**Evil Twin Attack**

Main purpose of the attack

Get access to victim's PC remotely.

Methodology

1. Victim is connecting to legitimate AP.
2. Attacker scans the air for the target AP information (SSID name, Channel number, MAC Address).
3. Attacker uses that information to create a fake access point with the same characteristics, and for de-authentication of clients from legitimate AP.
4. Clients on the legitimate AP are repeatedly disconnected, forcing them to connect to the fake AP.
5. As soon as the client is connected to the fake access point, S/he may start browsing the Internet.
6. Client opens up a browser window and sees a web administrator warning saying "To continue browsing you must download the latest version of WIFI driver".
7. Victim downloads the WIFI driver.
8. Victim's background has changed to "HACKED".
9. Hacking accomplished.

Prerequisites

Below is the following list of hardware and software used.

**Hardware used:**

1. Alfa AWUS036NH wireless adapter.
2. tp-link TL-WN722N USB adapter.
3. Victim's Laptop.
4. Attacker's Laptop.

**Software Used:**

1. Oracle VM VirtualBox.
2. Kali Linux VM installed on Attacker's Laptop.
3. Airmon-ng – change wireless adapter mode to monitor.
4. airodump-ng – Wireless adapter (ALFA) scans APs information.
5. aireplay-ng – deauthentication from legitimate AP.
6. hostapd – Createing Fake AP.
7. DNSmasq - configure apache and the dhcp server so that the access point will allocate the IP address to the victim and the client would be able to access our site remotely.
8. Apache – Server for our fake Intel site for downloading WIFI driver.
9. Iptables – configuring and routing IP.

Problems we were faced with

1. Choosing the best working environment to do the project on.
2. Get knowing the hardware, and how to integrate it with the script.
3. combine Apache web server, and integrate it with the software.

Strengths

* The executable was responsible only to changing background of victim's PC, but actually attacker could write **any program** he wants e.g. virus.
* The project was tested under private network with known password, although attack will be worked on every public network also (appropriate hardware is needed).
* The attacker can decide if the victim can have access to the internet or not.
* The victim can't know AP is changed to fake AP (only if he does active action and check the IP of the WIFI and recognize that the IP is not the same as his legitimate AP IP).

Weaknesses

* The project was tested under 2.4Ghz wireless frequency only (5Ghz wireless frequency not tested).
* The project combines additional hardware, and the attack depends on this hardware.