Wireless Security Assessment of Home Networks

Wireless Security Assessment of Commercial UK Broadband Routers

Module: SOC09109

PM - Willaim Donaldson | 40582998
Aaron Carrigan | 40537983
James Malcolm | 40583032
Claudio Neri | 40583043
Balram Singh | 40583059
Krystof Wrobel | 40583068

Executive Summary

This work evaluates the current state of wireless security using WPA2 in home networks around the United Kingdom. To do this, the latest models of wireless access points from the top three largest internet service providers (Sky, BT, Virgin) have been considered. To ensure proper testing across these ISPs, the cyber kill chain has been used as a common methodology.

The ultimate aim of this endeavour is to determine the impact exploitation of WPA2 has on real world systems. To this end, a variety of tools ranging from free and opens source to paid hardware have been analysed and used to achieve this goal. The findings have revealed that obtained the hashed password in a WPA2 authentication handshake capture is extremely easy and has been automated. The difficulty comes from cracking the hash which directly corelates to password complexity and length.

The research suggests that ISP provided routers are resistant against WPA2 authentication exploitation as they use strong default passwords that would take an improbable amount of time to crack, even when considering the law of averages. Finally, a range of mitigations have been discussed covering both technical and non-technical users ranging from using WPA3 authentication from an ISP provided wireless router to deploying your own custom access point.

Table of Contents

1. Introduction

Commented [JM1]: Introduction to the report. Include highlighted aim below?

Wireless network security has become critical, particularly in the context of residential broadband routers in the United Kingdom. This technical research goes into the Wireless Security Assessment of Commercial UK Broadband Routers, a detailed study designed to examine the vulnerabilities implicit in the WPA2 protocol and the routers' default security mechanisms. Through this research, the aim is to improve the cybersecurity posture of home networks, resulting in a safer digital environment for individuals and their organisations.

The primary aim of this project is to raise awareness about the essential importance of strong network security standards and to provide practical insights and remedial techniques for vulnerabilities uncovered during our wireless security evaluation. As a group of dedicated cybersecurity experts, recognise the constantly developing threat environment and the need for educated and proactive protection solutions. By publishing our results, the hope is to not only educate the public and industry stakeholders about common security issues but also to provide them with the information and tools required to protect their home networks from possible cyber-attacks.

This report details the steps taken through the assessment process, including the methodology used, vulnerabilities discovered, and recommendations for mitigating these risks. It demonstrates the commitment to supporting the cybersecurity community's continued efforts to protect digital infrastructures and enhance security awareness and resilience among users and service providers.

2. Scope

The scope of this security assessment is strictly within evaluating the security present on routers owned by the project team members, with a clear directive to remain within the legal boundaries of the computer misuse act explicitly remaining within the confines of the law. All testing will be restricted to the home networks of the team and will ensure that no firmware is flashed on to the routers, the team will ensure that no devices which are not owned by the team members will be connected to the network during the security assessment process.

Additionally, this assessment is conducted with the intent to comply with the terms and conditions as set by the team’s individual internet service providers (ISP). An exception to that is

made for the assessment of the virgin media router which has been purchased directly from eBay, by doing this the team are not bound by the restrictions set out in virgin medias terms and conditions thereby granting more flexibility to the team's approach to the assessment. The rules of engagement are as follows:

- Project Team Owed Routers
- No firmware flashing.
- No non-team member clients connected.
- Must remain within the boundaries of the home network.

3. Methodology

Cyber Kill Chain

This report delves into penetration testing techniques through the lens of the Cyber Kill Chain framework. Originating from Lockheed Martin, this framework outlines the seven stages of a cyber-attack: Reconnaissance, Weaponisation, Delivery, Exploitation, Installation, Command and Control, and Actions on Objectives. These stages offer a blueprint for understanding and addressing advanced cyber threats, allowing organisations to develop comprehensive strategies for prevention, detection, and response.

In the context of our assessment focusing on the security vulnerabilities of ISP routers, particularly those employing the WPA2 protocol we selectively apply four pivotal stages of the Cyber Kill Chain: Reconnaissance, Weaponisation, Exploitation, and Action and Objective. This tailored approach allows us to specifically target and expose the weaknesses inherent in the WPA2 protocol, showing how they can be exploited and what measures can be taken to mitigate these vulnerabilities.

Reconnaissance:

This initial phase incorporates both passive and active reconnaissance strategies to gather comprehensive information about the target networks and their configurations. Passive reconnaissance involves using tools like Kismet to detect available networks, identify their encryption types, and confirm the use of the WPA2 protocol. This passive approach ensures we gain a broad understanding of the network environment without alerting the target system to our presence.

In addition to these passive techniques, we also employ active reconnaissance methods, specifically through the execution of de-authentication attacks. These attacks actively disrupt network communications, forcing devices to reconnect and, in the process, reveal critical information about the network's security settings and vulnerabilities. De-authentication attacks serve as a practical tool for mapping network topologies and understanding the network's operational dynamics under stress conditions. This combination of passive and active reconnaissance is critical for thorough planning and identification of potential attack vectors, providing us with a detailed overview of the target environment.

Weaponisation:

Once sufficient information has been collected, the next step is to prepare the tools and methods needed to exploit the identified vulnerabilities in WPA2. This involves configuring software like John the ripper and wordlists to crack the hashed WPA2 encrypted data. Although no malicious software is created or used, this phase simulates how attackers might prepare their attack vectors based on the vulnerabilities and data discovered during reconnaissance. The objective here is to tailor our approach to specifically challenge the WPA2 protocol's security mechanisms.

Exploitation:

With our penetration testing toolkit primed, we transition from active reconnaissance to directly engaging with the vulnerabilities of the WPA2 protocol. The exploitation phase leverages the EAPOL frames captured earlier, employing techniques specifically aimed at decrypting the network's security keys. The primary tool in this phase is the offline hash cracking process, where captured WPA2 handshakes are analysed to uncover network passwords.

The de-authentication attacks initiated during the reconnaissance phase not only disrupt network communication, prompting the necessary handshake retransmissions, but also set the stage for this critical exploitation activity. By forcing devices to reconnect, we effectively capture the handshake data required for our analysis.

Once in possession of the handshake data, we employ sophisticated dictionary and brute force attacks against these hashes. Tools such as Hashcat are utilised for this purpose, testing thousands to millions of potential password combinations against the captured data. This methodical approach aims to demonstrate the feasibility of decrypting a WPA2-secured network's passphrase, thereby gaining unauthorised access. The primary goal of this phase is to highlight the critical vulnerabilities within WPA2 that can be exploited through sophisticated, yet commonly available, cryptographic attacks.

Action and Objective:

The culmination of the assessment is to analyse the data gathered through exploitation and to assess the real world impact of the vulnerabilities on network security. This involves determining the ease with which an attacker could decrypt WPA2 encryption and gain network access. The findings are then used to develop recommendations for mitigating the identified risks, such as upgrading to WPA3 where possible, changing default network settings, and educating users on the importance of strong, unique passwords. Ultimately, the objective is to enhance the security posture of home networks against the weaknesses of WPA2.

By concentrating on these specific stages of the Cyber Kill Chain, our report aims to provide a clear and comprehensive understanding of the vulnerabilities within the WPA2 protocol and to propose practical solutions to enhance wireless network security.

4. Reconnaissance

4.1 Introduction

To demonstrate the wireless vulnerability as being present as a standard when ISP's deploy routers to new customers the security researchers have targeted three separate routers these routers are Virgin hub 3.0, Sky SR203, BT Smart Hub 2, to demonstrate the ease of attack and the multiple attack vectors presented by previous research, the researchers have demonstrated four different tools to exploit the same attack vector, these tools have been selected due to their accessibility, those are, Kismet, Pwnagotchi, Flipper Zero, and Wifite.

4.2 Targets

4.2.1 Virgin hub3

The Virgin media hub was released in 2016, offering dual-band wireless connectivity over "WiFi 5" using the 802.11ac protocol, it has four 1Gbs ethernet adapters and comes with Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA2) and Wired Equivalent Privacy (WEP) encryption standards along with Wi-Fi Protected Setup (WPS) push button security. Despite offering a further two generations of advancement the hub 3 is the base standard offered by Virgin Media. The hub 3 offers four different speed options which are 125Mbs, 250Mbs, 350Mbs, and 500Mbs however these speeds may be limited depending on the area of deployment, the main difference in these four speeds is the maximum download speed. The virgin media hub comes preconfigured with a service set identifier (SSID), these are generally

the equivalent of VM123456-2g/5g

4.2.3 Sky SR203

The Sky SR203 router was released on September 4, 2019. The SR203, also known as the Sky Q Hub 2, was designed to offer improved wireless broadband connectivity, addressing the need for higher speeds and better coverage within the household. It supports a variety of features including the promise of a Wi-Fi connection guarantee. Although this is not the newest model for Sky it still has a lot of security features such as Encryption, Authentication, Firewall Packet inspection and Smart channel selection. Smart channel selection means the Smart Hub automatically connect devices to the fastest Wi-Fi channel and frequency available. Another feature is the dual band the Smart Hub uses both the 2.4GHz and 5GHz bands. Its security features include WEP WPA2-PSK (AES), and WPA/WPA2-PSK (Mixed Mode). WEP, although the oldest and least secure of these options, is still offered for compatibility with older devices. WPA2-PSK Mixed Mode allows for compatibility with devices supporting either WPA or WPA2 standards.

4.2.4 BT Smart Hub 2

The BT Smart Hub 2 was launched from BT around late 2018 to early 2019. the BT Smart Hub 2 is a sophisticated dual-band router that adheres to the latest 802.11ac wireless standard. It is designed to provide a reliable, high-speed internet connection, is around 433Mbp. A distinctive feature is the Smart Scan, which continuously checks your network connection and the router's performance, automatically rebooting if it detects a problem. This router accommodates both 2.4GHz and 5GHz bands and is equipped with four gigabit Ethernet ports for direct wired connections to up to four devices. Separating itself from its predecessors, the Smart Hub 2 incorporates seven antennas, surpassing the antenna count of earlier models, and features customisable LED lights that can be turned off to reduce visual disturbance. In the realm of security, the BT Smart Hub 2 incorporates the following security protocols WPA2 encryption, including WPA2-PSK (AES) and WPA/WPA2-PSK (Mixed Mode). The device supports Wi-Fi protected Setup (WPS), facilitating effortless device connections without the necessity of entering a password, though this feature can be disabled to enhance security measures further.

4.2.5 WPA2 Protocol

The common feature between these routers is the security protocol Wi-Fi WPA2 which will be the main target of the security assessment. WPA2 utilises the Advanced Encryption Standard (AES) encryption algorithm, this algorithm works by generating a four-way handshake which consists of the following:

Request and Response (Messages 1 and 2):

The client initiates the handshake by sending a request to join message to the access point (AP), the AP responds to the client's request by returning a message known as a nonce which is a random number used only once.

Client Authentication and Key Generation (Messages 3 and 4)

After receiving message 2 from the AP the client then generates its own nonce it then uses the information received from the AP along with its authentication credentials to create a cryptographic hash which it then sends to the AP. The AP receives message 3 from the client and verifies the provided credentials, in then calculates its own encryption key to verify the sent cryptographic hash, the AP then sends its own nonce to the client which is encrypted with the shared encryption key, once this fourth message is received by the client it decrypts the AP's nonce using the shared encryption key, now that both possess the same encryption key a secure connection can be established and encrypted communication can be engaged.

Extensible Authentication Protocol over LAN

These messages are known as Extensible Authentication Protocol (EAP) messages, these messages are encapsulated within Extensible Authentication Protocol over LAN (EAPOL) frames, the makeup of these frames can be viewed below in Fig 4A

EAPoL Frame Format

MAC Header	Ethernet Type	Version	Packet Type	Packet Body Length	Packet Body	Frame Check Sequence
12 bytes	2 bytes	1 byte	1 byte	2 bytes	variable length	4 bytes

Fig 4A : EAPoL Frame Format

5. Tools

5.1 Kismet

Kismet serves as a powerful Network Intrusion Detection System (NIDS) and a finder for 802.11 wireless networks. It functions by utilising a wireless device in monitor mode, enabling it to monitor and capture network packets discreetly, leaving no trace of its presence. This capability makes Kismet adept at detecting potential suspicious activities within wireless networks. It facilitates the identification of networks through passive packet collection, effectively detecting SSIDs, including those of hidden networks, and inferring the existence of non-beaconing networks through observed data traffic. Figure 5.1A demonstrates Kismet's ability to identify routers from which it intends to gather information. For the purposes of this project, and to enhance security, the physical addresses of personal routers have been obfuscated. Nonetheless, it's discernible that the router employs WPA2-PSK encryption, showcasing Kismet's utility in revealing network security protocols without compromising privacy.

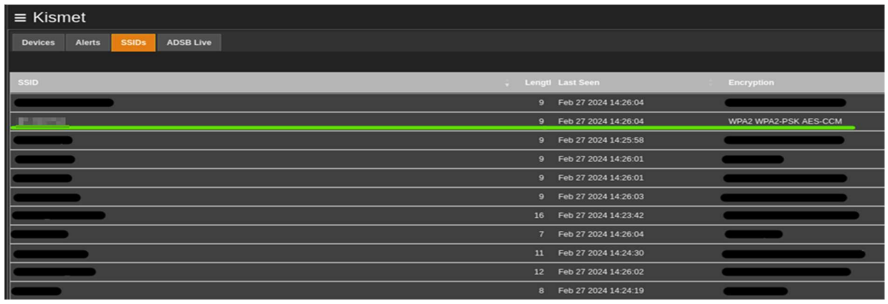


Fig 5.1A: Kismet scan

In Figure 5.1B the "Device Info" section presents data collection features regarding the wireless access point, The image provides detailed identification, indicating that the access point is utilising channel 11, which corresponds to a specific frequency range within the wireless spectrum. Another crucial note during the recognise is the MAC Address that can be used to identify the model of network hardware through the Organisationally Unique Identifier (OUI),

which may reveal potential vulnerabilities specific to certain devices. Knowing the channel and the MAC address can provide essential information for anyone looking to understand or target a specific network.

