Exploiting vulnerabilities in WLAN

1. Abstract

In the present period, the likelihood of the remote gadgets getting hacked due to certain WLAN weaknesses, the lack of user awareness and weaker security framework invites the hacker to break down into the system. the research(Pimple et al., 2020a) about WLAN highlights that lots of wireless routers are configured using weaker encryption algorithms such as WEP and WPA2, which can be easily exploited by the assault using aircrack-ng, airodump-ng utility and that program is already available in the operating system such as Kali Linux .and if the wireless network attacked by those tools it is harder to detect that your network is being compromised by the attacker

2. Introduction

The flexibility, effectiveness and(Tahar Mekhaznia, 2015) low cost of wireless network accepted by most of the Organization. In the contrast, wireless networks have many constraints regarding traditional networks such as reduced storage data and low-power consumption. And it also broadcast the radio waves which invites the hacker to capture the traffic using eavesdropping technique.it is although essential to keep the data transmitted through network nodes permanently encrypted to avoid unauthorized access to its content. In Wireless networks, hence, WEP, WPA and WPA2 protocols designed for protecting communications by providing encryption mechanism. However, security solutions intended for such networks become insufficient against attacks on secret keys.

This research paper explores various dimension about the wireless security-related flaws, and primarily focus on WEP, WPA2, MAC Authentication Flaws, which is still widely used by most of the organization. And these paper also proves that encryption implemented in most of the organization still pose threat for organization and invite hacker to take the control of their network by decrypting the secret key using FMS attack [which is based on the Initialization vector (IV) weakness present in WEP algorithm

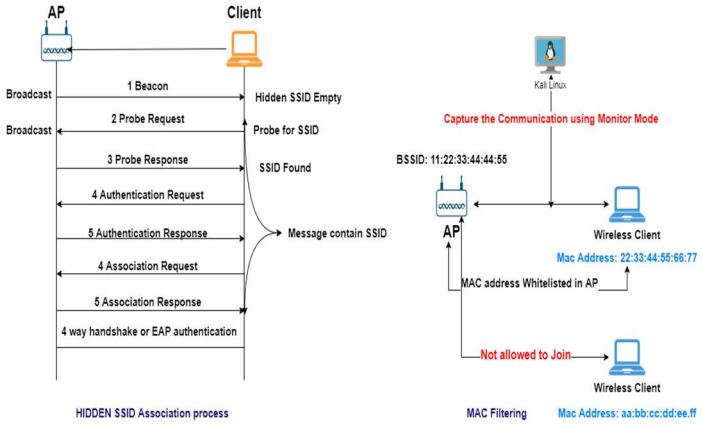
3. Technical flaws - Research how to bypass WLAN authentication if SSID is hidden and if administrators use MAC filtering

The most of the router(Akram, Saeed and Daud, 2018) has the inbuilt MAC filtering utility which allows the only legitimate user to connect to the access point if the mac address whitelisted under mac filtering utility. any authorized mac address which is not whitelisted in the Access point is not allowed to join the network

The Administrator of the wireless(Kumar Gupta, Kumar and Zeeshan, n.d.) device gives the common name to SSID according to their business requirements such as department name or a company name and since the SSID is human-readable format observer may recognize the network which they would like to connect, thus it invites the hacker to penetrate the wireless network. because SSID is broadcasting over the air, hence the administrator uses hidden SSID feature which is built-in most of the router to prevent the sensitive information broadcasting and make them vulnerable to unwanted attention

Graphical Explanation for(Kumar Gupta, Kumar and Zeeshan, n.d.)

