WLAN Scanning and Auditing Tools

WLAN Hardware Audit Tools

- Typically only a laptop with wireless network adapter is needed
- Using a special tool rather than laptop useful for conducting audits in a remote location with limited access to AC power
- https://shop.hak5.org/products/wifi-pineapple
  - A pentesting and network auditing toolbox
  - Comes loaded with preconfigured attack software such as the Aircrack-ng suite, dsniff, Kismet, Karma, Nmap, and tcpdump, among others

Using Virtual Machines for Wi-Fi Testing

- Virtual machines will generally not use native Wi-Fi adapter for wireless
  - Require a USB adaptor

WLAN Scanning Active vs Passive

- Passive listens for beacons
- Active sends probes
- Most scans are currently passive, but may have an active option
- Tools
  - Netspot
  - Android Wifi Analyzer
  - Kismet
  - Airodump-ng

Wireless Adapter Modes

- **Managed mode** - the wireless card and driver software rely on a local AP in managed mode to provide connectivity to the wireless network
- **Ad-hoc mode** (or Independent Basic Service Set [IBSS] mode -two wireless stations that want to communicate with each other directly can do so by sharing the responsibilities of an AP for a limited subset of wireless LAN services
- **Master mode** - the wireless card provides the services of an AP when paired with the appropriate software
- **Monitor mode** - sniffing the packets in the air without connecting (associating) with any access point or transmitting data. Can sniff the currently configured channel, reporting the contents of any observed packets

Monitor Mode vs. Promiscuous Mode

- Monitor mode – Completely passive and not detectable by a WIDS. Think of it like listening to people's conversations while you walk down the street
- Promiscuous mode - Sniffing the packets after connecting to an access point. Because you connect to the AP, your device is detectable. Think of it like joining a group of people in a conversation, but at the same time being able to hear when someone else speaks.
  - Wireshark example

When Monitor Mode is Needed

- See Wi-Fi management frames
- See all access points
- See Wi-Fi level DoS or spoofing attacks
- Find hidden and Rogue APs
- Attack WEP or WPA

Tools to Set Monitor Mode

- Ability to access monitor mode is HIGHLY dependent on chipset and driver
- Windows
  - Microsoft Network Monitor
  - Wireshark – IF Wi-Fi driver supports it
- Linux
  - Iwconfig commands from command line
  - Airmon-ng check kill
    - To kill interfering services
  - Airmon-ng start wlan0 will start the interface in monitor mode
  - Airodump-ng starts capture in monitor mode

Monitor Mode Tools

- OS X
  - Native, hidden airport tool (Not Airport Utility)
  - System/Library/PrivateFrameworks/Apple802.11framework/Version/Current/Resources/airport/usr/local/bin/airport
  - Airport sniff (channel number) can also support active and passive scanning with –s

Wi-Fi Vulnerability Testing

Monitor Network Traffic

- Use a **protocol analyzer** like Wireshark to monitor traffic on the network
- Detect active scans from nmap, Nessus or other network discovery tool
- Detect deauthentication attacks
- Understand what eavesdroppers can learn from your network
- Capture traffic for offline analysis and cracking

Passive Scanning

- Identify SSIDs and MAC addresses on your network
  - Identify:
    - Rogue access points unauthorized Access Points on your network
    - Evil Twins – rogue APs posing as valid APs
      - Evil twins can be used to decrypt and scan traffic or steal authentication keys
- Inssider or Netspot in Windows
- Kismet or Airmon-ng (part of aircrack-ng) in Linux