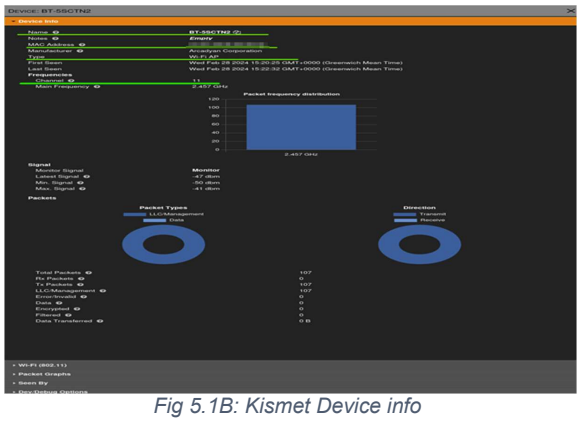


Fig 5.1B: Kismet Device info

In Figure 5.1C, within the 'Wi-Fi 802.11' analysis, we illustrate Kismet's capability to identify devices connected to a network. This identification is made possible by capturing and analysing packets circulating through the wireless network, revealing the MAC addresses of the connected clients. Identifying these devices is a fundamental step towards launching a Deauthentication attack, which temporarily disrupts their network connection. This compels the devices to attempt reconnection, during which the authentication handshake between the client and the network is reestablished. Kismet seizes this opportunity to capture the handshake, storing it in a Pcap file. This file, containing the encrypted network password, becomes a critical asset for offline analysis in the exploitation phase of the security assessment.

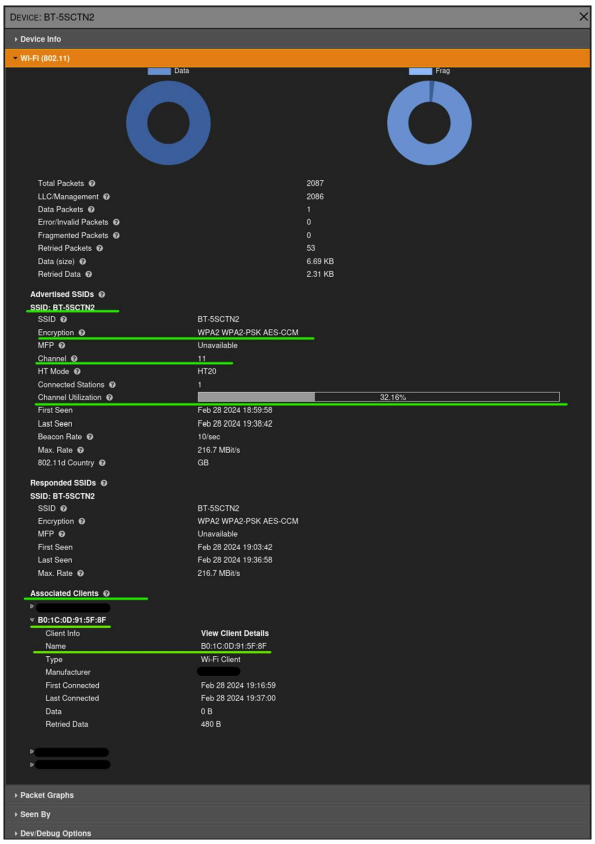


Fig 5.1C: Devices connected (kismet)

In Figure 5.1D, highlighted under the "Wi-Fi 802.11" segment, we mark the completion of a significant phase of the reconnaissance process, underscored by Kismet's effective capture of the 4-way handshake. This key phase in data collection successfully secures the network's encrypted password encapsulated within the handshake. The precision of Kismet's network surveillance, coupled with its targeted observation of client-device interactions, has facilitated the isolation, and recording of this critical encryption key exchange between the client device and the wireless network.

With this phase of reconnaissance culminating in the secure archival of pertinent data within the Pcap file, our focus shifts to the subsequent analysis. The transition into deeper analytical endeavours will be spearheaded by Wireshark, a tool renowned for its detailed network protocol analysis capabilities. Wireshark empowers us to conduct a granular inspection of network traffic, facilitating the precise filtration of protocols, the meticulous examination of individual packets, and the comprehensive assessment of the data's contents. The Pcap file, named "C0 D7 AA 8F 85 98-B0 46 92 59 5C 5B-handshake.pcap," will undergo a thorough analysis in Wireshark to affirm the data's successful capture. This step is integral to validating the reconnaissance efforts and will serve as a foundation for decrypting the WPA2 passphrase, leveraging the detailed insights obtained from the handshake.

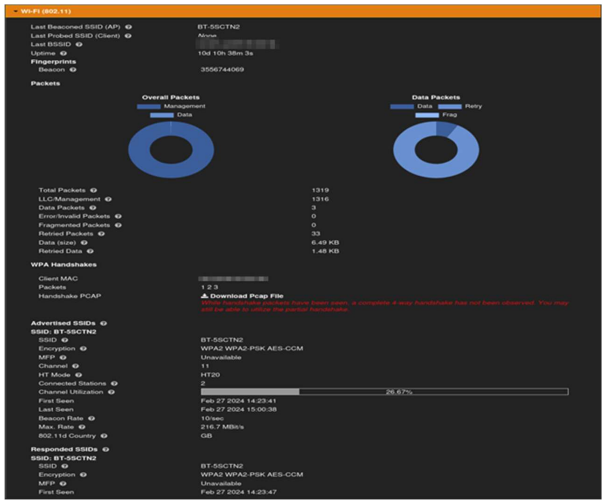


FIG 5.1D: Pcap Capture (Kismet)

In Figure 5.1E, we are presented with a detailed examination of wireless network communications, starting with a beacon frame. This beacon frame, originating from a specific MAC address, broadcasts to all devices to announce the presence of the wireless network.

Following this, the second packet captured plays a crucial role in the network's authentication mechanism, being a segment of the EAPOL protocol. The packet originates from a device labelled with a partial MAC address identified as "GuangdongOpp_xx:xx:xx," presumably a client device, and is destined for another device associated with "Arcadyan_xx:xx:xx." It is characterised as Key

(Message 2 of 4), signifying its place as the second message within the four-way handshake, with a total length of 155 bytes.

Subsequently, the third packet, also falling under the EAPOL protocol, represents Key (Message 1 of 4), marking the commencement of the four-way handshake. The transmission vectors from the Arcadyan device towards the GuangdongOpp device, as indicated by the source and destination MAC addresses.

The narrative extends to the fourth packet, also encapsulated within the EAPOL protocol, recognised as Key (Message 3 of 4) within the four-way handshake. The flow is from the Arcadyan device to the GuangdongOpp device, maintaining the dialogue necessary for the handshake's completion.

Crucially, the packet poised for in-depth analysis in pursuit of the network passphrase is the second packet. This packet reveals the interaction between the router and the client, embodying a critical moment in the authentication process. It is within this exchange that the potential to uncover the network passphrase lies, making it a focal point for analysis in understanding the dynamics of network security.

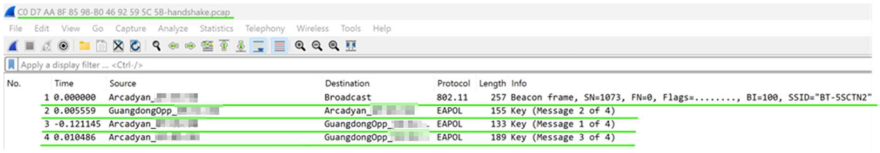


Fig 5.1E: Wireshark Pcap (Kismet)

5.2 Aircrack-ng

Aircrack-ng is another very useful tool in the reconnaissance and exploitation stages of the Cyber Kill Chain framework when assessing the security of ISP routers. Aircrack-ng is an all-encompassing toolkit aimed at examining the security of Wi-Fi networks. It offers a wide range of capabilities, from monitoring and attacking to testing and cracking Wi-Fi networks. Aircrack-ng will mainly use for its ability to monitor network traffic. It allows the interception of Wi-Fi packets and has the ability to save this information for deeper examination later. This feature is vital for spotting accessible Wi-Fi networks, gathering information about them, and figuring out how they are protected. Through packet analysis, researchers can uncover what kind of

encryption the network uses, how strong the signal is, and other relevant details that help in developing a focused approach for testing the network's security.

Figure 5.2A shows monitoring a wireless network on the IPS router provided by Sky, using Aircrack-ng it shows the network monitoring to analyse the traffic that is around the area. Figure 5.2A shows the BSSID as a unique marker for identifying the target access point, alongside the signal strength (PWR) which is strong, suggesting the researcher is well within range to launch an effective attack. The presence of beacon frames signals that the access point is actively broadcasting, while the number of data packets indicates there's current activity on the network.

The mentioned data rate is measured in megabytes and highlights the network's ability to handle fast data transfers. From a security standpoint, the network uses WPA2 with CCMP encryption and PSK authentication. This level of security is robust, indicating that only advanced hacking techniques could potentially compromise it. The network's ESSID, "SKY8CTPQ," with a BSSID of “80:xx:xx:xx:xx:xx” serves as a clear identifier for those testing the network, sitting on channel 6 this will make it easier to locate during the exploitation phase.

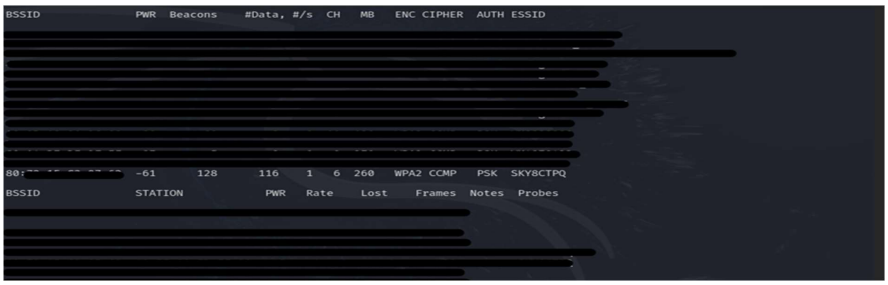


Fig 5.2A: Aircrack-ng Scan

Figure 5.2B, displaying Wireshark's visualisation, highlights the capture of EAPOL frames pivotal to the WPA/WPA2 authentication mechanism. The frames are meticulously labelled "Key," representing the entire 4-way handshake sequence, encompassing "Message 1 of 4" through "Message 4 of 4." This complete capture, executed by Aircrack-ng, signifies the culmination of the reconnaissance phase using Aircrack-ng. With all four messages successfully captured, Aircrack-ng has concluded its real-time network monitoring and is now poised for the offline weaponisation and exploitation phase.

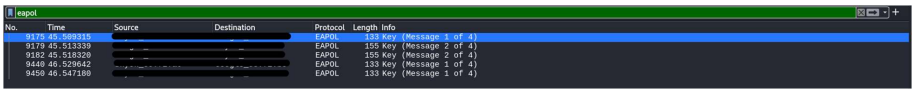


Fig 5.2B: WireShark Pcap (AirCrack-ng)

5.3 Pwnagotchi

Pwnagotchi is a device created with the use of a Raspberry Pi Zero W typically, however any device capable of running the Raspbian based distribution of Linux can be used as seen below in Figure 5.3A.

Figure 5.3A: Pwnagotchi assembled with a display.

A Pwnagotchi is capable of monitoring network traffic by default when powered with the custom image loaded onto an SD card. Without further configuration, the device can and will automatically begin Wi-Fi Deauthentication attacks that target the communications between access points (AP) and clients/users to capture a 4-way handshake where secure key information is passed. With this secure information captured, connections can be tracked, login details and private information captured and even the secure passphrase can be gained through cracking the WPA2 hash generated by the 4-way handshake.

This section details the process of capturing a handshake using the Bettercap UI v1.3.0 using Bettercap V2.24. Bettercap UI being an interface that allows better manual control of the Pwnagotchi which normally operates in the auto/AI modes. And through the Auto and AI modes of the Pwnagotchi which are enabled by default when only supplied with power.

To prevent malicious and unintended attacks against networks in an area, disable Deauthentication completely by adding a line that sets Deauthentication to off. Doing this before using the Pwnagotchi is vital to ensure no laws are broken when the device is put into Auto or AI modes. Once complete accessing the Bettercap UI through a browser allows for the initial recon to be completed where a list of BSSID's and ESSIDs can be collected, then added to a whitelist,

preventing Deauthentication attacks happening on those networks and any omitted will be deauthenticated. This is completed by editing a “config.toml” file within the /etc directory. Reenabling the Deauthentication will then allow network sniffing to happen, and clients seen on non-whitelisted networks will be attacked forcing a handshake to happen.

Figure 5.3B below shows the Wi-Fi module running on the Bettercap UI. This enables monitor mode for the Raspberry Pi Zero’s Wi-Fi chip and any networks that broadcast on the 2.4GHz band can be seen are listed. If the vendor can be identified from the MAC address, this is displayed along with the encryption type, channel the network is operating on, clients connected, and any data sent or received. These are sorted by signal strength to the Pwnagotchi.

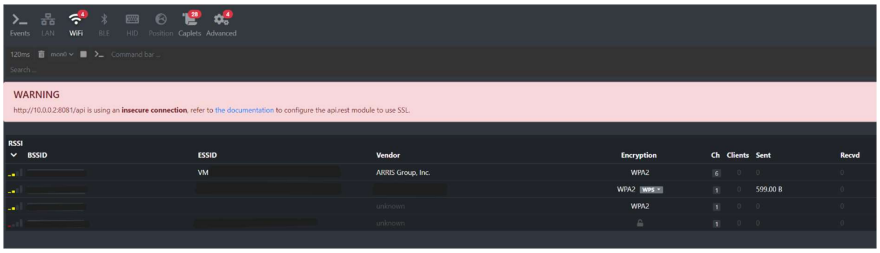


Figure 1: Bettercap UI; Wi-Fi Module

When a client has been seen by the Pwnagotchi, if in Auto or AI modes, the Deauthentication process is automatically completed until a handshake is captured, which is displayed as “PWND”. The handshake is saved as a PCAP file to the “/etc/pwnagotchi” directory. Operating in these modes is seen below in Figure 5.3C.

