|  |  |
| --- | --- |
| Course | Wireless Network Security |
| Lab | Lab 6- WEP Cracking |
| Student ID | 100899259 |
| Student Name | Maisha Khatoon |

# LAB: 06

WEP Cracking

**Objective:**

WEP stands for Wired Equivalent Privacy, which is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.

WEP Uses RC4 stream cipher and 64-or 128-bit keys. Static master key must be manually entered into each device.

WEP was introduced in 1999. Within a few years, several security researchers discovered flaws in its design. The “24 additional bits of system-generated data” mentioned above is technically known as the Initialization Vector and proved to be the most critical protocol flaw. With simple and readily available tools, a hacker can determine the WEP key and use it to break into an active Wi-Fi network within a matter of minutes.

Vendor-specific enhancements to WEP like WEP+ and Dynamic WEP were implemented in attempts to patch some of the shortcomings of WEP, but these technologies are also not viable today.

In this lab students will explore ways to perform wireless attacks and understand potential defenses. The attacks that will be covered are inspecting and modifying wireless card parameters, changing the wireless transmission channel, flooding attacks, and cracking keys of WEP protected networks.

**Activities:**

Download and install Kali Linux

Configure ALFA network WiFi USB adapter

Configure WiFi AP

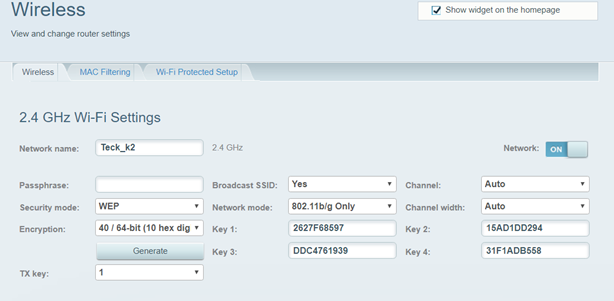
**Leaning Activities:**

At the end of these activities, you should understand:

* Information Gathering
* Traffic Collection
* How to the analysis WEP traffic
* Joining the Wireless Network

**Task-1**

**Wifi router setting and configure it to WEP**

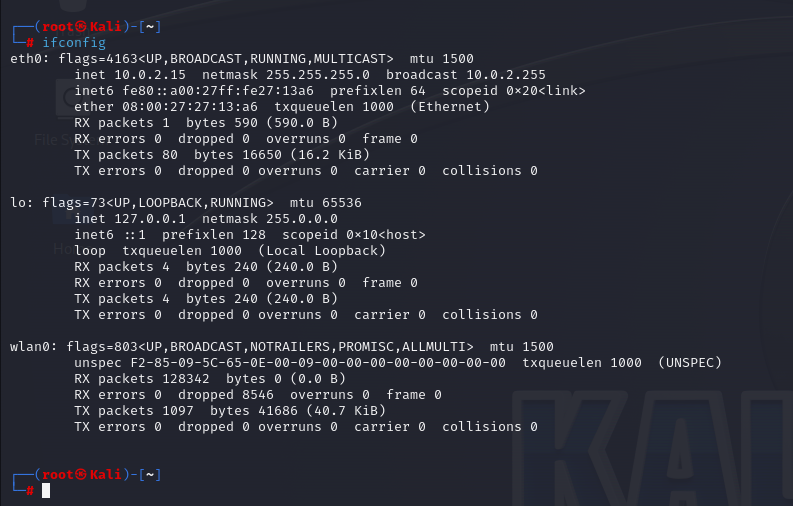


**NOTE: New WiFi router will not support WEP.**

There you will see two options one to create encryption keys with 40 / 64-bit (10 hex digits) and one with 104 / 128-bit (26 hex digits) this is the security feature which they added before WPA was formally adopted in 2003. This option is not available in many routers because WEP is obsolete.