Fig-1 **Hidden SSID Association** and **Mac filtering**



Hidden SSID Flaws

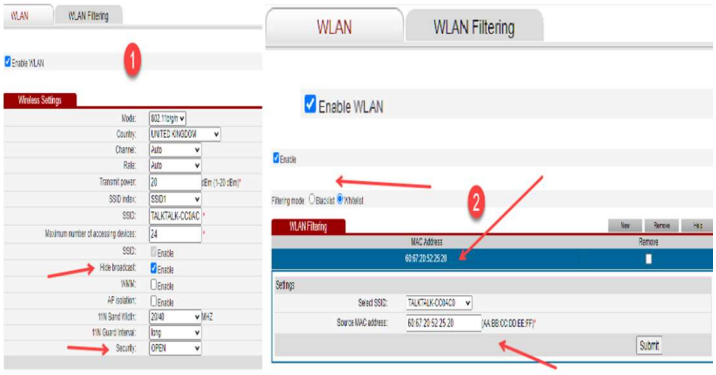
According to the graphical explanation for **Hidden SSID association process** , the AP send the **Beacon frame** to client and that frame contain the SSID which is chosen by the network operator. the wireless client sends the **probe request** to check the AP availability. Then AP generate **probe response** back to client and verify the SSID which is entered by the client. after the probe response **authentication packet** sent from client to AP for Association and if AP verify the encryption algorithm then AP send **Association frame** to client, until now the process not reveal the SSID over the air but if the hacker send the De-authentication packet to Client then client machine will re-initiate the connection to AP and hacker will able to find Hidden SSID in clear text format using **airodump-ng** Utility with Monitor mode functionalities

MAC Filtering Flaws

The **media Access Control** [MAC] uniquely assign the(Alsahlany, Alfatlawy and Almusawy, n.d.) 48-bit hexadecimal number to each unique network equipment , The mac filtering utility provides the security mechanism which is used by the IEEE 802.11 to ensure the protection of WLAN. in these mechanism AP whitelist the Authorised MAC address and whenever AP receive Association request from the whitelisted mac address it accept it and allow the connection to established however in these process hacker easily identify the whitelisted mac address using Airodump-ng and clone the 48 bit mac address using mac changer utility and re-initiate the connection from Kali Linux machine

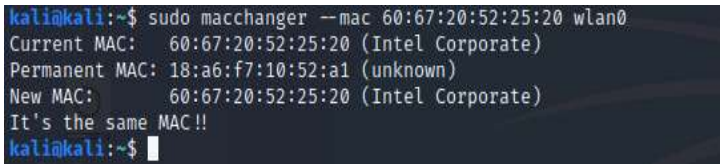
Practical Demonstration for Hidden SSID and Mac Filtering Flaws

1 Configure the Router so only allowed Mac address can connect to Access Point and turn on the checkbox to hide SSID

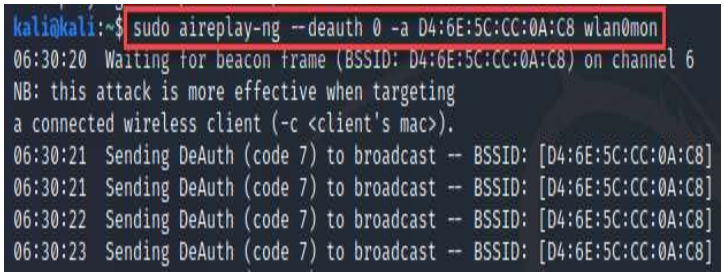


2 Find the Hidden SSID network and whitelisted mac address using **airodump-ng** utility

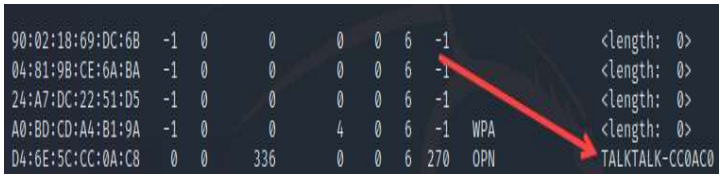
3 Change the mac address of **wlan0** using **macchanger** utility in kali Linux machine



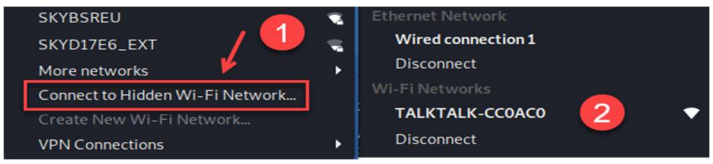
4 To reveal the Hidden SSID execute **airodump-ng -c 6 wlan0mon** and keep running it and in the new tab send de-auth packet to client to re-initiate the current connection