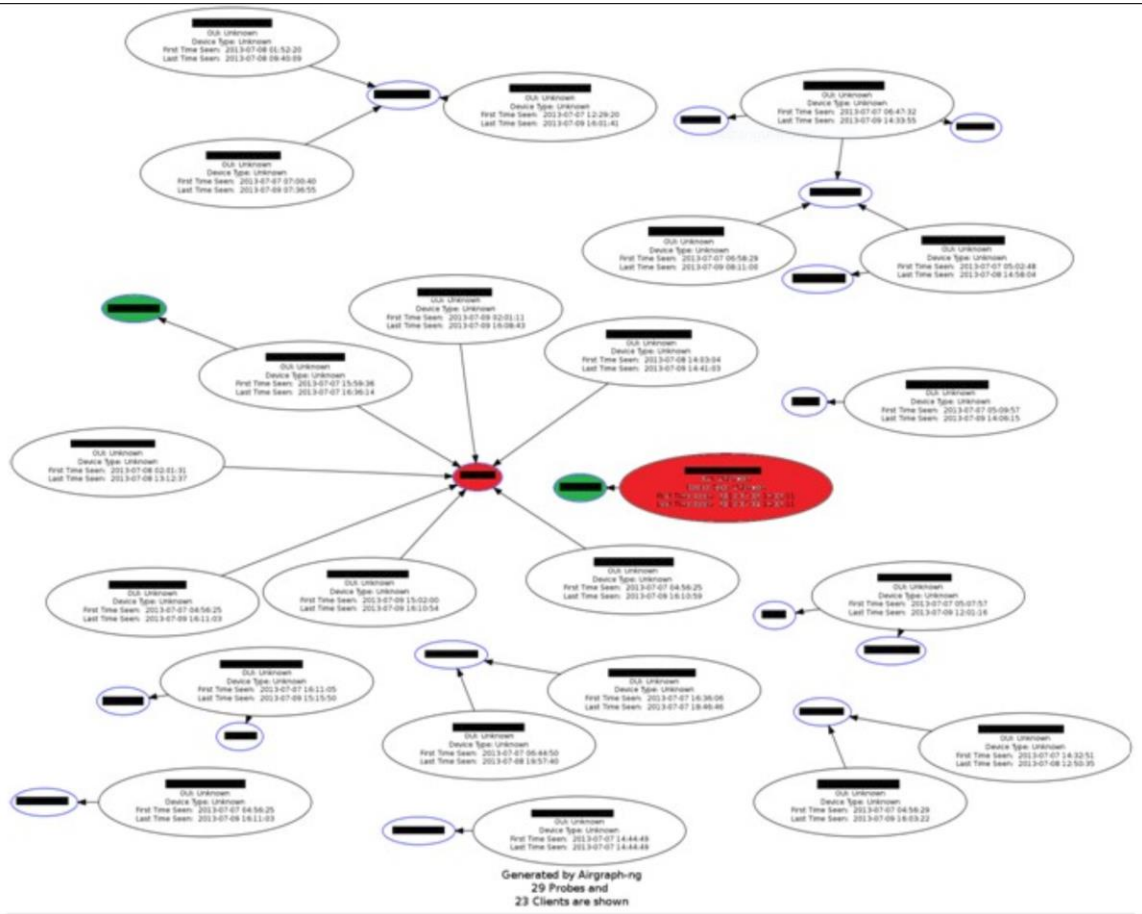
Kismet

- A Wi-Fi scanner that runs on Linux
- Detects and interrogates 802.11a, 802.11b, 802.11g, and 802.11n and 802.11ac networks
- Works as a network sniffer and detector, and possibly as an intrusion detection system (IDS) https://www.kismetwireless.net/docs/readme/alerts/alerts/
- Can determine network IP ranges
- Supports built-in channel hopping
- Can "decloak" SSIDs hidden from network
- Useful for wardriving, site surveys, and detecting rogue APs

Airodump-ng

- Similar to Kismet
- Displays hidden networks
- Used when we want to focus on a single network

Airograph-ng - Uses output from airodump-ng in CSV format



Network Enumerators

- Software programs that scan a network for active hosts; often list IP addresses in a subnet and fingerprint each IP
- **Examples:**
  - Archived MS Network Monitor (https://www.microsoft.com/en-us/download/details.aspx?id=4865)
  - Nmap
  - OpenVAS http://openvas.org/
  - Nessus

Wi-Fi Penetration Testing

Pen Testing From Open WLANs

- Capture traffic and attempt to decrypt
- Setup a rogue AP with advanced software or use WiFi Pineapple

Identify Hidden Access Points

- Use Airodump-ng or Kismet and wait for probe response
- De-authenticate a connected device and watch for probe response
  - Aireplay-ng to specify target
- Brute force the SSID with mkd3

Crack Access Point Administration

- Use Kali hydra utility to conduct password spray attack
  - Provide a list of usernames and a list of passwords
  - Many access points don't limit login attempts

Password Capture and Decryption

- **Tools available in Kali or can be installed on other Linux distros**
- Nessus is good at spotting default administrator passwords for Web applications
- Aircrack-ng can crack WEP, WPA, and WPA2-PSK passwords, perform packet capture and forced deauthentication and reauthentication
- Wifite - All purpose "set it and forget it" scanner and cracker
  - It uses aircrack-ng, pyrit, reaver, tshark tools to perform the audit
  - https://github.com/derv82/wifite2
  - https://tools.kali.org/wireless-attacks/wifite

Password Capture and Decryption

- **Brute-force attacks**
- Cracks the password by comparing all possible combinations of characters for a given password length
- Are generally inefficient against strong, complex passwords
  - Five-character password has 1.934 billion possible combinations
  - Eight-character password has 722,200 billion combinations

