Technologies ORINOCO Gold Car (the classic)
  - Proxim Silver - ORiNOCO 11b/g
  - USB EDIMAX
- Antenna (x2)
  - Long distance: Yagi Wifi
  - Standard laptop antenna
- Handheld radios

Make your life easy buy card and antenna kit!

External Physical Site

- Locate positions outside the building where intruder can work unobserved. Document them.
- Select the closest unobserved position.
- Scan between the hours of 9am and 11am and 2:00pm and 4:00pm. Why?
- Use long range antenna to identify APs
  - Log all data
- Use short range antenna to identify APs
  - Log all data
- What data are we logging?

First Data Set (long and short range)

- SSID & No SSID & BSSID
- Encryption (None, WEP, WPA)
- Channel
- Type (Managed, Ad-hoc, Probe, Tunnel)
- Packets
- Data Collected
- Document which SSID/BSSIDs were located using long, using short.

Internal Physical Site

- Floor-by-Floor Walkthrough
- Record second data set
- Locate rogue access points (helps to have two people with radios):
  - On physical premises
  - Off physical premises

Discover

- Identify authorized access points with IT
  - Netstumbler
  - AiroPeek
  - Kismet
  - Kismac,
  - Aireplay
- Select targets - only authorized access points are permitted to be targets.
  - Not encrypted
  - WEP
  - WPA
- Begin data gathering against targets

Basic Attacks

- Hidden SSID - De-authenticate Users Attack
  - Raw packet injection kicks the client off the network.
  - Watch for the SSID when the client re-authenticates.
- MAC Address filtering
  - Capture traffic with MAC address.
  - Bump the authorized client-off and use the MAC address.

Basic Attacks

- WEP
  - 40 bit and 104 bit WEP keys (the extra 24 bit is the initialization vector (IV)).
    - Brute-Force: 40 bit keys can be broken in 24 hours, all keys tested based on the number of CPUs (10)
      - jc-wepcrack: Server - Client (part of Airbase)
    - Brute-Force:104 bit keys (tougher)
      - jc-aircrack
    - Statistical Attacks: Vulnerability in the key scheduling algorithm
      - Aircrack: Christophe Devine
      - Airsnort: The Shmoo group

Basic Attacks

- Statistical Attacks: Vulnerability in the key scheduling algorithm
  - Upward of 300,000 to 1,000,000 required
  - Re-inject packets using aireplay in order to capture enough “weak” Initialized Vectors (IV) (24 bit)
  - Or cheat! De-authorize the user, force client re-authorization and increasing the number of IV packets.
  - Then crack using aircrack-ng, jc-aircrack, kismac etc.
- Other Attacks
  - Dictionary Attack
  - ChopChop Attacks

Basic Attacks

- WPA (1-2)
  - 1: RC4 Encryption, 2: AES Encryption
  - Home or Enterprise Mode: Home uses a pre-shared key (PSK), Enterprise uses a RADIUS server for authentication.
  - WPA-PSK
    - Dictionary Attack: coWPAtty and the Church of Wifi Lookup Tables
      - Two ingredients: Capture file with the four-way handshake and the SSID of the target network

Good Karma, Bad Karma

Who have you connected to today?

Wireless

- Loss of Physical Security
- Easy to Deploy
- Cheap to Deploy
- Easy to Configure Incorrectly
- Attacks are Moderate to Difficult to Perform

Audit your wireless today!

Presented by Jefferson Wells

Jeff Camiel

- Director Technology Risk Management
- 408.310.0549
- jeffrey.camiel@jeffersonwells.com

Robert Tillman

- Professional Technology Risk Management
- 408.454.2455
- robert.tillman@jeffersonwells.com