5 After the de-authentication **Airodump-ng** utility will show the SSID

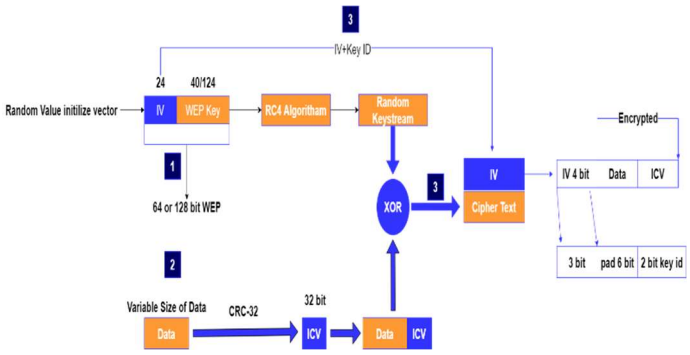


6 Now connect to an Access point using kali Linux machine



4. Technical flaws - Research WLAN encryption flaws (WEP, WPA2)

Fig-2 Graphical Explanation for the WEP Encryption and its Flaws



How the WEP Works

The WEP is the first encryption scheme made available for Wi-Fi and it use the RC4 Encryption algorithm which is one kind of symmetric key encryption ,these means that transmitter and receiver have identical wep key ,which transmitter use to encrypt and receiver used to decrypt

Step1: According to graphical Explanation step 1 ,The 24 bits Initialization vector [random value] plus 124 wep key make the 128bit encryption and using RC4 Algorithm it generates the random keystream

Step2: process the Variable size of data using Cyclic Redundancy Check and generate the 32 bits integrity check value [ICV] then afterwards it concatenates the data and ICV into Block

Step3 the Mathematical calculation using XOR algorithms between random keystream and Data and ICV create the Ciphertext value as in these process the client does not know the IV which is generated by Access points ,hence the IV appended to Ciphertext

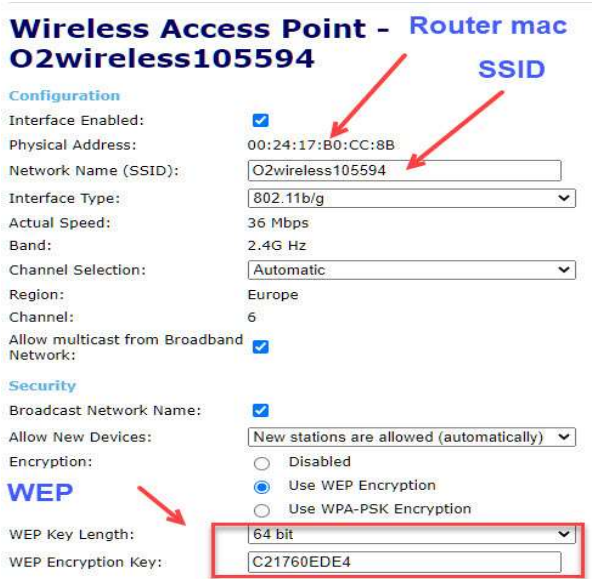
WEP Encryption Vulnerabilities

WEP features introduced in 1997 as a part of 802.11 standards to protect wireless communication by using RC4 Encryption algorithm. The WEP encryption model was started with 64 bits key and later it evolved up to 256 bits key, however it still not prevents prevent forgery of packets. It does not protect against replay strikes, and the attacker (Martin, Mohammed and Ramadhin, 2019)can get into an Access Point without getting the encryption key due to the reuse of initialization vectors. Due to the poor implementation of the RC4 encryption hacker can capture initialization vector over the air and able to reveal the cleartext key using tool like **Aircrack-ng** and **Airodump-ng**