Password Capture and Decryption

- **Dictionary-style attacks**
- Each item in word list is encrypted in sequence using the same encryption method as the password; resulting hash code is compared to original password's hash code. If they match, password is revealed
- Dictionary password crackers: Aircrack-ng, Cain & Abel, and John the Ripper

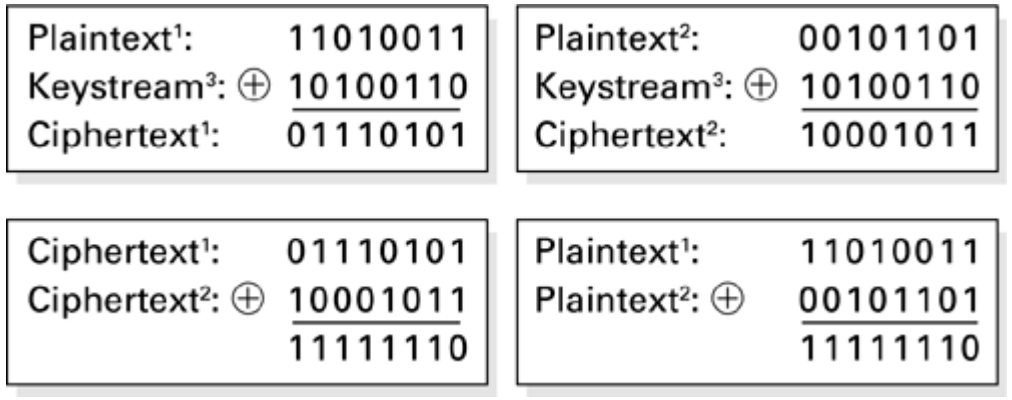
Cracking Passwords Not in Wordlists

- Reaver attack on Wifi Protected Setup WPS
  - Can take hours, but works
- Defense
  - Turn off WPS
- Create custom word lists

Cracking WEP

- Fluhrer, Mantin, and Shamir discovered a flaw in WEP key algorithm (FSM attack)
  - Weak IVs dramatically reduce the number of possible keys
  - Speeds brute force attack
- Duplicate IVs
  - Duplicate IVs plus known plaintext allow detection WEP key
  - Known plain text – can be captured from forcing ARP responses
- Trivial to crack if duplicate IVs available
  - If aircrack-ng crack doesn't work explore –f option to set fudge factor to > 2. Takes longer but continues to brute force.

How the key is found

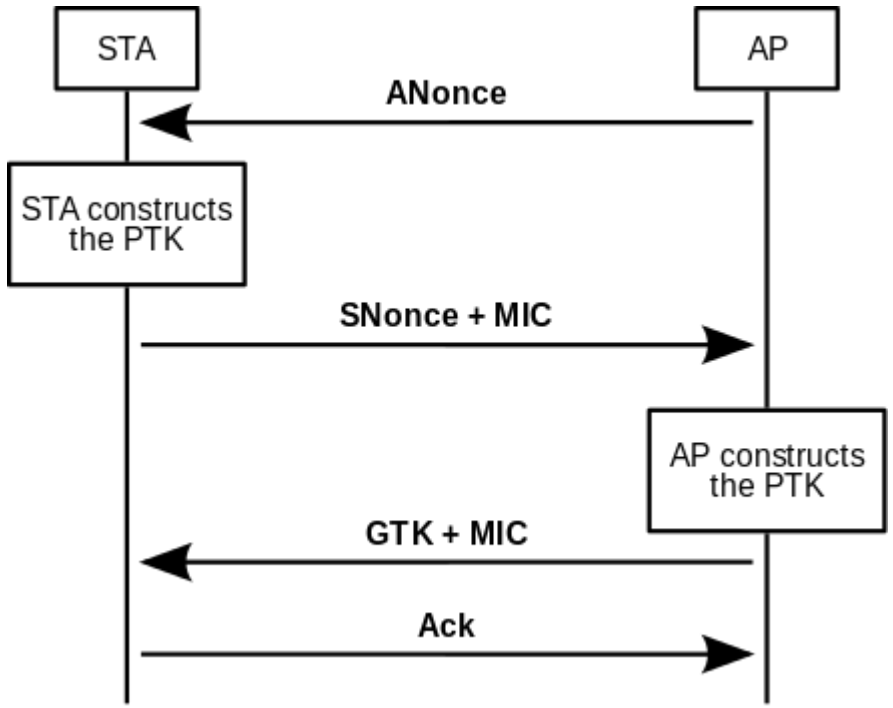


Both Ciphertexts are known

If one plaintext can be discovered from known ARP or DHCP packet with duplicate IV, a second plain text can be derived. From these, the key can be derived

