Computer Science Department
University of Crete

CS-455: Internet Attacks
Spring 2022 – 2023

Assignment 2
Wireless Attacks

Uploaded: 25/02/23
Deadline: 15/03/23, 23:59

Introduction

In this assignment you will experiment with Wi-Fi vulnerabilities, attacks, and countermeasures. Further to our discussion in class, you will exploit Wi-Fi misconfigurations to gain access to the network and elaborate on how to prevent certain attacks.

Notes:

- In this assignment you are required to use Kali Linux to perform the attacks.
- For every question, you need to provide all the necessary commands used with adequate explanation of the command and the relevant result/output.
- You should focus on packets related to the HY455 network. Ignore the rest of the traffic captured.
- Useful tools: airmong-ng, airodump-ng, ipconfig, iwconfig.

Questions

1. [5%] **Pawning SSID**:
    - One of the security mechanisms used by Wi-Fi networks is to hide their names, since a client device can only connect to a Wi-Fi network with a known SSID. However, this is an obsolete security mechanism as there are several ways to find out a hidden network's SSID.

- Demonstrate the attack (i.e., retrieving a hidden SSID). Explain the commands used and the results.
- Discuss countermeasures for this attack.

2. [10%] **MAC spoofing**:
   - List reasons why MAC spoofing is possible.
   - Discuss ways to spoof a MAC and a countermeasure for each one of these ways.
   - Demonstrate ways to spoof a MAC and relevant countermeasures.
   - Demonstrate how to bypass MAC filtering enforced by an access point and relevant countermeasures.

3. [5%] **Scanning for wireless networks**:
   - Provide the necessary commands to list all the available networks in the area. Explain the commands used and the results. If you do not have access to an antenna refer to Figure 1.
   - Provide the necessary commands to list all the connected devices with the network HY455. Explain the commands used and the results. If you do not have access to an antenna refer to Figure 2.

4. [25%] **Attacking WEP**:
   - Provide the necessary commands to capture all the traffic of the **HY455-wep** access point. Explain the commands that you used and the results.
   - Demonstrate the attack. Use the pcap file provided (**HY455_wep.cap**) to find the network's password based on known WEP vulnerabilities. Explain the commands used and the results (e.g., password found).
   - Briefly discuss WEP vulnerabilities as well as countermeasures suggested in the past.

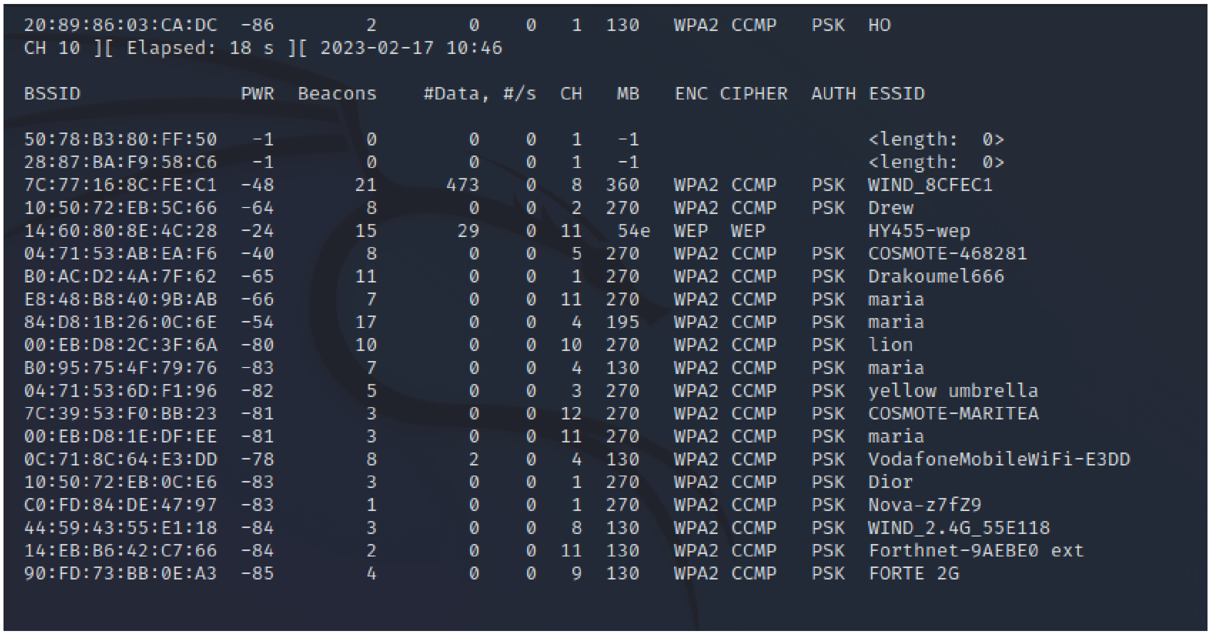
5. [30%] **Attacking WPA**:
   - Explain the commands used to disconnect a device from the access point to later capture a handshake. Discuss de-authentication countermeasures.
   - Explain the commands used to capture the handshake between a Wi-Fi client and the access points named **HY455_wpa.cap**. Note: to be able to capture the handshake, the client must connect to the access point after you start capturing traffic.
   - Use the **rockyou.txt** wordlist and the captured handshake to find the access point's password. Explain the commands used and their output. See https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt

- Discuss countermeasures for this type of attack (including WPA3).