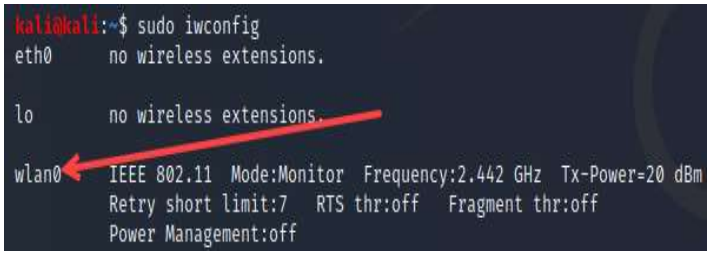
The WEP use only one secret Key(Muhammad Aleem Raza1, 2020), and even the size of the Key is limited to 40 bits or 128 bits which can easily cracked by the hacker by capturing the IV using monitor mode

Intention behind IV in RC4 is to generate the unique combination but the size of 24 bit of IV i adequately produce only (Garg, 2016)16,777,216 combination of the key so if 54Mbps network continually send 1500-byte bundle every subsequent which utilizes 24 bit IV at that point entire key space exhaust in approx. 1 hours. IV recovery bring about corruption in execution of RC4. When enough bundles get different assaults can be applied to discover key,

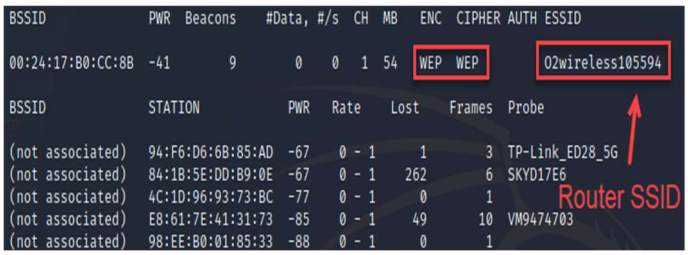
1. wireless Router Configure using 64 Bit WEP keys



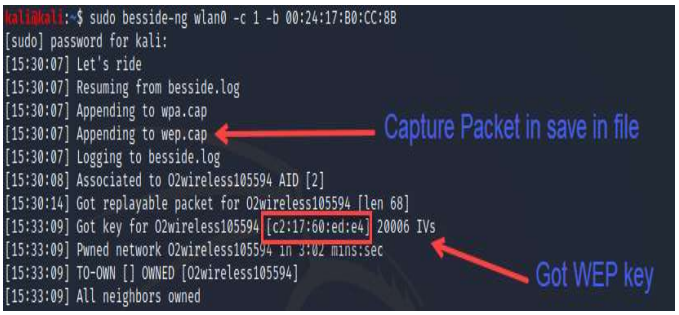
1 Check the status of the WLAN using the command **sudo iwconfig**



2 Execute the **sudo airodump-ng wlan0 –encrypt wep** to list all the wireless details



3 Copy the **BSSID** of the Router and perform attack on **Channel 1** by executing the **beside-ng wlan0 -c 1 -b <mac-address>** it will provide the WEP key after twenty thousand IV [-c for wireless channel -b for BSSID]

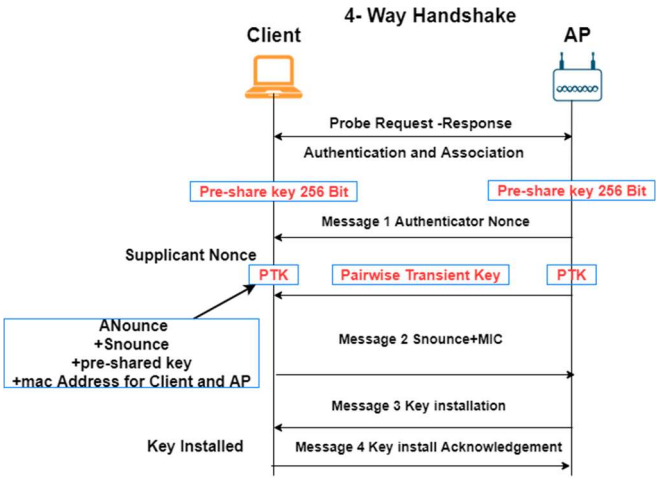


WPA2 encryption security and Associated Flaws

The WPA2 protocol was introduced to replace the security weakness in WEP protocol (Abo-Soliman and Azer, 2018)