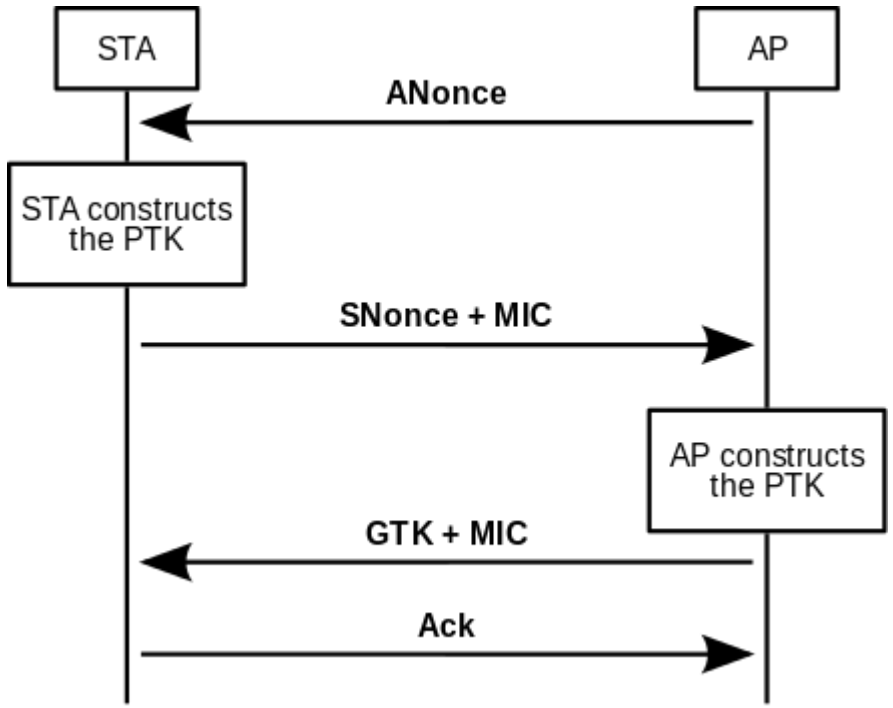
Cracking WPA2-PSK

- Aircrack-ng must be able to associate all 4 steps of the EAPOL handshake.
  - Multiple devices may create multiple authentication requests.



Cracking WPA2-PSK

- Aircrack-ng must be able to associate all 4 steps of the EAPOL handshake.
  - Multiple devices may create multiple authentication requests.



WPA3 and Clientless Cracking

- PMKID attack
  - 802.11r protocol uses PKMID for quick roaming
  - PKMID can be sniffed from first packet in EAPOL handshake
  - PMKID = HMAC-SHA1-128 (PMK, "PMK Name" | MAC_AP | MAC_STA)
  - Packet capture of any authentication attempt will get necessary information
  - Aircrack-ng can perform dictionary attack against packet capture file
  - https://kalitut.com/pmkid-attack/

Evil Twins

- Can be used by attackers or penetration testers
- Mimic legitimate access point
- Run as OSA so clients just connect to strongest signal
  - All unencrypted traffic can be read
- Can use deauth/decypt attack to use real key and decrypt traffic
- Can bypass WPA3 by doing a downgrade attack
  - Deauth and offer downgrade to WPA2-PSK
  - Capture first two steps of 4-way handshake and attempt dictionary attack against the pre-shared key

Evil Twins- continued

- Steal passwords through fake active portal
  - Can steal WPA2-Enterprise credentials
  - Can request PSK for WPA3

Evil Twin Tools

- EAPHammer is a toolkit for performing targeted evil twin attacks against WPA2-Enterprise networks.
  - https://github.com/s0lst1c3/eaphammer
  - Advantage is a simple command line that continues the attack
- WiFi Pineapple

Locating Access Points

- Android WiFi Analyzer is simple tool to view signal strength when searching within building
- GPS location of Access Points found in a log, capture file or active probe can be done at https://www.wigle.net/

Mitigate Threat of WiFi Password Cracking

- Turn off Wifi Protected Setup (WPS)
- Creating strong (non-dictionary) passwords and pre-shared keys
- Turn off PMKID by disabling 802.11r on access point or move to WPA2-Enterprise
- Mitigate Evil Twin attacks by monitoring network and alerting if new AP appears
  - kismet alerts tab
  - In main menu data sources select channel and select lock to capture all traffic