6. [25%] **Attacking WPS**:
    - List the requirements for this type of attack to work. Explain the commands that should be used to perform this type of attack.
    - Discuss countermeasures for this type of attack.

7. [BONUS 5%] **Café Latte attack**:
    - The so-called 'Cafe Latte' attack aims to retrieve the WEP keys from the laptops of road warriors. The approach concentrates its attack on wireless clients, as opposed to other attacks that crack the key on wireless networks after sniffing a sufficient amount of traffic on a network.
    - Demonstrate the attack.
    - Discuss countermeasures for this type of attack.

Figure 1: List of nearby networks

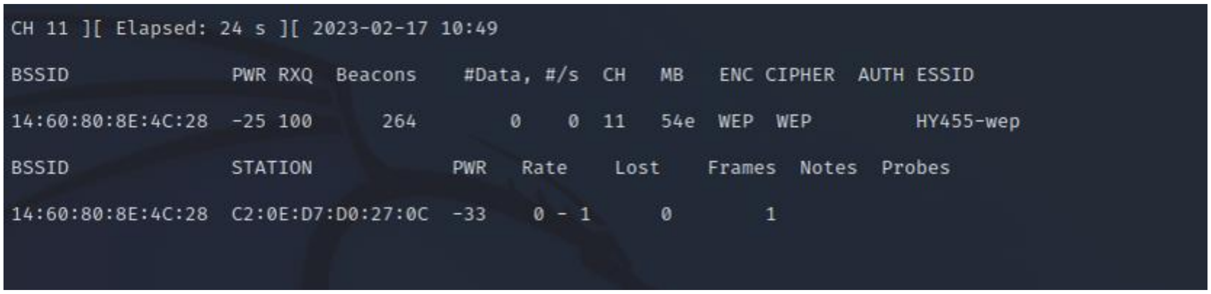


```
20:89:86:03:CA:DC  -86        2        0    0   1  130   WPA2 CCMP   PSK  HO
CH 10 ][ Elapsed: 18 s ][ 2023-02-17 10:46

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

50:78:B3:80:FF:50   -1        0        0    0   1   -1                    <length:  0>
28:87:BA:F9:58:C6   -1        0        0    0   1   -1                    <length:  0>
7C:77:16:8C:FE:C1  -48       21      473    0   8  360   WPA2 CCMP   PSK  WIND_8CFEC1
10:50:72:EB:5C:66  -64        8        0    0   2  270   WPA2 CCMP   PSK  Drew
14:60:80:8E:4C:28  -24       15       29    0  11   54e  WEP  WEP         HY455-wep
04:71:53:AB:EA:F6  -40        8        0    0   5  270   WPA2 CCMP   PSK  COSMOTE-468281
B0:AC:D2:4A:7F:62  -65       11        0    0   1  270   WPA2 CCMP   PSK  Drakoumel666
E8:48:B8:40:9B:AB  -66        7        0    0  11  270   WPA2 CCMP   PSK  maria
84:D8:1B:26:0C:6E  -54       17        0    0   4  195   WPA2 CCMP   PSK  maria
00:EB:D8:2C:3F:6A  -80       10        0    0  10  270   WPA2 CCMP   PSK  lion
B0:95:75:4F:79:76  -83        7        0    0   4  130   WPA2 CCMP   PSK  maria
04:71:53:6D:F1:96  -82        5        0    0   3  270   WPA2 CCMP   PSK  yellow umbrella
7C:39:53:F0:BB:23  -81        3        0    0  12  270   WPA2 CCMP   PSK  COSMOTE-MARITEA
00:EB:D8:1E:DF:EE  -81        3        0    0  11  270   WPA2 CCMP   PSK  maria
0C:71:8C:64:E3:DD  -78        8        2    0   4  130   WPA2 CCMP   PSK  VodafoneMobileWiFi-E3DD
10:50:72:EB:0C:E6  -83        3        0    0   1  270   WPA2 CCMP   PSK  Dior
C0:FD:84:DE:47:97  -83        1        0    0   1  270   WPA2 CCMP   PSK  Nova-z7fZ9
44:59:43:55:E1:18  -84        3        0    0   8  130   WPA2 CCMP   PSK  WIND_2.4G_55E118
14:EB:B6:42:C7:66  -84        2        0    0  11  130   WPA2 CCMP   PSK  Forthnet-9AEBE0 ext
90:FD:73:BB:0E:A3  -85        4        0    0   9  130   WPA2 CCMP   PSK  FORTE 2G
```

Figure 2: List of connected devices in the network HY455-wep



```
CH 11 ][ Elapsed: 24 s ][ 2023-02-17 10:49

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

14:60:80:8E:4C:28  -25 100      264        0    0  11   54e  WEP  WEP         HY455-wep

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

14:60:80:8E:4C:28  C2:0E:D7:D0:27:0C  -33    0 - 1      0        1
```

Submission

- Submit a pdf document including all the information requested above.
- Submissions will be done through eLearn.
- This assignment is an individual creative process and students must submit their own work. You are not allowed, under any circumstances, to copy another person's work. You must also ensure that your work won't be accessible to others.
- You are encouraged to post any questions you may have in the eLearn forum. If however you believe that your question contains part of the solution or spoilers for the other students you can communicate directly with the course staff at hy455@csd.uoc.gr.

Disclaimer

It is **ILLEGAL** to attempt any type of attack against a target (individual, network, public/private entity, etc.) without authorization / explicit permission. Such actions are **prohibited and punished by law and university policies**.