As per IEEE 802.11i standards the WPA2 offer the AES encryption for confidentiality and mandate Cipher Block Chaining message authentication protocol for integrity. the four-way handshake and authentication mechanism allow encryption cipher and key to be exchanged between client and supplicant

Fig-3 Four-way Handshake Under WPA2



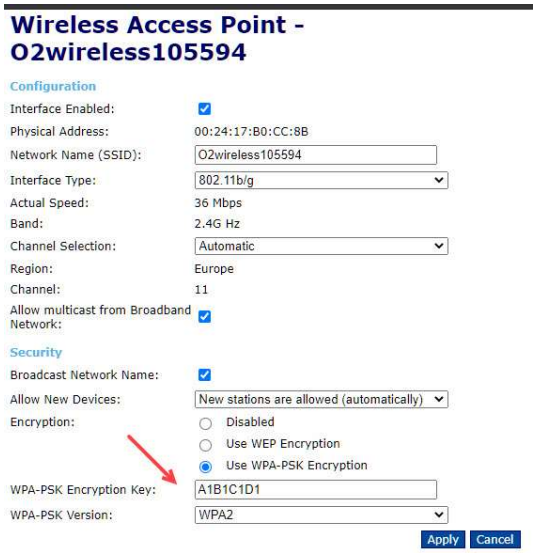
As Per Graphics WPA2 process client and AP participate in probe request and response and based on that AP send authenticator Nonce and afterwards client generate PTK using {anonce+snonce+pre shared key +mac address of client and AP] and By confirming the value of pairwise transient key client send Snonce+mic message to AP and Once AP match the Value then AP initiate key installation message and client provide the confirmation for the Key Validation

The WPA2 Flaws

The attacker send the de-authentication packet between client and AP and Once the Client re-initiate the connection with Access point ,the attacker capture the four(Fehér and Sándor, 2018a) way handshake between client and AP.then afterwards the hacker run the dictionary attack using common password list to decrypt the WPA keys

Cracking the WPA2

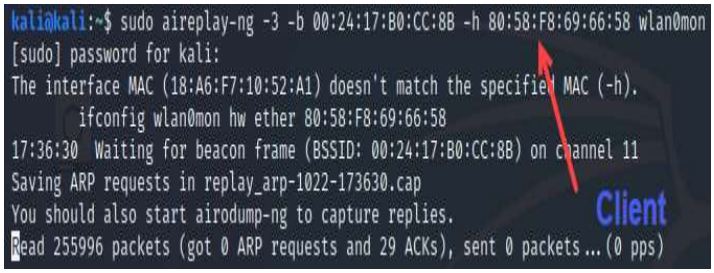
1 Change the Encryption from **WEP** to **WPA2** in the same Router and set the Different Key



2 Execute **Airmon-ng** with specific base station id so it demonstrates only relevant information

3 Capture the Base station communication which is running on channel 11 and write it down into wpacrack file

4 Capture Base station and connected host ARP Request Packets in the interval of 3 seconds



5 Send De-auth packet to re-initiate connection for the client which is connected to router so it can re-negotiate

```
kali@kali:~$ sudo aireplay-ng --deauth 0 -a 00:24:17:B0:CC:8B -h 80:58:F8:69:66:58 wlan0mon
[sudo] password for kali:
The interface MAC (18:A6:F7:10:52:A1) doesn't match the specified MAC (-h).
    ifconfig wlan0mon hw ether 80:58:F8:69:66:58
17:38:26  Waiting for beacon frame (BSSID: 00:24:17:B0:CC:8B) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
17:38:26  Sending DeAuth (code 7) to broadcast -- BSSID: [00:24:17:B0:CC:8B]
```

6 Airodump-ng utility capture the handshake

```
CH 11 ][ Elapsed: 5 mins ][ 2020-10-22 17:39 ][ PMKID found: 00:24:17:B0:CC:8B

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

00:24:17:B0:CC:8B    0   0     2361       49    0  11  54   WPA2 CCMP   PSK  O2wireless105594

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

00:24:17:B0:CC:8B  80:58:F8:69:66:58  -31   36 - 1      0       112  PMKID  O2wireless105594
```