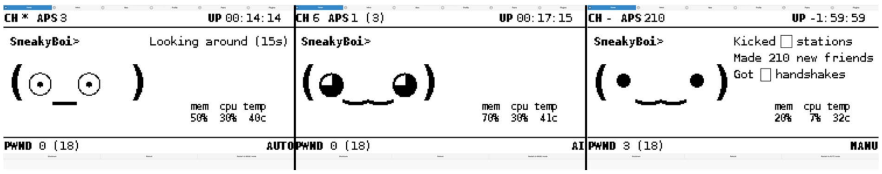


Figure 5.2C: Pwnagotchi modes; Left: Auto, Middle: AI, Right: Manual

Using Bettercap allows for better control over actions conducted. Where scripts can allow for mass Deauthentication as would be done in Auto and AI modes, the Bettercap gives a command bar, where commands to control the device are entered. From there Deauthentication to specific devices can be carried out by entering either a BSSID or ESSID. If no clients are seen, errors are thrown. The list of actions that can be carried out by the Wi-Fi module are extensive in that recon can be carried out, channel hopping can be stopped, and events can be tracked and monitored.

When Bettercap is successful in capturing a handshake, next to the encryption a red key is shown to signify that the key has been captured either monitoring a connection happen between the AP and a client or a Deauthentication attack has been conducted on a client forcing a handshake. Like the Pwnagotchi modes, the handshake is captured as a PCAP and saved similarly in "/etc/pwnagotchi/bettercap/handshakes".

Below in Figure 5.3D shows the 4 way-handshake captured by Bettercap; each step identified by Wireshark using the EAPOL protocol. With this information, it can be converted into a usable WPA2 hash.

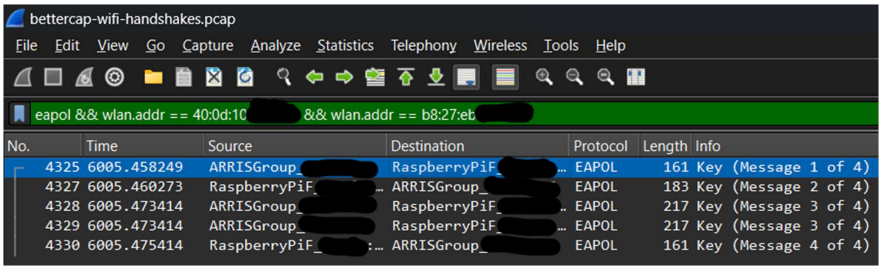


Figure 5.3D: Bettercap handshake capture (Wireshark)

It is important to note that not all clients connected to APs can be seen by the Raspberry Pi Zero, as some devices increase their own security using personal protection shown by "WPA2-Personal" on devices. Lower end devices with less security such as printers and even Raspberry Pi's make excellent targets to aid in capturing a handshake using the above methods.

5.4 Wifite

Wifite is a python script that allows for automatic auditing of wireless networks. It does this providing a wrapper to aircrack-ng and similar tools depending on the attacks that occur. By default, wifite runs in interactive mode allowing for the user to select specific targets. Optional command line arguments can be provided to the tool to only use specific attacks or to specifically target a certain SSID. For this walkthrough, the authorised network being targeted is VM734980-2G.

To use Wifite, the program of the same name can be executed from the terminal. To specially target WPA and WPA2 networks, the –wpa flag has been provided as an argument as seen below in Figure 5.4A.

Figure 5.4A Execute Wifite to target WPA2 Networks

Being an automatic tool, Wifite works on its own and automatically places the wireless adapter into monitor mode. It then listens to the wireless traffic within range of the antenna and lists all available wireless networks as can be seen in Figure 5.4B.

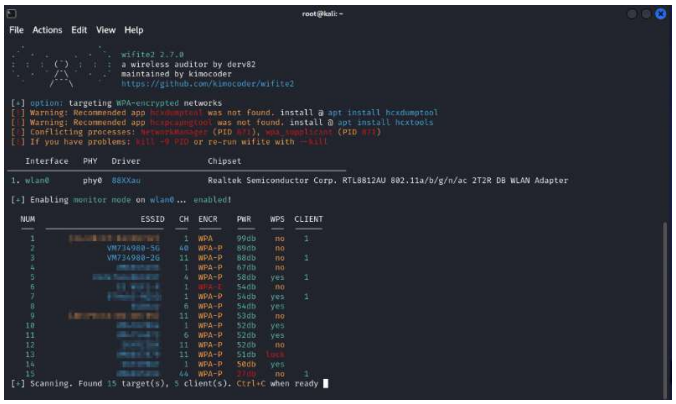


Figure 5.4B Wifite AP Findings

To stop scanning, the CTRL+C keys must be pressed. Once this happens, the program allows for the user to select which network or combination of to target attacks against as seen in Figure 5.4C.

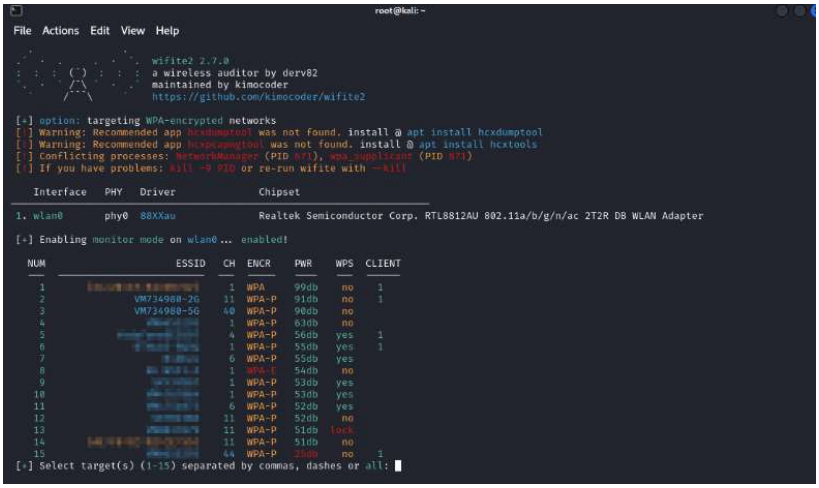


Figure 5.4C Wifite Attack Options

From the list shown below, the network with the ID of 1 was targeted. The tool then began to capture the handshake used in the WPA2 authentication process. To do this aircrack is being used to de-authenticate the connected client and intercept the handshake as they re-authenticate. Additionally, it performs a quick cracking process by default using a short wordlist as seen in Figure 5.4D. Whilst this is not part of the reconnaissance stage, it's part of Wifite's operation by default. To avoid this the –skip-crack option should be provided.

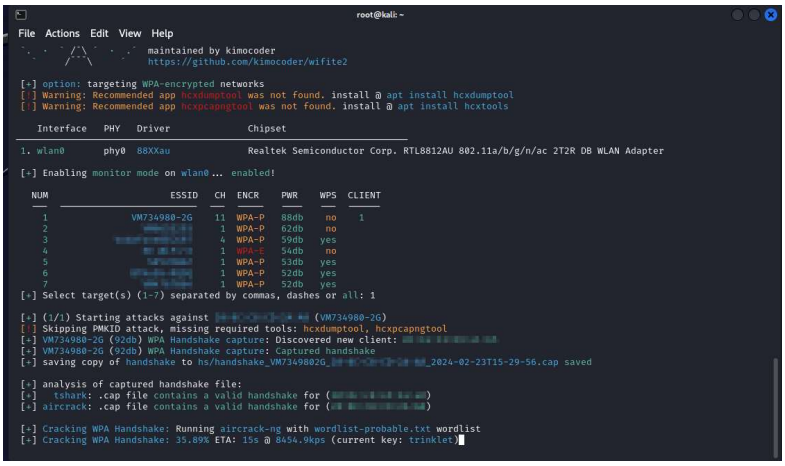


Figure 5.4D Wifite WPA2 Authentication Capture

5.5 Flipper Zero with WiFi dev board

The Flipper Zero is versatile multi tool which is easily accessible to anyone with the financial ability to purchase it, considered completely legal in the UK and available for purchase from various websites both hosted inside and outside the UK. It is a compact form factor tool which combines functionalities such as radio frequency sniffing, infrared communication and near field communication, it also has a selection of general purpose input/output (GPIO) ports which allows for additional components to be added, in this case we will add the Wi-Fi Dev board.

WiFi dev board (esp32)

The ESP32 WiFi dev board offers extensive additional features to the Flipper Zero mainly aimed at wireless security assessment enabling the Flipper Zero to communicate with wireless network devices. When combined with various applications available to the Flipper Zero it presents itself as an easily accessible highly powerful wireless security protocol analyser providing the ability to perform the reconnaissance, weaponisation and exploitation stages of the cyber kill chain framework.

Flipper Extreme Firmware

There are a number of firmware's available for the Flipper Zero with new firmware's being released regularly, for the purposes of this analysis the researchers with employ the use of Flipper Extreme firmware which provides all the tools necessary to carry out the assessment

from applications installed directly on the Flipper Zero, whereas comparatively with some other firmware versions, to use the WiFi dev board you have to use a serial connection to connect directly to the board. Taking the approach of using the Extreme firmware allows for a smoother and more streamlined vulnerability assessment to be conducted.

WiFi Sniffing

By leveraging the Flipper Zero alongside the WiFi Dev Board and employing applications like Wi-Fi Marauder (Figure 5.5A), researchers can effectively survey the airwaves for any access points actively broadcasting their availability for connection.

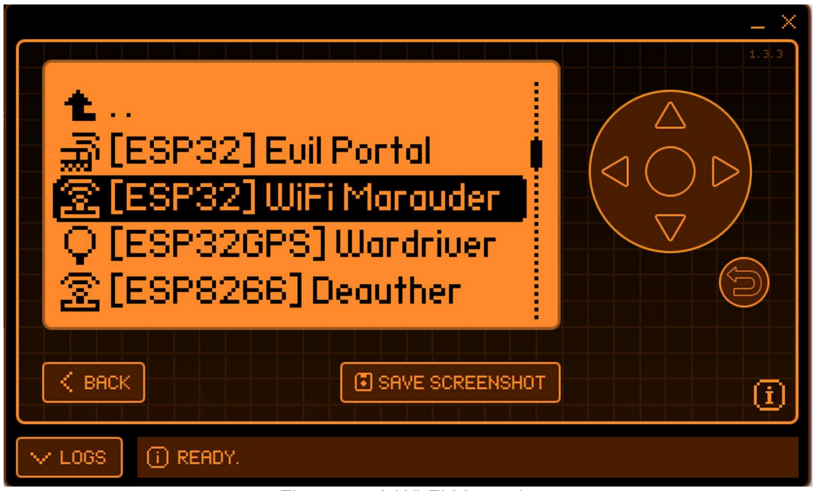


Figure 5.5A Wi-Fi Marauder

Figure 5.5B illustrates how all accessible access points in the proximity of the Flipper Zero are displayed, simplifying the identification process. The presence of default SSIDs, such as those commonly used by Virgin Media routers, provides researchers with direct targets for assessment. This demonstration underscores the Flipper Zero's proficiency in executing WiFi reconnaissance tasks.

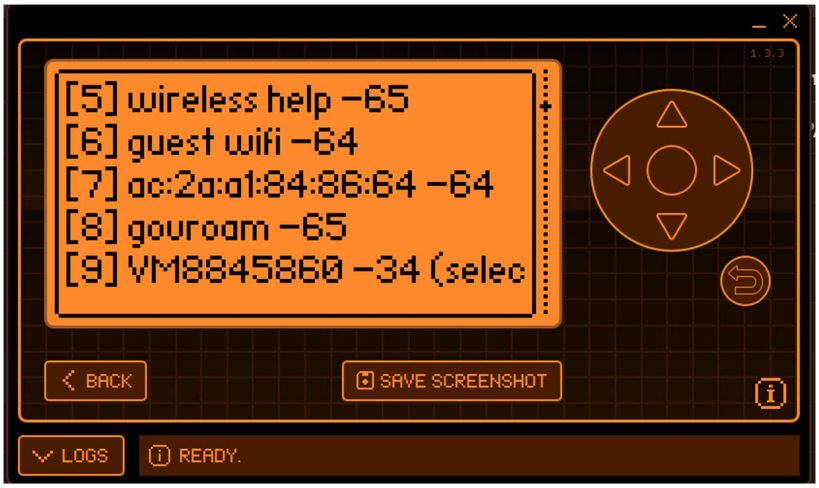


Figure 5.5B Scan AP

After the target has been set the researchers used the Flipper Zero to Sniff the Pairwise master key identifier (PMKID) as seen in Figure 5.5C. By leveraging the Flipper Zero's capabilities for packet sniffing while simultaneously executing a Deauthentication attack (Figure 5.5D), disrupting the normal operation of the target Wi-Fi network. By forcing connected devices to disconnect and attempt reconnection, the Deauthentication attack facilitated the interception of EAPOL frames containing the PMKID as seen in Figure 5.5E.

