Vulnerability of Wireless Home Networks
Hacking into WPA

**Purpose of Project**
- Understand the Vulnerability of Wireless Home Network
- Understand the wireless security mechanism
- Gain access to a WPA protected wireless network using hacking tools

**Background**
Wireless home networks are a growing trend in today's world. 802.11 a/b/g/n has been used to build the wireless home networks.

How Secure is the Wireless Network? Keep in mind...
- No Wireless traffic can be channeled to a particular device, must be broadcasted over the air on frequencies
- The attacker can pick up traffic containing the key

These networks are protected under different security mechanisms.
- Open Authentication
- WEP: Wireless Equivalent Privacy.
- WPA/WPA2: Wi-fi Protected Access.
- 802.1x: Radius Server

**How Does WPA - PSK Work?**

**How Does the Aircrack Tool Work?**

Through a combination of tools retrieve the correct passphrase

**Airmong-ng**
- Enables the Promiscuous mode on wireless interfaces to enable the monitoring mode on a virtual Interface

**Airodump-ng**
- Jumps across channels, unless specified, and captures packets. Listing information
  - First use: Airodump-ng
    - This will allow you to scan for all networks and access points
  - Second Use:
    - Capture on the specified channel, all traffic for the specified Access Point using the interface

**Aireplay-ng:**
- Inject packet onto network in order to generate desired authentication traffic. Broadcasted as the target BSSID, devices start generating the authentication packets and commence the handshake.

**Aircrack-ng**
- Opens the Captured handshake, and uses a dictionary attack to attempt to find passphrase

**Conclusions**
- Wireless Home Networks are not secure.
- Aircrack tools can capture the authentication requests and use a dictionary attack to find the passphrase.

To improve the security of the Home network one should
- Limit the Mac Addresses Permitted
- Use a Security Method (WPA+)
- Use Complex Passphrases
- Use uncommon words