7 Decrypt the WPA 2 password using the Dictionary attack by executing **sudo aircrack-ng wpacrack-01.cap -w password.txt** [file should have the password that match with encrypted file]

```
[00:00:00] 2/3 keys tested (89.35 k/s)

Time left: 0 seconds                                      66.67%

                        KEY FOUND! [ A1B1C1D1 ]


Master Key     : 14 DD 54 3F 91 7B 90 CD 5D F1 D0 08 47 C6 03 2A
                 E7 70 66 2B B5 6C 22 50 49 59 BC 0A 64 58 97 9F

Transient Key  : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

5. Technical flaws - Research 802.11 clients and identify flaws and they can Exploited

1 Caffe Latte attack

The two researchers(Antoniewicz, n.d.) at Airtight Networks discover the ;café latte attack' it is one kind of WEP attack in which attacker can recover the key without being in the same vicinity of wireless network(Choi et al., 2008) by exploiting the isolated client in the public area. the shared key authentication flaws under WEP algorithm leverage by the hacker and intentionally use message modification flaws in WEP. An (Fahmy, Nasir and Shamsuddin, 2012)attacker can use the *ARP* responses to obtain the WEP key in less than 6 minutes

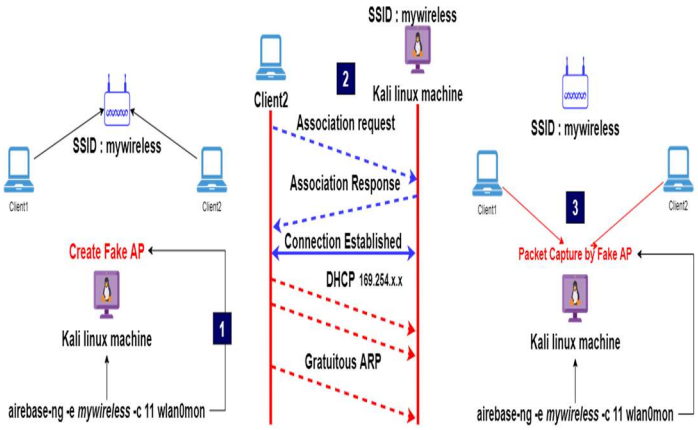


Fig-4 Café latte attack Graphical Presentation

Step1 : The Attacker create the fake access point with common SSID name ,for which client already store the WEP key in Operation System Cache

Step2: once the client recognize the Identical SSID which are they used to connect earlier it thinks it is legitimate wireless Access Point and Connect to the software based Access point which is created by the hacker using Kali Linux machine with Airbase-ng Utility

Step3 once the connection established then client send DHCP request for the IP address from fake Access point ,and after few attempts the request will time out and then client send Gratuitous ARP packet which is captured by the attack machine and Once enough packet is captured. the attacker run the Aircrack-ng Utility to decrypt the WEP key from the Capture File

2 Evil twin attacks

In the Evil twin attacks, the attacker(Gonzales et al., 2010) forcefully closes the client association to AP by sending the de-authentication packet. Once the client disconnects from the legitimate AP, the Attacker then trick the client to automatically connect the Fake Access Point which is exactly have same BSSID and SSID as the Legitimate Access point and Once the Client connects to the Fake access point then the client will be redirected to Captive portal which is created by the attacker.

The Captive Portal page ask the client to enter WPA Key to browse the Internet and if clients enter the Key then that key will be received by a hacker in clear text format in Kali Linux Machine

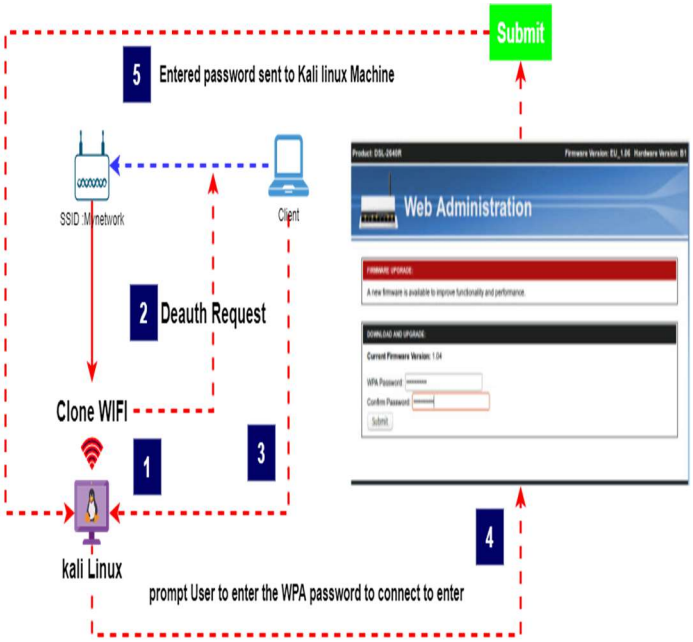


Fig-5 Evil Twin Attacks

There is some pre-requisite for it (Kumar and Paul, 2016) that must be taken care of by the attacker before attempting an attack

- The attacker needs to Grab the BSSID for the legitimate Access Point using Airodump-ng utility
- Attacker Require the SSID and its wireless Channel on which they can perform an attack
- Fluxion tool wizard-based hacking utility attack(Permatasari and Eaganathan, n.d.)