Figure 5.5C Sniff PMKID

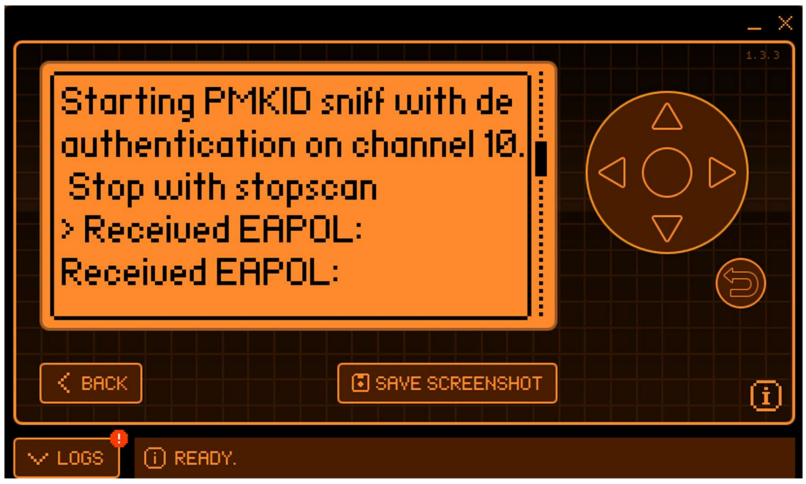


Figure 5.5D Flipper Deauthentication

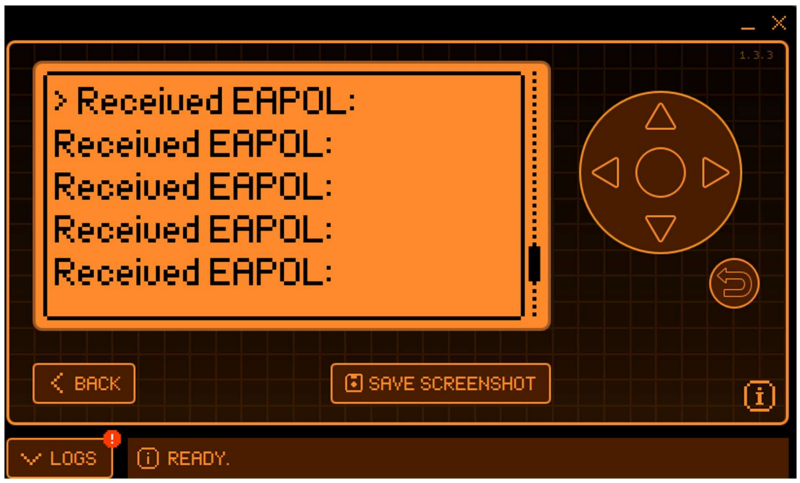


Figure 5.5E Flipper EAPOL Capture

During this packet capture, the researchers targeted the exchange of EAPOL frames containing the PMKID, which is crucial for subsequent offline dictionary attacks. By capturing these frames, the researchers gained insight into the authentication process and obtained the necessary

information to launch offline brute-force or dictionary attacks aimed at recovering the passphrase.

6. Weaponisation / Exploitation

6.1 Brute Force Default Password

Having completed initial reconnaissance and gained the information needed to move onto exploiting the captured 4 way-handshake, the focus is to exploit weaknesses in the authentication process and encryption by hoping that the password is weak. Although default passwords are long enough to pose a challenge and not transmitted over the network plainly, there are resources available today that enhance the ability to extract it from the hash by trying different password combinations or exploiting vulnerabilities in the hashing algorithm. This section focuses solely on brute forcing by trying different combinations.

To begin the brute force process, Hashcat will be utilised due to the free access and ability to run on any device available. To begin the brute force attempt, the PCAP file containing any handshakes will need to be converted to a modern Hashcat compatible file. To do this a tool provided by Hashcat[1] is used, which converts any wpa2 handshakes found in a PCAP file. Once converted the hash should look like that shown below in Figure 6.1A.

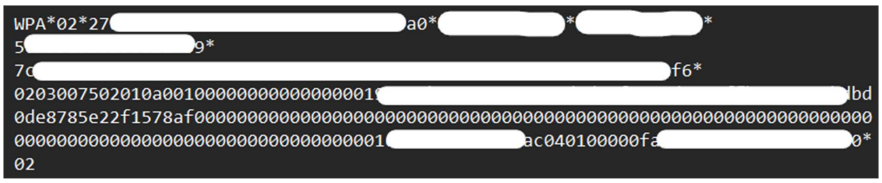


Figure 6.1A WPA2 Converted Hash

Presenting this file to Hashcat identifies it as WPA2 immediately due to the file extension of ".hc22000", 22000 being the mode for WPA-PBKDF2-PMKID+EAPOL which matches the presented hash. To begin the brute force process using this file, the command shown below in Figure 3.1B is used. In the figure "-a 3" means to attack via brute force and "-m 22000" being the mode which it uses, in this case its WPA-PBKDF2-PMKID+EAPOL.

[1] https://Hashcat.net/cap2Hashcat/

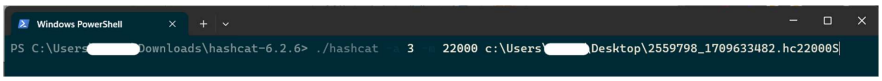


Figure 3.1B Hashcat command.

The resources being used to conduct the brute force attack are solely GPUs. For this attack it is utilising one MSI Ventus 2x RTX 4070 12GB GPU and an AMD Ryzen 5 7600 AMD Radeon(TM) Graphics (integrated graphics with access to 15.6GB of shared and 512MB dedicated GPU memory). Going into this with a default password from a Virgin Media router, the character set is only letters and numbers with no symbols, allowing for no mask to be provided to Hashcat.

Results from running the hash through Hashcat has proven unsuccessful due to the time it will take with the described resources above. Figure 6.1C below shows the status of the running attack against the captured and converted handshake. The time estimated states greater than 10 years, however the actual calculated time is closer to 13,000 years given the complexity and variations it needs to run through.

```
Session..........: hashcat
Status...........: Running
Hash.Mode........: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target......: c:\Users\      \Desktop\2559798_1709633482.hc22000
Time.Started.....: Sat Mar 09 14:15:07 2024 (56 secs)
Time.Estimated...: Next Big Bang (> 10 years)
Kernel.Feature...: Pure Kernel
Guess.Mask.......: ?1?2?2?2?2?2?2?3?3?3?3?d [12]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue......: 5/8 (62.50%)
Speed.#1.........:   883.2 kH/s (6.54ms) @ Accel:16 Loops:128 Thr:256 Vec:1
Speed.#3.........:    27690 H/s (9.02ms) @ Accel:128 Loops:32 Thr:256 Vec:1
Speed.#*.........:   910.9 kH/s
Recovered........: 0/4 (0.00%) Digests (total), 0/4 (0.00%) Digests (new), 0/2 (0.00%) Salts
Progress.........: 51093504/76273226218915430 40 (0.00%)
Rejected.........: 0/51093504 (0.00%)
Restore.Point....: 0/61510666305576960 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:30-31 Iteration:3072-3328
Restore.Sub.#3...: Salt:0 Amplifier:47-48 Iteration:1984-2016
Candidate.Engine.: Device Generator
Candidates.#1....: 7kax30000000 -> 7cw5ananere1
Candidates.#3....: Kfjalerdere1 -> Ki7nierdere1
Hardware.Mon.#1..: Temp: 73c Fan: 62% Util: 99% Core:2685MHz Mem:10251MHz Bus:16
Hardware.Mon.#3..: Temp:  0c Fan:  0% Util:100% Core:2200MHz Mem:2400MHz Bus:16

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit => |
```

Figure 6.1C: WPA2 crack attempt with RTX4070 & Ryzen 5 7600

Should some characters of the password be known, or a pattern recognised, this time can be

brought down drastically, where a mask of 5 characters was provided on the command this reduced the time to just 54 minutes but took as little as 32 minutes to actually crack. However, this essentially reduced the password length to only 7 characters from 12 and can be seen below in Figure 6.1D.

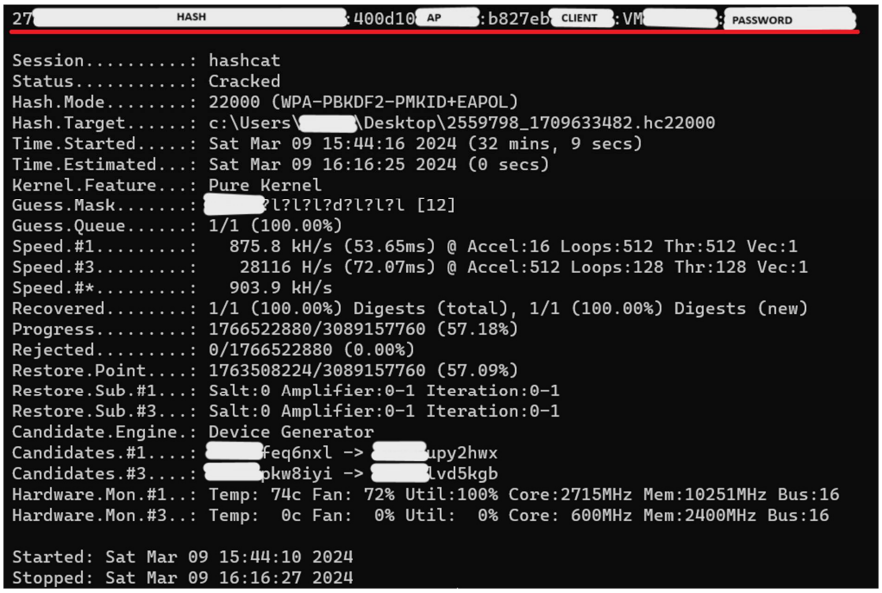


Figure 6.1D WPA2 cracked after given mask.

With current consumer components, brute forcing a default password proves unsuccessful and highly unlikely for the foreseeable future.

6.2 Cloud GPU Infrastructure as a Service (IaaS) – Virtual Machines

With data centre GPUs being computationally more powerful than the average consumer GPU that is aimed at the gaming industry, data centre GPUs can be thought of being out of reach to the average person due to the higher price. For example, a GPU such as a Nvidia H100 priced at £32,000 and a RTX 4070 which costs £520 new. That makes the H100 60 times more expensive than an RTX 4070.

Data centre GPUs and high-end PC components can easily be accessed by anyone with a little knowledge of what they're looking for. In this case it being Infrastructure as a service (IaaS). IaaS can be accessed through many platforms such as Microsoft Azure and Amazon AWS, and

the cost is quite low depending on services provided. IaaS is as simple as connecting to a virtual machine (VM) provided through the cloud.

Microsoft Azure offers spot VMs, where if the hardware is not being used by the person/service it is distributed to, then you can use it at a reduced cost. With the main concern being that if the resources are requested, you can be cut off without notice and you have to wait for resources to become available again.

The VM used to conduct a brute force attack here is the NC64as T4 v3 VM provided by Azure. This instance has an AMD EPYC 7V12 64-Core Processor, 440GB of system memory and 8 Nvidia T4 data centre GPUs. With 8 GPUs the expectation was that the time would be cut short drastically with 8 data centre GPUs, as seen below in Figure 6.2A however what was seen that the time was only reduced by around 5 years however Hashcat showing only greater than 10 years. Also note that the GPUs used had a much lower hash rate than the RTX 4070 but the combined total being 500 kH/s more in total. This is due to the Hashcat relying on Nvidia's Cuda cores.

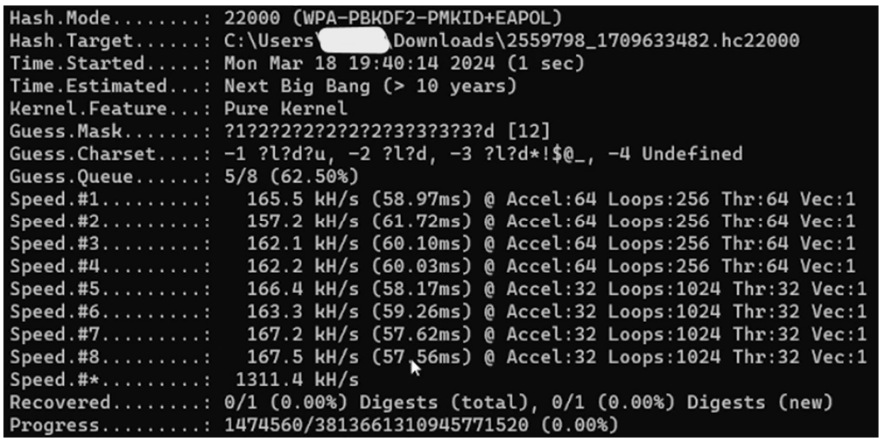


Figure 6.2A Microsoft Azure VM with 8 Nvidia T4 GPUs

With access to greater GPUs such as the Nvidia H100, times could be brought down drastically, and possibly even more with the use of a quantum computer. However, even with reduced costs such as the VM used here where it cost only $2.35 for an hour of use, to gain access to more powerful components the price increases greatly going above $20 per hour.
Using IaaS could prove successful on shorter passwords of 8 characters or less, however on

greater lengths of passwords this still proves unsuccessful.

6.3 Dictionary Attack Phase 1 Default Password

BT

This stage demonstrates a Dictionary Attack on BT Smart Hub 2, applying the Kill Chain methodology, specially focusing on the “Weaponisation” and “Exploitation” stage. Here, the process of cracking the BT Smart Hub 2's default password is outlined. The initial step involves identifying the type of hash obtained during the reconnaissance phase, using the "Hash-Identifier" tool.

In the "Weaponisation" stage, the second stage of the Kill Chain methodology, the "Hash-Identifier" tool is employed to analyse cryptographic hashes to deduce the hashing algorithm likely used to create them.

In figure 6.3A present a list of hash values, matching the format and characteristics of the observed hash. The analysis indicates that the hash in question could be SHA-256. This identification is crucial for tailoring the attack to be more effective, allowing for the password to be cracked with tools like John the Ripper.

Figure 6.3A List of hash values

The fourth stage, "Exploitation," is utilised to crack the default password of the BT Smart Hub 2 using John the Ripper, an open-source password cracking tool, used to identify weak passwords by employing various cracking techniques. It uses common algorithms such DES, MD5, Blowfish, SHA1, SHA224, SHA256 and SHA512. In this section John the Ripper operates using dictionary attack, the most common file “rockyou.txt” having 14,341,564 unique passwords. The hash has been stored in a file called defaultpassword.txt and was launched by the command –format=raw-sha256. This command tells John the Ripper to identify the hash, and the –wordlist=rockyou.txt which allows John the Ripper to use the dictionary attack to find the password.

