Network Security

Week I: Offense

Scott
Melanie
Enrique
**Topics**

- Wireshark Overview
- WEP & WPA2 Cracking
- Wireless Sniffing
- Man-in-the-Middle
Tools We’ll Use

* All of which come pre-installed on Backtrack:
  * Wireshark
  * Aircrack-ng
  * Kismet
Wireshark
Wireshark Overview

- Popular Network Analyzer
- Runs on Windows, Linux, and OS X
- Captures network data in real-time, allowing for later, offline analysis
- Supports following TCP streams and extracting files from network packets
Wireshark Demo
Wireless Protocols
Wireless Protocols

- WEP (Wired Equivalent Privacy)
  - Ratified in 1999; deprecated in 2004
  - Vulnerabilities: Weak and Repeated IVs
- WPA/WPA2 (Wi-Fi Protected Access)
  - Vulnerability: Pre-Shared Keys (PSKs)
**Four-Way Handshake**

- Intercept all four handshakes
- Repeatedly guess PMK
- Construct PTK using: $\text{Hash(PMK} + \text{Nonces} + \text{MACs})$
- If PTK matches, PMK has been found
Pre-crack Checklist

- Use and boot into Backtrack if at all possible
- Make sure your wireless card is in monitor mode and can inject packets
  - Set your card in monitor mode: `airmon-ng start wlan0 <CHANNEL>`
  - Test injection: `aireplay-ng -9 -e SSID -a BSSID interface`
Wireless Cracking Demo
**Demo Review**

- Airmon-ng to set card into monitor mode
- Airodump-ng to store packets
- Aireplay-ng to de-authenticate clients and get handshake
- Airdecap-ng to decrypt captured packets
- Wireshark to view packet capture
Man-in-the-middle
Rogue Access Points

- The idea is that we masquerade as a wireless access point

- Give user access to the internet

- Steal all the user’s goodies

Process:

- Install and configure DHCP Server

- Use airbase-ng to advertise the AP

- Route traffic through our AP interface to the “real” network

- Sniff the traffic as it flows
Demo

Demo script follows tutorial at http://teh-geek.com/?p=512
Questions?
References

http://www.wireshark.org/about.html

http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy