CS 3433 - Principles of Computer and Information Security

Assignment 6 : WEP Insecurities

Due Friday, November 22nd 2021, before the start of class (3:00pm)

This assignment is designed to investigate the insecurities of WEP encryption and other issues in wireless networks. In the security lab there are 12 access points (including arrakis), 5 APs are Raspeberry Pi Zero Ws running a custom compiled version of OpenWRT 19.07.4 and 7 APs are Buffalo Air Station G54 running OpenWRT 10.03.1 (Backfire). The SSIDs of the access points are all planets from the Dune series of books. The characteristics of the 12 systems are:

1. Eight of the access points use WEP encryption with non-passphrase generated 128 bit keys and open authentication.

2. Four of the access points use WPA-PSK (WPA2/AES) encryption. One of these is a word (without any modifications) randomly chosen from the dictionary used in assignment 3, another is two concatenated words randomly chosen from the same dictionary. The remaining two systems use a word randomly chosen from the dictionary with character replacement. The character replacements used are:

   ```
   a <- @
   e <- 3
   i <- !
   l <- |
   o <- 0
   ```

   All characters that can be replaced in a the word are replaced.

3. Every access point uses a different channel.

4. Five of the access points have a hidden (non-broadcasting) SSID.

5. Three of the access points may appear to have a non standard SSID. Try looking at the different SSIDs on kismet and airodump-ng. If you walk by the lab in person sometime, check out the wireless networks on your phone, Windows, or Mac.

6. Three of the access points have frequent connections and data packets being transfered.

7. Six of the access points have periodic connections and data packets transferred but are not as frequent.

8. Two of the access points have occasional connections and data packets but are significantly less frequent.

9. One of the access points have very infrequent connections and data packets.

10. One of the access points has MAC filtering enabled.

11. One of the access points has a static arp table and will not automatically generate arp packets, but does not have arp completely disabled

12. One of the access points stays constantly connected to the client(s)

Additionally:

- There will be two or three systems that may give some confusion.
- There is a system which I will use as a demo in class on which you can practice. The SSID will be arrakis which is one of the three access points mentioned above with frequent connections and data packets.
- I highly recommend passing the `-x nbpps` option to `aireplay-ng`. If the access points receive too many packets then they may temporarily stop functioning correctly.
- Do **NOT** perform any type of DoS attack that will affect other students negatively.
- If you want to disassociate a connection, do **NOT** send more than 3 or 4 disassociate packets and do **NOT!!!** run an infinite loop!

The basic assignment is simple, install the `aircrack-ng` package and any other packages that you want to use and determine the following information for each of the systems, to be turned in to the class portal with all fields separated by **commas**:

```
abc123,Full Name
SSID,Hidden,BSSID,Channel,Crypt,Key,Client MAC,Attack mode
```

- Your abc123 and name should be on the first line separated by a :
- When specifying the SSID (ESSID) use the exact **ascii SSID/Name displayed by kismet** including spaces (this may not be the actual SSID).
- Hidden should be one of `true` or `false`.
- ALL BSSID and MAC addresses should be exactly 12 hex characters and 5 `:` characters
- Include all `:` characters in the BSSID and MAC addresses.
- Channel should be a numeric value.
- Crypt be one of `WEP` or `WPA`.
- Please use the **numeric (hex)** (non-ascii) key for WEP systems.
- Client MAC address is the MAC address you used for this SSID when gathering and generating data. If you used more than one MAC choose the one that is most appropriate.
- Attack mode should be one of the non-numerical attack modes displayed by `aireplay-ng --help`. Attack mode is not automatically checked in any way but will be an indirect factor in your final grade as you are required to be able to demonstrate different attacks. Choose the primary attack method that was used to gather data.
- Order rows by channel.

- You should have a maximum of 13 rows, 1 row with your name and abc123, and 1 line for each AP.
- Each row, except for the first, should have exactly 7 commas and 8 fields (columns).
- Make sure and format the file exactly as specified even if automatic scoring is not enabled.
- Check your work carefully, typos and incorrect capitalization will be counted as an incorrect answer.
- Partial credit may be given at my discretion if the flag is partially correct.
- There will be **NO** late submissions allowed as always.
- If you receive an automatic score for this it is not your grade. Your grade will be given by me during a final interview.
- Additional submission instructions may be posted in the Discord announcements for this assignment.

An example submission would look like (with completely made up data):

```
abc123,Keith Harrison
mars,false,66:8f:fa:c3:0b:55,1,WEP,5a765f7739352435384d6c3333,92:ac:4b:4f:92:61,arpreplay
venus,true,36:e6:56:1e:00:12,6,WEP,276b304f6f4b795f28614e6c2f,1a:aa:6a:11:b3:dc,chopchop
jupiter,false,52:7e:3c:57:ce:87,11,WPA,europa,ee:a5:8a:f4:f6:1a,none
```

I want you to collect sufficient IVs/packets/handshakes for each system (for which it makes sense) so that you can crack the key/passphrase. You must have collected these IVs/packets yourself. You may not get them from others although you may collect them by simply sniffing the wireless traffic unless otherwise specified. However you get more points if you created the traffic yourself.

All information that you can discover about the system including a remote exploit of the system is welcome however you may not make use of physical access to the system nor may you do DoS or any other operation which will interfere with others performing this assignment.

On the due date we will schedule an interview for you to demonstrate successful attacks on different access points of my choosing, different attack methods, different challenges you encountered, and anything related to the assignment.

Keep a log of your activities and commands that you ran so that you can discuss the challenges associated with each AP and what actions you took in order to successfully compromise them. Be prepared to demonstrate breaking into any access point, along with all of the following items:

- Different types of attacks against WEP including but not limited to arp replay, and chopchop.
- Different methods of recovering WEP keys including the FMS/KoreK method, and the PTW method.
- Capturing the WPA2 authentication handshake, and cracking with `aircrack-ng`, `john`, or `hashcat`.

- How you overcame additional obstacles such as MAC filtering, hidden or non standard SSIDs, and lack of connections, arp packets, or data packets.

Troubleshooting:

1. If `kismet` stops capture traffic after a a few minutes, then NetworkManager or `wpa_supplicant` are likely causing problems.

2. If you are not seeing any data packets, something is wrong. If you have the older single-antenna `ath5k` wireless card, make sure that you are running the older kernel. You can check your currently running kernel with the `uname` command:

   ```
   uname -a
   ```

3. I do not recommend trying to run `kismet` at the same time you are trying to use aircrack.

4. I personally do not use `airmon-ng`, it can be useful and maybe even necessary at times but I feel like it can also cause problems. `airodump-ng` can and will put your card into monitor mode for you without using `airmon-ng`. Try with and without using `airmon-ng`.

5. The commands I list below help me when troubleshooting, but you will definitely need to adjust them for your specific interface name(s) and use case.

6. Delete all of your wireless interfaces add a new interface:

   ```
   iw dev wlan0 del
   iw dev mon0 del
   iw phy phy0 interface add wlan0 type station
   ip link set dev wlan0 up
   ```

7. The following commands delete the interface addresses, disconnect, and bring the interface down, switch to managed mode, and then back up:

   ```
   ip addr flush dev wlan0
   iw dev wlan0 disconnect
   ip link set dev wlan0 down
   iw dev wlan0 set type managed
   ip link set dev wlan0 up
   ```

8. Or, if you prefer to use ifconfig/iwconfig you can bring the interface down, switch to managed mode, and then back up:

   ```
   ifconfig wlan0 down
   iwconfig wlan0 mode managed
   ifconfig wlan0 up
   ```

9. Connecting to a WEP access point and setting an IP address:

```
iw dev wlan0 connect -w arrakis key 0:522127207c27264e347d542f27
ip addr add 192.168.1.101/24 dev wlan0
ip addr show dev wlan0
```

10. Connecting to a WPA access point

```
wpa_passphrase ssid passphrase > ssid.conf
wpa_supplicant -B -i wlan0 -c ssid.conf -D nl80211
```