6. Choose the most suitable security measures for your scenario and justify your choice

Wireless Threats Against Lan Security (Frankel et al., n.d.)

Threat Category	Description
Denial of Service	Attacker prevents or prohibits the normal use or management of networks or network devices.
Eavesdropping	Attacker passively monitors network communications for data, including authentication credentials.
Man-in-the-Middle	Attacker actively intercepts the path of communications between two legitimate parties, thereby obtaining authentication credentials and data. Attacker can then masquerade as a legitimate party. In the context of a WLAN, a man-in-the-middle attack can be achieved through a *bogus* or *rogue AP*, which looks like an authorized AP to legitimate parties.
Masquerading	Attacker impersonates an authorized user and gains certain unauthorized privileges.
Message Modification	Attacker alters a legitimate message by deleting, adding to, changing, or reordering it.
Message Replay	Attacker passively monitors transmissions and retransmits messages, acting as if the attacker were a legitimate user.
Traffic Analysis	Attacker passively monitors transmissions to identify communication patterns and participants.

The WEP is the first encryption algorithm Developed by IEEE for the Wireless Communication. And it is also most criticized by the security researcher community for its Weakness. Because the associated WEP key can be Easily decrypted and there is nothing as Administrator can do for that .the only option to enhance the security framework is either Administrator of the device implement IDS (Zhang et al., 2010) or IPS if device support it or they can change encryption method to WPA2

The WPA2 Provide the AES encryption, which is more secure than WEP encryption. However, the attacker can gain the Access (Pimple et al., 2020b)of Wireless device using brute force attack if the administrator of device forgets to disable WPS Default Pin, no matter how many time administrators modified the WPA pre-share key the attacker still gain the access of device using WPS pin. Hence WPS setting should be disabled to prevent a hacking attempt

The administrator of device chooses the weaker WPA2 Passphrase then an attacker might be able to decrypt the (Fehér and Sándor, 2018b)password by using brute force attack hence it is recommended to use a more complex password to overcome the dictionary-based attack

IEEE 802.1X standard can be integrated for secure Access Control and EAP [extensible Authentication Protocol] as a framework for authentication message, such as Radius Server [Remote Authentication Dial-in Service] to authenticate (Kang et al., 2004)each user. If the hacker ,somehow get WPA key then .still it will be impossible for him to access the network resources due to additional user authentication server radius

Periodically changing the WEP and WPA key with stronger password scheme to protect the network being compromised

The SNMP and Syslog server can be applied on the device so any (Frankel et al., n.d.)events or logs can be captured and store by the server for the compliance purpose

The end user security software ,which can differentiate between (Frankel et al.,