**Task-2**

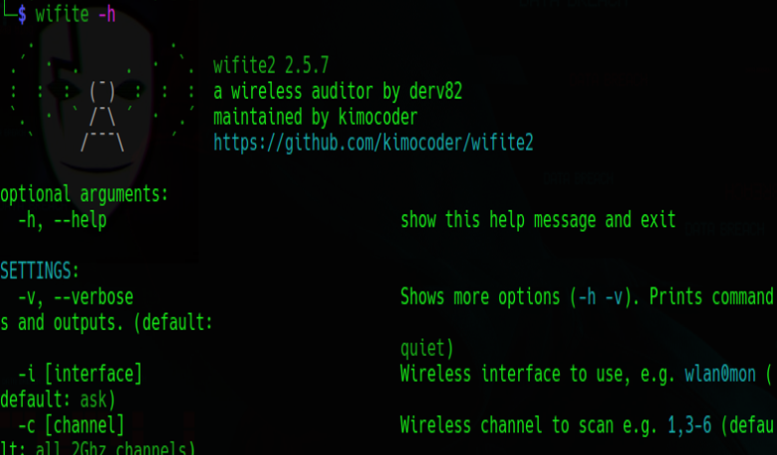
Make sure your Alfa card is working before Task -3 (screenshot)



**Task-3**

* 1. Using Wifite, which will automate a lot of stuff for us, using airodump-ng, aireplay-ng and aircrack-ng in the background and will give us our desired result.

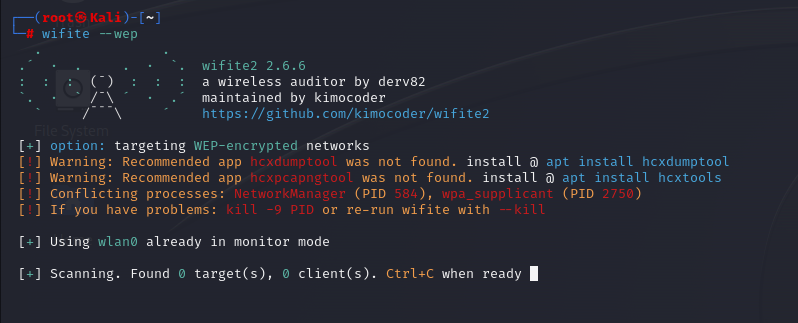
To get help, type the following command:



* 1. What is the command to list ONLY WEP encrypted networks? (screenshot)

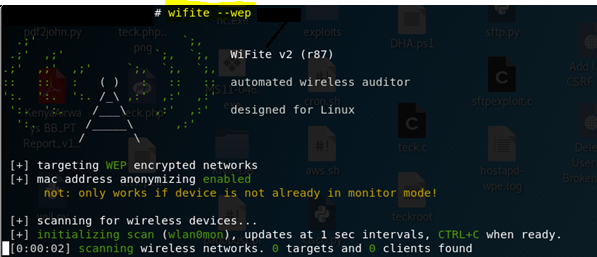
wifite –wep

since there are no WEP-encrypted networks my router could not find them.



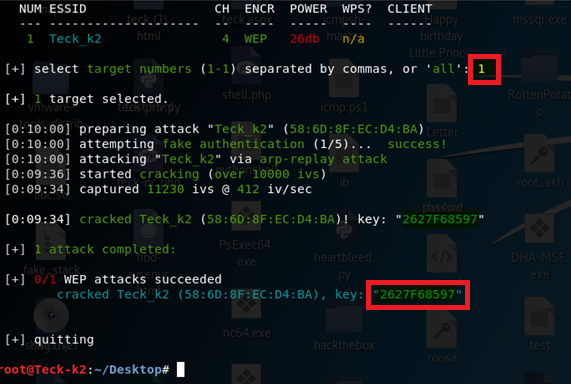
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3.3 Type the following command:



Now as we start this tool with –wep which we used to search only WEP enables devices and –mac to randomize our Wlan mac.( -mac optinal)

You may see the following screenshot:



As soon you see your target SSID press ctrl+c and it will ask you for option which target you want to select and attack based on the number, and then it will start attacking the target by first capturing the handshake and once the handshake is done, it will start the cracking the password, as you all know WEP algorithm is not that secure, it cracked the Key within 40-Sec. In the above example the Key is **2627F68597**.