John the Ripper used the default input encoding UTF-8 to be interpreting the input files as being encoded in UTF-8 which is a standard text encoding.

The figure 6.3B demonstrates that the default password was not successfully discovered through the dictionary attack, as the rockyou.txt file does not contain the router's default password.

Figure 6.3B Default password crack attempt

Aircrack-ng (SKY)

Figure 6.4.1 shows a screenshot of the results of running the Aireplay-ng command, part of the Aircrack-ng toolkit designed for testing the security of networks. This command is being used to carry out a de-authentication attack on a wireless access point. The ISP router, identified by its BSSID 80:xx:xx:xx:xx:62, operates on channel 6. The de-authentication attack represents a form of attack known as denial-of-service (DoS), where the goal is to disrupt the network's normal

operations. This attack involves sending de-authentication packets over and over to the network's broadcast address. This action suggests an attempt to sever the connection of all devices linked to the ISP router. The mention of 'code 7' in the details of the attack is a specific indicator used by an access point (AP) to signal to a device that it has been forcefully disconnected from the network. This code essentially serves as a notification to the client that they have been de-authenticated.

Each line is marked with a timestamp that represents an instance where the Aireplay-ng tool has sent a de-authentication packet to the broadcast address on the network. This is typically done to force clients to reconnect, allowing the attacker to capture the handshake process which can then be used to try to crack the network's encryption key. The output explains that the de-authentication attack is more effective when targeting a specific connected client, using the -c option followed by the client's MAC address. This is because the attack can be more directed and can reduce noise on the network, increasing the chances of capturing the necessary data without causing unnecessary disconnections to other devices.

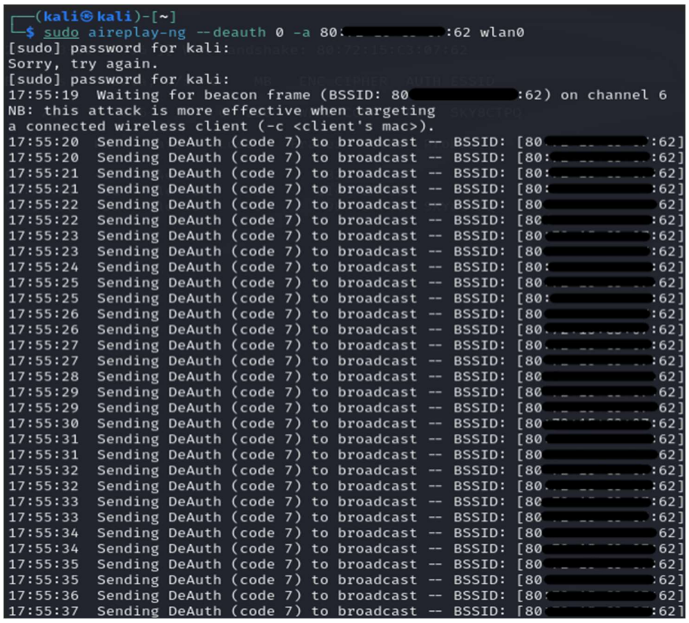


Figure 6.4.1

Figure 6.4.2 shows a view of a wireless network and its connected clients. Figure 8 shows the captures of the wireless access point, identified by the BSSID 80:xx:xx:xx:xx:62, which serves

as a distinctive hardware identifier within the network infrastructure. The signal strength, denoted by PWR, is strong at -62 dBm, suggesting that the monitoring tool is close to the access point. This access point transmits at a high rate, as evidenced by 690 beacon frames and 219 data packets, indicative of a busy network. Operating on channel 6, the network boasts a maximum throughput of 260 Mbps and employs WPA2 encryption with a CCMP cipher, authenticated using a PSK method. The ESSID 'SKY8CTPQ' labels the network, and the capture of the WPA handshake signals the possibility of decrypting the network's password.

Figure 8 shows the capture of the four-way handshake, the client's devices connected to the network through their respective MAC addresses. The signal strengths of these clients vary, with the strongest being -29 PWR indicating a close and likely reliable connection to the access point. The transmission rate for these clients appears low, which could suggest a variety of conditions including power-saving modes or potential inaccuracies in data reporting.

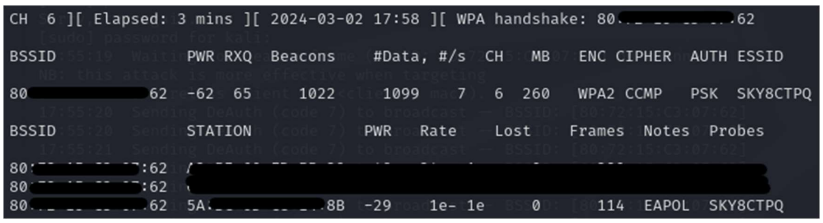


Figure 6.4.2 wireless network and its connected clients

Figure 6.4.3 shows that Aircrack-ng performing a dictionary attack, trying to crack a WPA key. Despite using the "rockyou.txt" file as a source for potential passwords through the command aircrack-ng test1.pcap -w /home/kali/rockyou.txt, it's important to note that the "KEY NOT FOUND" message indicates that the attempted cracking has not been successful. The negative time shown for completion suggests a software error and the need for further investigation into the tool's functionality. The unsuccessful attempt shows that the actual password may not be present in the dictionary file used. Future efforts should ensure the integrity of the handshake file and consider a broader set of passwords for testing.

Figure 6.4.3 Aircrack-ng performing a dictionary attack.

6.4 Reconnaissance Phase 2 (Password Reconnaissance OSINT)

In the initial planning phase of this assessment, the researchers conducted research into the use of default and non-default passwords. To do this they reached out to the public via social media to gain an understanding of the procedures the average person uses when initiating their wireless connections at home. 6.5.1 shows the most common replies to the questionnaire that was given to the public via social media this is because some of the replies are the same. For full questionnaire answers please refer to Appendix A.

Questions Asked	Answers Given
Have you ever changed the default password and username for your router's admin interface?	• Yes, to a long and complicated password. • Yes, I have repeatedly changed the password provided by the administrator interface of my route. • I have, but I followed a step-by-step guide on how to do it and can't remember how to off top of my head. • No, I've never changed it. It's always been kept the same.
How secure do you feel your home network is from hackers?	• More secure than the average home.

	• While the network is not initially secure, I have enhanced its security by implementing additional measures. • Above average(security software and configuration) although has not been put to test as it's not targeted. • Kinda secure, personally never been the victim of hackers yet but know it's a very real possibility. • Quite vulnerable. • Not as secure as it could be
Do you use your home network primarily for personal use, or do you connect work devices to it?	• Mostly personal use, but will use work-related applications when necessary, such as when someone needs a shift changed last minute. • Both, but have segregation between them. • Personal use. • Personal and education.
If you could only choose one, would you prioritise security or ease of access for your Wi-Fi router?	• Prioritise security. • Security for sure. • Security. My Wi-Fi passwords are ridiculously hard to input. • I'm not sure, I would like to think I would prioritise security if I had to choose.
Do you connect to your Wi-Fi using the default password provided by your internet service provider (ISP)?	• No, never. • Changing default password first. • Yes • I think I do use the default password lol.

Figure 6.5.1 Public feedback

In conducting this research, they found that 10 out of 14 as displayed in Figure 6.5.1 would change from the default password to a more memorable and personalised password indicating the need to demonstrate the use of common passwords as an attack vector. To find these common passwords and create an impartial approach, the researchers divided their resources for each router to create a password, each researcher had their methodology to determine the passwords which can be viewed in the following sections.

6.5 SKY

Figure 6.6.1 shows that the CyberPilot website, lists "chocolate" as one of the "positively loaded words and phrases" that are commonly used in passwords. Words like these are chosen because they are easy to remember and have positive connotations, but this also makes them vulnerable to dictionary attacks, as they are often included in lists used by attackers to guess passwords. A Python script was created to generate a password from the rockyou word list, specifically including the word "chocolate", which would search through the file to generate a password with the word “chocolate”. The Python script granted the password “chocolate95”. Which was used to change the password for the sky router.

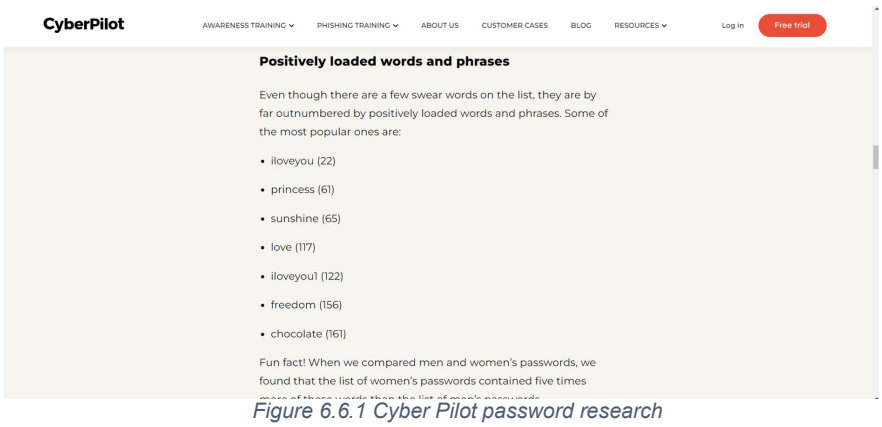


Figure 6.6.1 Cyber Pilot password research

6.6 BT Smart Hub 2

As illustrated in figure 6.7.1 which features the Pink Connect website, which reveals the most common passwords used in the UK in 2022. It highlights that many individuals continue to use passwords related to football teams, with "liverpool" being a specific example. Such passwords, despite being easily memorable for users, are still found in compromised password databases like the rockyou word list, indicating a preference for easily remembered but insecure passwords. The password chosen by the team it was “liverpool123456” from rockyou word list.

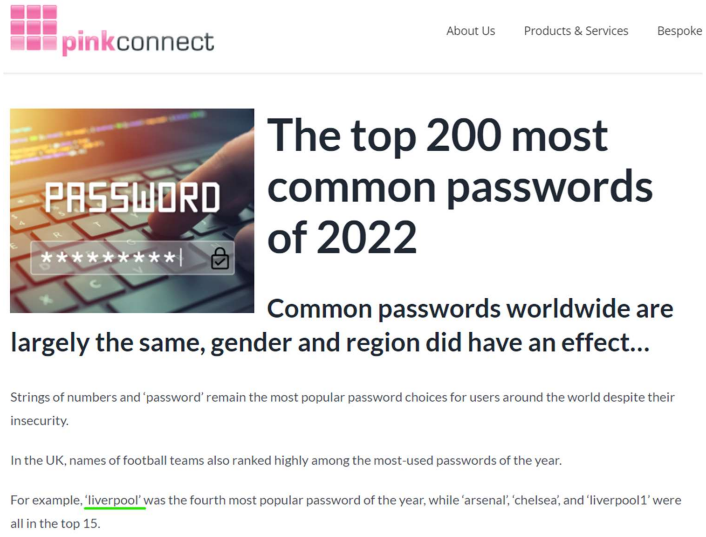


Figure 6.7.1 Pink Connect Password research.

6.7 Virgin Hub 3

A google search relating to the most used passwords led to the discovery that the greatest number of users in the UK use passwords relating to a football team and the most common of those is Liverpool as seen in Figure 6.8.1.

Figure 6.8.1 Google password research

Following on from this a python script was created (Figure 6.8.2)which would search the rockyou wordlist for any passwords relating to Liverpool which meet the minimum criteria for the router, the group then selected one at random as seen in figure 6.8.3 and set this as the Wi-Fi password as seen in Figure 6.8.4.

```python
import re

def get_words_containing(file_path, substring):
    with open(file_path, 'r', errors='ignore') as file:
        # Filter words containing the substring
        words = [word.strip() for word in file.readlines() if re.search(substring, word, re.IGNORECASE)]
        return words

file_path = '/usr/share/wordlists/rockyou.txt'
substring = 'liverpool'
words_containing_liverpool = get_words_containing(file_path, substring)

```

Figure 6.8.2 Python password script

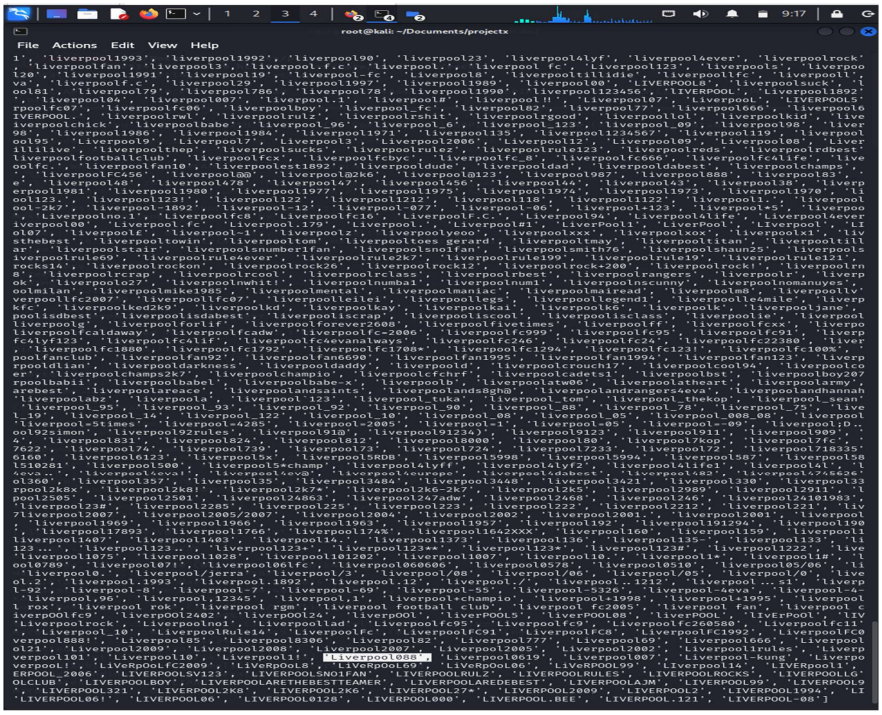


Figure 6.8.3 Random password selection.

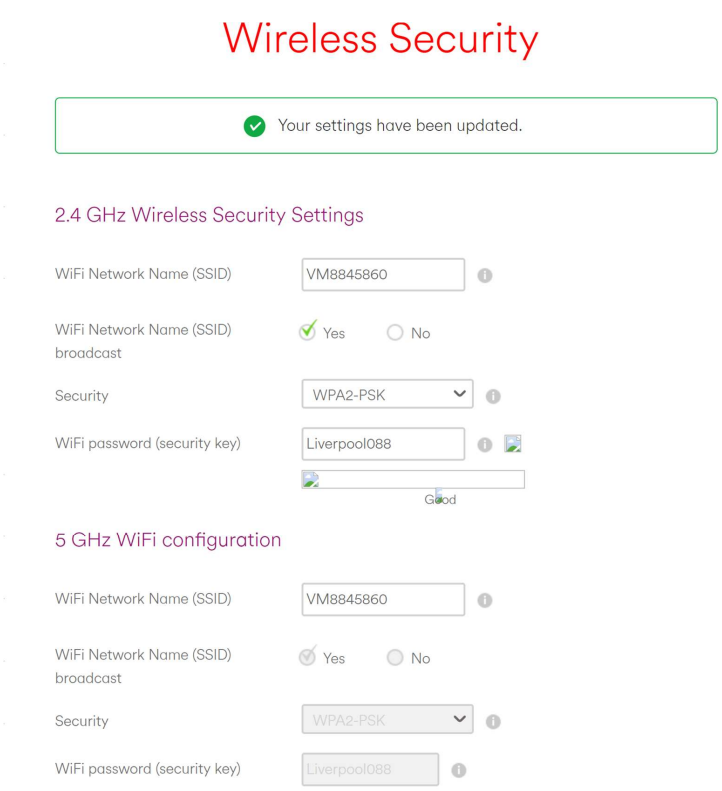


Figure 6.8.4 Setting virgin hub password

6.8 Dictionary Attack Phase 2 User Generated Password

Hashcat and rockyou (Virgin)

After capturing the EAPOL frames containing the PMKID, the researchers proceeded to convert the captured data using Hashcat's online conversion facility. This step involved transforming the captured PMKID into a format suitable for offline password cracking.

The researchers the utilised Hashcat's powerful password cracking capabilities and the extensive RockYou wordlist, the researchers initiated an offline brute-force attack against the captured PMKID to recover the original passphrase as seen in Figure 6.9.1. Remarkably, the password cracking process was completed in under 10 seconds showing how easily a commonly used password can be cracked using openly available tools.

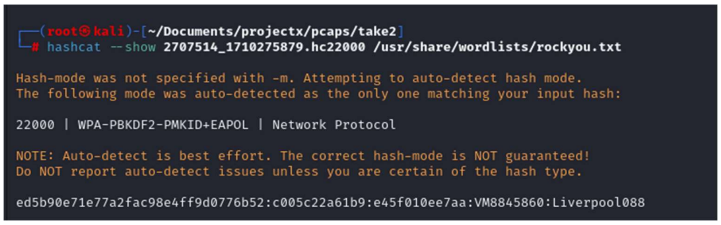


Figure 6.9.1 Virgin media dictionary attack

Aircrack-ng and Rockyou (SKY)

Figure 6.9.2 shows that that Aircrack-ng was used for a dictionary attack against a WPA-secured network, using the command aircrack-ng test2.pac -w /home/kali/rockyou.txt. This specifies that the test2.pac file, which likely contains captured network traffic including the WPA handshake, was tested against the passwords listed in the rockyou.txt file. The successful outcome is denoted by the discovery of the password "chocolates95", the vulnerability of the network to this kind of attack when a weak passphrase is used.

Figure 6.9.2 Aircrack-ng Dictionary attack

Dictionary Attack john the ripper and Rock you (BT)

Following the selection of the password recommended by the Pink Connect website, the "Exploitation" phase was revisited using John the Ripper.

Once the file reading process concluded, it displayed the number of password hashes loaded into the hash256.txt file. The details provided in brackets indicated the type of hash to be cracked and the use of a CPU with AVX512BW capabilities.

The output as seen in figure 6.9.3 confirmed the session's completion and the successful cracking of the hash. The password "liverpool123456" was identified as the compromised password in this instance.

```
┌──(root㉿claudio)-[/home/claudio/Documents]
└─# john --format=raw-sha256 --wordlist=rockyou.txt hash256.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA256 [SHA256 512/512 AVX512BW 16x])
Warning: poor OpenMP scalability for this hash type, consider --fork=8
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 1 candidate left, minimum 128 needed for performance.
0g 0:00:00:00 DONE (2024-03-17 15:37) 0g/s 100.0p/s 100.0c/s 100.0C/s liverpool123456
Session completed.
```

Figure 6.9.3 Dictionary attack using john the ripper.

7. Remediation

In response to the vulnerabilities identified within the WPA2 protocol, the project team has taken significant steps to enhance the security and reliability of the wireless network infrastructure. Their approach centres on the implementation of WPA3, the latest advancement in wireless security protocols, unveiled by the Wi-Fi Alliance in 2018. WPA3 represents a significant enhancement over WPA2, introducing a host of security improvements aimed at bolstering network security through advanced authentication, encryption, and integrity protocols.

Central to this initiative is the innovative deployment of OpenWrt on Raspberry Pi devices. OpenWrt, with its Linux-based, open-source standard, offers an alternative to standard manufacturer firmware, granting unparalleled control and customisation over networking hardware. Its compatibility with Raspberry Pi, a compact and cost-effective computing platform, facilitates a customizable, highly functional wireless network environment, perfectly suited for the implementation of WPA3 protocols.

The Raspberry Pi's robust processing capabilities, coupled with Openwork's flexibility, empowers the team to enhance network security significantly. This setup not only facilitates the

adoption of WPA3's cutting-edge security features, such as Simultaneous Authentication of Equals (SAE) and advanced encryption standards (AES), but also offers the versatility to tailor network firmware, ensuring resilience against emerging cyber threats.

WPA3's introduction is a cornerstone of the team's security strategy, offering rigorous protection mechanisms against the vulnerabilities of its predecessor, WPA2. Notable among its features is the implementation of SAE, which mitigates the risk of offline dictionary attacks by necessitating interaction with each authentication attempt, thereby rendering brute-force attacks more challenging. Furthermore, WPA3 employs AES in CCMP-128 for personal networks and GCMP-256 protocols for enterprise networks, significantly enhancing data security. CCMP-128, based on AES encryption with a 128-bit key, is a standard for personal networks offering robust security. GCMP-256, using Galois/Counter Mode with a 256-bit key, based on WPA3 security protocol, provides enhanced encryption for enterprise networks, ensuring higher security levels against sophisticated attacks.

By leveraging elliptic curve cryptography (ECC) for the SAE handshake, WPA3 ensures a secure exchange of cryptographic parameters between the client and access point, establishing a shared secret without airborne transmission. This method not only safeguards against eavesdropping and dictionary attacks but also facilitates the independent computation of a Pairwise Master Key (PMK) by both parties. This PMK is then used to derive dynamic encryption keys, ensuring the integrity of each session.

The adoption of WPA3 through OpenWrt on Raspberry Pi dramatically advances wireless network security, providing robust encryption and authentication measures while mitigating potential security risks. This approach introduces forward secrecy, protecting past transmissions even if a current key is compromised, and incorporates Wi-Fi Easy Connect for simpler device additions to the network. For enterprise environments, WPA3-Enterprise offers a comprehensive 192-bit security suite, ensuring the secure transmission of sensitive and classified data.

The global transition to WPA3 signifies a significant leap forward in securing digital communications, effectively addressing vulnerabilities inherent in previous protocols and future-proofing networks against evolving cyber threats. This strategic implementation not only enhances the cybersecurity posture worldwide but also demonstrates the project team's commitment to continuous improvement and adaptation in the ever-changing landscape of network security.

In this section the project team has successfully executed the deployment of OpenWrt on a Raspberry Pi 4, aimed at elevating the network's infrastructure to new heights of performance and security. In this stage it will shows the counter measure provided by the integration of OpenWrt with the Raspberry Pi 4 setup.

In figure 7.1 it shows the Raspberry Pi model employed as a countermeasure in the network's security strategy.

Figure 7.1 Raspberry pi router (openwrt)

This table outlines the materials and steps involved in configuring OpenWrt on the Raspberry Pi hardware, used to the project team.

Hardware	Software
Raspberry Pi 4 B with power supply	openwrt-23.05.0-bcm27xx-bcm2711-rpi-4-squashfs-factory.img
RJ45 Ethernet capable	Raspberry PI Imager
SD card 8GB minimum	

Figure 7.2 Router hardware table

After Openwrt has been deployed figure 7.3 shows Openwork's web interface after a successful login, Details about the system is shown, such as the hostname being "OpenWrt," the model as a Raspberry Pi 4 Model B Rev 1.4, and various software versions and statuses. Memory usage is detailed, showing a total available memory close to 7.64 GB. The group navigate to the 'Wireless' section, accessible via the 'Network' dropdown menu, where they will have the option to activate the wireless adapter and configure wireless security, including the WPA3 protocol.

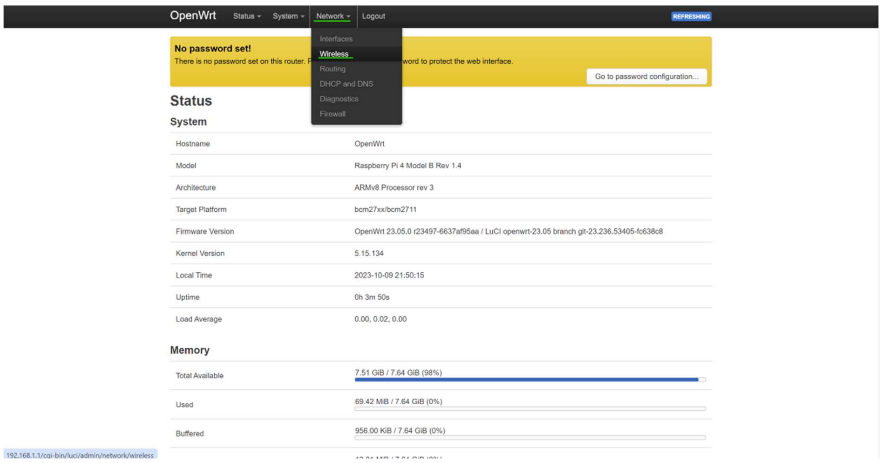


Figure 7.3 OpenWrt Gui

Figure 7.4 shows that the wireless network interface, named Cypress CYW43455 and supporting the 802.11ac/b/g/n standards, is shown as "not active" and the SSID, "OpenWrt," is

as disabled. For the device to broadcast the SSID and become visible to other devices for wireless connectivity, the group will enable the wireless function by clicking the "Enable" button.

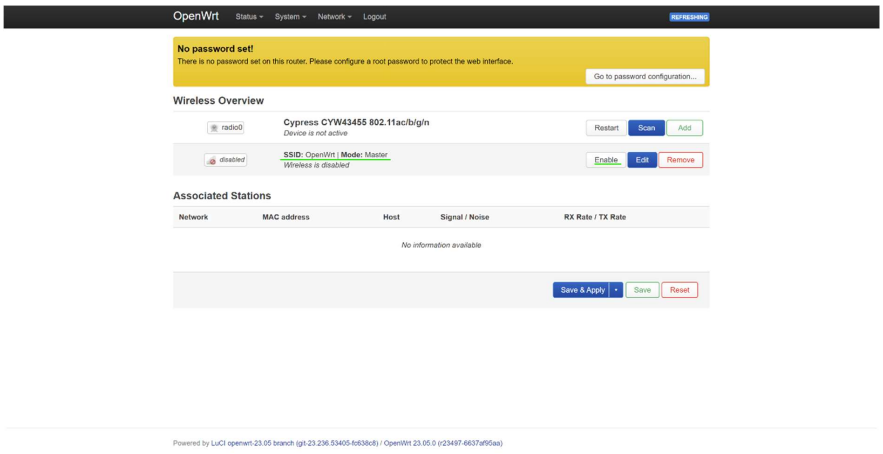


Figure 7.4 OpenWrt configuration

Figure7.5 shows that a device with WPA3 compatibility has connected to the OpenWrt access point. The device is "Connected" to the network named "OpenWrt." It is set to automatically reconnect whenever it's within range of this network. The network's signal strength is excellent at -46 dB, and the link speed is reported as 325 Mbps. The security section confirms the use of WPA3-Personal, this proves that the device is using the latest WPA3 security protocol for a secure connection.

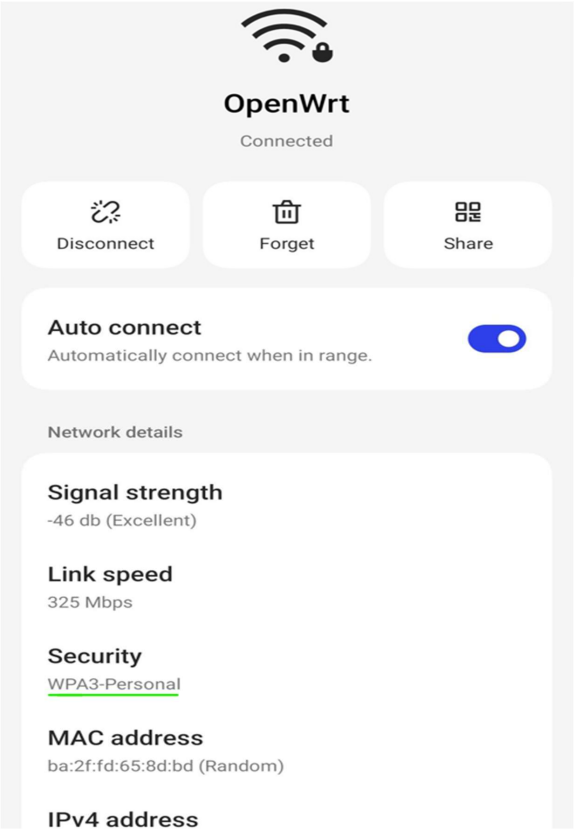


Figure 7.5 Connection to WPA3

Testing OpenWrt

Upon completion of the remediation process, considerable security enhancements have been deployed across the network infrastructure, the aim of the project is to provide WPA3 security improvements introduced with this protocol, make it significantly more resistant to the types of attacks. The team its follow-up assessments will be carried out to ascertain whether vulnerabilities have been mitigated or entirely eradicated.

In accordance with the team it will be conducted a pen testing simulations, with emphasis on examining wireless security, testing approaches will be applied without an extensive explanation of the underlying reasons, concentrating instead on the results.

Wireless Penetration Testing

In order to replicate the prior testing, the same strategy will be employed, utilising tools such as Kismet, Aircrack-ng, Pwnagotchi, and Flipper Zero.

Kismet

The simulation will begin with Kismet trying to detect networks. The figure 7.6 illustrates that Kismet has identified the network named 'OpenWrt' which is secured using the WPA3 protocol. The figure also demonstrates that capturing the 4-way handshake, which was previously possible during the reconnaissance stage with WPA2, is not feasible with WPA3's enhanced security measures.

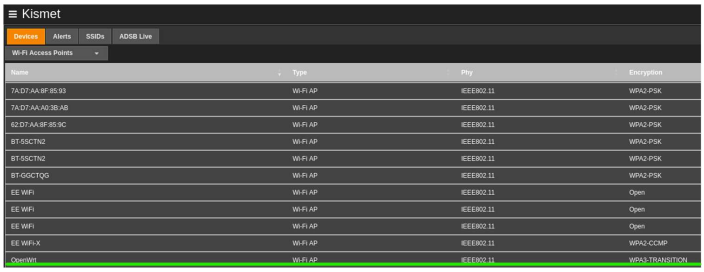


Figure 7.6 Security testing WPA3

In this figure, the researchers corroborate their previous discussions on the workings of WPA3 by examining its security enhancements, specifically through the lens of Kismet's inability to intercept the 4-way handshake. This limitation arises due to the deployment of the WPA3 SAE protocol, a successor to the WPA2's PSK exchange mechanism. As mentioned, SAE introduces a more secure handshake protocol, Offering a more robust defences against offline dictionary attacks. This advancement proves the integrity of session keys, even in scenarios where long-term keys might be compromised, with each session key being distinct and not reliant on a static, long-term key. Consequently, intercepting a single session's key does not jeopardise the security of other sessions.

The challenge in circumventing Forward Secrecy under WPA3 lies with Kismet's inability to capture the 4-way handshake stemming from the use of unique encryption keys for each session between a device and the Access Point. Should an attacker succeed in decrypting the encryption key for a session, this breach would not facilitate the decryption of any preceding or subsequent sessions. Given that each session key is ephemeral and not derived from a master key, it eliminates a singular point of failure. As such targeting a master key to decrypt all traffic becomes an unviable strategy for attackers.

Adding to challenges presented by the tools used, the SAE protocol presents a secure password-based key exchange mechanism that significantly mitigates the risk of offline dictionary attacks. Upon connecting to a Wi-Fi network, a device initiates the SAE exchange by dispatching a commit message to the access point. This message does not contain the actual password but employs cryptographic functions to which the access point responds with its commit message.

Both the client and the access point then independently calculate a cryptographic value, known as the Password Element (PE), through complex mathematical operations within a finite cyclic group known as an elliptic curve group, ensuring that the derived values are impervious to attacks.

Following the exchange of commitments, both parties generate a confirmation message comprising a cryptographic hash that encapsulates the commits and the derived PE. Each side sends its confirmation to the other, whereupon receipt, they verify that the received hash corresponds with their computed hash. Successful mutual authentication leads to the utilisation of the derived PE to forge the PMK facilitating secure communications. With the establishment of session keys, the devices and the access point can now engage in encrypted communication, underscoring the formidable security provisions inherent in WPA3.

8. Conclusion

In conclusion, the researchers discovered that ISPs deploy routers operating on a vulnerable protocol as the highest form of wireless security but mitigate this vulnerability by providing uncrackable default passwords. While default SSIDs clearly displaying the ISP's name may serve as easily identifiable attack vectors, users who retain default credentials are presently protected from password cracking attempts with tools accessible to the public.

As part of this project the researchers also compiled an educational supplement providing a walk through guide on how to carry out a security assessment of home routers which operate using the WPA2 security protocol, this is also complimented by the creation of an interactive website that can teach users how to both secure and test their home wireless environments, excerpts of which can be viewed in the appendices, titled appendix B and C.

The researchers suggest that the end user plays a pivotal role in creating an environment vulnerable to WPA2 exploitation by opting for easily crackable passwords. To mitigate the vulnerability in WPA2, the deployment of custom access points is recommended. While this may require a significant leap in technological awareness for end users to implement, ISPs could alleviate this barrier by providing such devices at a nominal cost.

Although numerous tools exist for compromising the security of wireless protocols in home networks, the researchers commend ISPs for their due diligence in deploying routers with uncrackable passwords. However, they caution end users against changing default passwords to more memorable ones, as this introduces unnecessary flaws in their home network security. If users opt to change from the default password, it is imperative that they select passwords of at least 16 characters in length and avoid commonly used words.

By adhering to these recommendations, end users can bolster the security of their home networks and reduce the risk of unauthorised access and data breaches.

Appendices

Appendix A – Public Q&A

This is the full complete question and answers form that was given to the public via social media.

Questions Asked	Answers Given
Have you ever changed the default password and username for your router's admin interface?	• Yes, I have. • Yes, to a long and complicated password. • Yes, I have. • Yes • Yes, I did, immediately. • Yes • No • Yes, I have repeatedly changed the password provided by the administrator interface of my route. • Yes - forth Valley police. • No. • Yes. • Yes. • I have, but I followed a step by step guide on how to do it and can't remember how to off top of my head. • No, I've never changed it. It's always been kept the same.
How secure do you feel your home network is from hackers?	• More secure than the average home. • Judging by the amount of dropped packets in my logs, I'm secure enough for now but someone is going to get through eventually. • More secure than the average home • On the scale 1-10(2 on the security measures taken by isp and 8 if I secure it via vpn and other. • While the network is not initially secure, I have enhanced its security by implementing additional measures. • Above average(security software and configuration) although has

	not been put to test as it's not targeted. • Quite vulnerable. • If a hacker wants to enter my network, he thinks I know ways to do it since I don't have special software to protect myself. • Not as secure as it could be. • No probably not as secure as it can be. • Not at all. • Good • Kinda secure, personally never been the victim of hackers yet but know it's a very real possibility. • Pretty secure. It's a completely randomised password that no one would be able to guess.
Do you use your home network primarily for personal use, or do you connect work devices to it?	• Both. • Mostly home use and some school. • More secure than the average home. • Both. • Both cases. • Personal and education. • Connect work devices such as tablet/laptop. • Network use for private use only. • Personal use. • Personal use/ • Private + work • Both but have segregation between them. • Mostly personal use, but will use work related applications when necessary, such as when someone needs a shift changed last minute 😅. • Pretty much just use it for personal use. Not got a work device.
If you could only choose one, would you prioritise security or ease of access for your Wi-Fi router?	• Prioritise security. • Security. I've already made this choice, my family hates my password policy 😂 • In the past it would be ease of use, but I understand the huge increase of cybercrime so think my view is shifting.

	• Prioritise security. • Security for sure. • Security. • Security. • give priority to safety. • Deffo security. • Ease for laziness. • Ease. • Security. My Wi-Fi passwords are ridiculously hard to input. • Security. • I'm not sure, I would like to think I would prioritise security if I had to choose.
Do you connect to your Wi-Fi using the default password provided by your internet service provider (ISP)?	• No. • No, never. • No. • I used to change it, but I haven't since I started using a Wi-Fi 6 modem. • Changing default password first. • No. • Yes. • No, I changed the password. • Nope was changed ASAP • Yeah • No. • No. • No, changing default first thing we did when getting a new router. • I think I do use the default password lol.

Appendix B - Website

Website address

https://wrobe.github.io/set08101/?fbclid=IwAR12VF1sEzTALVvyprWxIRhW5Ld4Gt7yJtEX0Vv9Zll2F3HJoViZYrlqZ_w_aem_AZvelHmHGsdNctUFrXMAeaEZfaUO96_2AEoEbagoAmNq3Z8dNOLo5fsM1m4G4Irm-6ZXWl70V7RlO8kVeRmUuT31

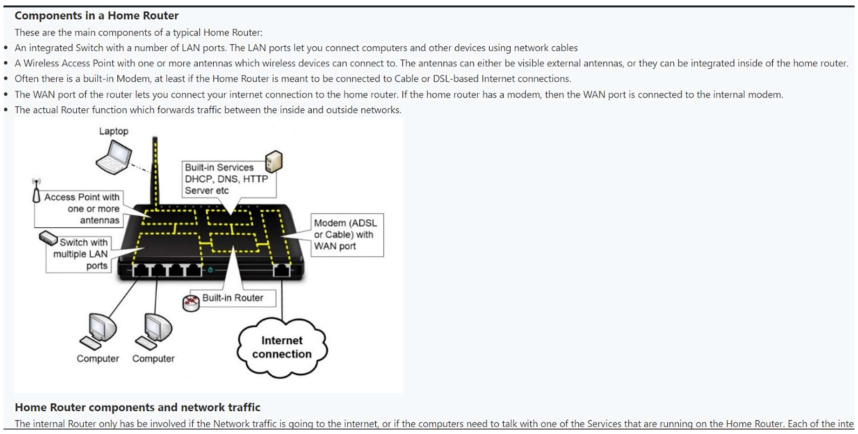
Documentation

Secure Your Digital World Platform

Our user-friendly educational tool is designed to assist the public in defending their digital presence. This portal offers straightforward guidelines and interactive materials, making it accessible even to individuals without technological knowledge. It covers essential topics such as home network foundations, Wi-Fi router security, and password strength. Users can confidently learn how to secure their home networks, from creating strong passwords to configuring secure routers and even building a secure router themselves. Each website component was designed with security in mind.

Basic Networking

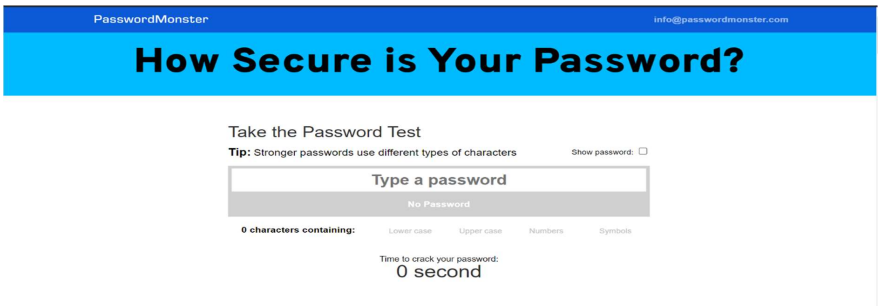
This section is an essential tool for anybody wanting to learn the fundamentals of home network security. It provides the basis by explaining essential ideas and terminology, allowing users to grasp better how home networks work. The material is intended to clarify complicated concepts, such as the distinctions between different types of network connections and the function of routers and their components.



Password Strength Checker

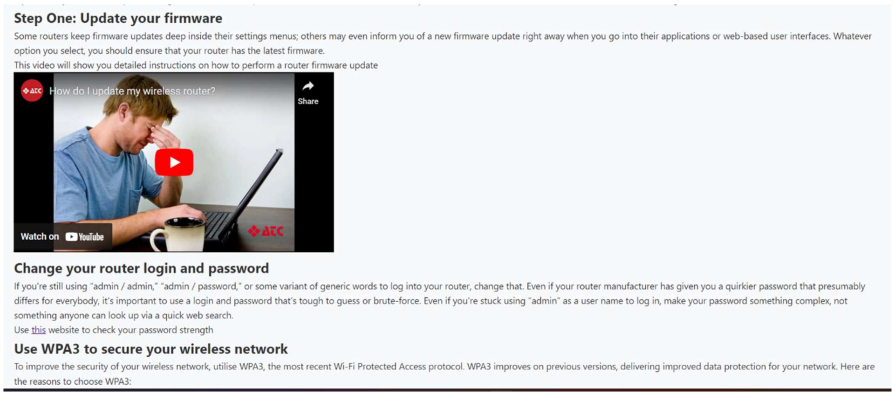
The Password Strength Checker is an interactive application on the site that provides users with quick insight into the security quality of their passwords. By inputting a password into this tool, users may quickly evaluate how solid or vulnerable their password is to typical hacking tactics like brute force and dictionary attacks. This feature assesses the password using various criteria, including length, difficulty, and the usage of various characters (letters, digits, and symbols).

Furthermore, the tool educates rather than simply assessing. After reviewing a password, it provides helpful recommendations for improving it, such as extending the length or using a more diverse mix of characters. This fast, personalised input is crucial to users to help in creating robust passwords.



Secure Your Home Router Guide

The "Secure Your Home Router Guide" was deliberately created to be helpful to those who may not be very tech-savvy. This tutorial provides extensive instructions in a clear and user-friendly manner, allowing even novices to protect their home networks confidently. To improve comprehension and ensure that instructions are clear, the guide includes visual features such as infographics, which provide quick insights into complicated issues, and screenshots, which provide step-by-step visual clues on how to conduct certain activities. These visual elements are critical for simplifying technical procedures and allowing people to follow along and adopt the instructions. Whether changing default passwords, upgrading firmware, or adjusting security settings, this guide simplifies the process and makes digital security accessible to everyone.



Build Your Own Secure Router

"Build Your Own Secure Router" is a specialised section of our site targeted at individuals with technical backgrounds. This section includes detailed instructions on how to use the features of OpenWRT, a highly customisable open-source firmware installed on a Raspberry Pi. By following these step-by-step instructions, users can significantly enhance the security of their network while also gaining access to a variety

of sophisticated capabilities. The article covers everything from the Raspberry Pi's initial setup, including the required hardware components, to the entire procedure of installing OpenWRT. It also goes into detail on configuring the system to match individual security needs and preferences, allowing users to build a strong, secure, and efficient home network.

DIY Raspberry Pi Router with OpenWRT

To enhance website accessibility, a QR code was created and widely distributed as a sticker. This solution lets users rapidly access the platform by scanning the code with their mobile phones. These stickers will be available in various public places, community centres, and electronics stores, allowing anybody to quickly access essential information for securing their digital life. This strategy streamlines the process of accessing our educational platform and promotes wider involvement and an understanding of digital security.

Appendix C -Educational supplement

WPA2 Exploit Walkthrough and open WRT deployment

Disclaimer

All activities performed in this walkthrough are performed on authorised equipment owned by the writer. Do not target unauthorised equipment. Do not use this walkthrough for illegal purposes, it is purely for educational purposes.

Introduction

Wireless routers in home networks use an authentication scheme to allow for users to enter a password and gain access to the network (Wi-Fi). The mechanism used is commonly WPA2 despite WPA3 being available as older hardware is not compatible. Despite this, WPA2-PSK has an inherit security weakness that binds security to the length and complexity of the password used.
The exploitation process that this walkthrough uses involves using reconnaissance to sniff and capture the target wireless network activities and to perform a de-authentication attack to capture the WPA2-PSK handshake. This can be done regardless of how strong the wireless network security is. The hash value used for authentication is then extracted from this capture and cracked locally using a brute force attack involving hashcat and GPUs.
The consequences of this attack are that an attacker can get the password to the wireless network which can then be used to allow them to authenticate and perform further exploitation activities for malicious purposes. Additionally, an attacker could just perform the de-authentication attack to annoy the target and prevent them from using the wireless network.

Requirements

- Working Linux machine (physical or virtual) – Any distro, Kali comes with the packages preinstalled.
- Wi-Fi Adapter
- Authorised WPA2 wireless network

Walkthrough

The first thing that must be done to be able to exploit WPA2 is to perform some reconnaissance upon the wireless network being targeted. There are a plethora of methods that can be performed here, ranging from manual to fully automatic. The one that this walkthrough will explore is a semi-manual process using the Aircrack-ng tool suite.

Before the reconnaissance can start however, the system should be updated to the latest package versions provided by the distribution. The package manager varies but Kali Linux being in the Debain family uses apt.

```
┌──(sysadmin㉿kali)-[~]
└─$ sudo apt update && sudo apt dist-upgrade
Hit:1 http://http.kali.org/kali kali-rolling InRelease
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
All packages are up to date.
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Calculating upgrade ... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

After connecting the Wi-Fi adapter to the Linux machine, the iwconfig program can be used to verify that adapter is working correctly. Some hardware require for additional drivers to be installed and will not work out of the box. The Alfa AWUS036ACH being used for this guide is one of these devices and requires the RTL8812AU driver to allow for the Linux system to interface with the chipset.

```
┌──(sysadmin㉿kali)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.
```

To install this driver, the source code must first be obtained by cloning the git repo from GitHub.

```
┌──(sysadmin㉿kali)-[~]
└─$ git clone https://github.com/aircrack-ng/rtl8812au.git
Cloning into 'rtl8812au'...
remote: Enumerating objects: 11252, done.
remote: Counting objects: 100% (2261/2261), done.
remote: Compressing objects: 100% (209/209), done.
remote: Total 11252 (delta 2110), reused 2053 (delta 2052), pack-reused 8991
Receiving objects: 100% (11252/11252), 70.36 MiB | 3.68 MiB/s, done.
Resolving deltas: 100% (7819/7819), done.
```

Additionally, the system must have the needed development packages that are requirement to compile the driver.

```
┌──(sysadmin㉿kali)-[~]
└─$ sudo apt install bc mokutil build-essential libelf-dev linux-headers-`una
me -r`
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  dpkg-dev libzstd-dev linux-headers-6.6.9-common linux-kbuild-6.6.9
  xz-utils
Suggested packages:
  debian-keyring
The following NEW packages will be installed:
  bc build-essential dpkg-dev libelf-dev libzstd-dev
  linux-headers-6.6.9-amd64 linux-headers-6.6.9-common linux-kbuild-6.6.9
  mokutil xz-utils
0 upgraded, 10 newly installed, 0 to remove and 0 not upgraded.
Need to get 14.9 MB of archives.
After this operation, 70.7 MB of additional disk space will be used.
Do you want to continue? [Y/n] 
```

An interesting note that should be mentioned here is the xz-utils package that's being pulled in a dependency. Andres Freund recently revealed that the most recent development versions of the XZ package contained a backdoor in its library code that some distributions were using with SSH as part of compression functionality. More information can be found by browsing the mail list found here. It was also later identified that this was done by a recent (2ish years) maintainer of the XZ project. Thus, at the time of writing, its unknown if XZ contains other malicious code and should be treated with caution until further notice.
Regardless of the situation, the driver can be compiled by changed into the directory containing the source code (the one that was just cloned using Git) and using the GNU auto tools to handle the compilation process. Note that `make install` may need a higher privilege level and thus may be required to be run with the `sudo` prefix like with previous commands or as root.

```
┌──(sysadmin㉿kali)-[~]
└─$ cd rtl8812au

┌──(sysadmin㉿kali)-[~/rtl8812au]
└─$ make && make install
make ARCH=x86_64 CROSS_COMPILE= -C /lib/modules/6.6.9-amd64/build M=/home/sys
admin/rtl8812au  modules
make[1]: Entering directory '/usr/src/linux-headers-6.6.9-amd64'
  CC [M]  /home/sysadmin/rtl8812au/core/rtw_cmd.o
```

After rebooting, the iwconfig command can be used to verify that the driver is successfully installed, and the wireless card can be accessed.

```
┌──(sysadmin㉿kali)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     unassociated  ESSID:""  Nickname:"<WIFI@REALTEK>"
          Mode:Managed  Frequency=2.412 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

The final task that must be performed before the reconnaissance can start is to switch the Wi-Fi adapter into monitor mode. This is a special state that allows for all wireless traffic within range to be monitored without having to authenticate against the wireless network first. To switch into this state, first airmon-ng can be used to terminate any running processes that may interfere with the operation. Monitor mode can then be successfully enabled using the airmon-ng command against the name of the adapter interface (by default wlan0).

```
┌──(sysadmin㉿kali)-[~]
└─$ sudo airmon-ng check kill

Killing these processes:

    PID Name
   1104 wpa_supplicant


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


PHY     Interface       Driver          Chipset

phy0    wlan0           88XXau          Realtek Semiconductor Corp. RTL8812AU
 802.11a/b/g/n/ac 2T2R DB WLAN Adapter
                (monitor mode enabled)
```

Finally, to begin the reconnaissance the airodump-ng command can be used to listen and list every available wireless network the wireless adapter can reach. This command takes over the terminal and will constantly refresh its results, the q button can be pressed twice to exit back to the terminal.

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

The output from this command can be seen below, with the MAC addresses redacted. As shown, a list of available wireless networks and associated stations (colloquially known as clients). The wireless network that this walkthrough is targeting has been left partially uncensored. The ESSSID (name of the network) can be seen as “VM734980-2G” and the first half of the MAC address (OUI) can be seen as 20:0C:C8. The full MAC address of the target wireless network must be noted as its used in the next steps.

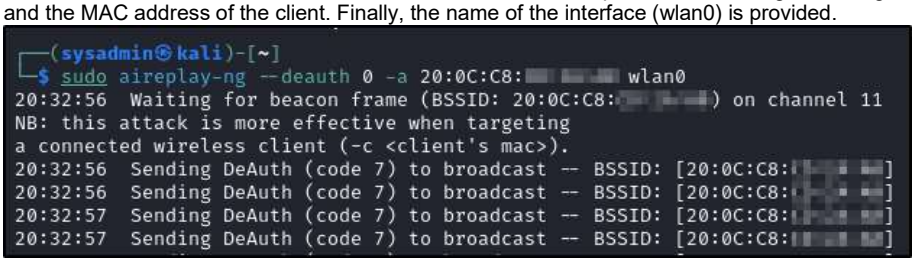
```
BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

[redacted]         -41       71        0    0  11  130   WPA2 CCMP   PSK  [redacted]
[redacted]         -41       70        0    0  11  130   WPA2 CCMP   MGT  [redacted]
[redacted]         -41       76        0    0  11  130   OPN              [redacted]
[redacted]         -38        1        5    0  12  720   WPA3 CCMP   SAE  [redacted]
[redacted]         -34      293        0    0   1  130   WPA2 CCMP   PSK  [redacted]
20:0C:C8[redacted] -33      697       12    0  11  130   WPA2 CCMP   PSK  VM734980-2G

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   [redacted]         -39    0 - 1      0         1
(not associated)   [redacted]         -23    0 - 1      0         2
(not associated)   [redacted]         -33    0 - 1      0        77         [redacted]
[redacted]         [redacted]         -25    0 - 1      0       477
[redacted]         [redacted]          -1    0 - 1      0        70
```

While this is great for browsing, the attack should only happen to the specific target network. To make the results clearer, airodump-ng can be honed in on specific characteristics. By default,

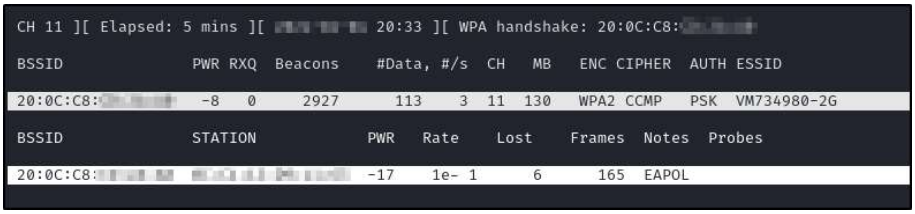
this program will iterate through all available channels, but as the target network's channel is known (11 – can be seen under the "CH" column in the previous screenshot) and can be specified using the -c flag. Additionally, the –bssid flag is being used to only view the target wireless network by its MAC address that was previously recorded in the last step. Finally, the -w flag followed by "capture" is using to record the findings to disk in a file called "capture". Any text can be used here.

As shown below, only the target network and its clients (only one connected) can be seen.

The next stage is to de-authenticate the client so that it reconnects back to the wireless router and performs its WPA2 handshake authentication in the process. This will allow for airodump to intercept the handshake for later cracking. To perform this attack, the aireplay-ng command can be used with the –deuath parameter set to zero. This just means that a de-authentication attack will be occurring. The -a parameter is used to specify the MAC address of the wireless router that was previously noted. This allows for the attack to be carefully targeted and not involve unauthorised wireless networks. This can be further refined to specific clients using the -c flag and the MAC address of the client. Finally, the name of the interface (wlan0) is provided.

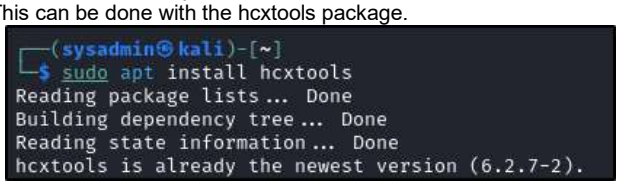


After the client is disconnected and reconnects, ensure that the de-authentication attack is stopped or else it will continue endlessly. Navigating back to the airodump output, successfully capture of the handshake can be verified by the "WPA handshake" followed by the routers MAC address.



With the WPA2 authentication handshake captured, it can be cracked locally. However, the time needed to crack the password is inherently related to its strength. A password that uses lowercase, uppercase, special characters, and digits while also being 12-14 characters will take an improbable amount of time to crack and is probably not worth the money spent on the computation needed. Alternatively, a dictionary attack could be used if its known that the password isn't a randomised garbled mess of characters but instead some kind of word.
For demonstration purposes, the captured handshake contained a default password that was eight lowercase characters in length. The cracking process will show how long it take for this particular instance, but in reality, will be longer for recent WPA2 networks as ISPs are most likely increasing the default security of their passwords.

Before this can be cracked, the capture needs to be converted into a format that hashcat understands. This can be done with the hcxtools package.



Using the provided hcxpcapngtool provided by this package, the capture can be specified and extracted into a new specified file using the -o flag followed by its name. This file can then be used in hashcat's processing.

The method of cracking shown next uses a singular instance of a Nvidia H100 GPU from Paperspace with hashcat running on top of it. This is a highly optimised program that can be used for cracking hashes such as the one captured by the WPA2 handshake. Particularly, hashcat has mode 22000 otherwise known as WPA-PBKDF2-PMKID+EAPOL for cracking WPA2 authentication hashes. This can be seen below selected with -m flag. This is followed by the name of the file that contains the WPA2 hash. The -w 3 will increase the workload profile from the default and make hashcat run faster at the expensive of other programs, however as this is the only important program being executed its fine. The -a 3 flag indicates this is a brute force attack followed by the hashcat mask that helps cut down on time. This mask is eight sets of ?l, this indicate a singular lowercase character. Together this indicates that the hash is being crack into a password for eight characters. If it's known that the wireless router uses a different default password, then a different mask should be used that reflects that.

```
paperspace@psev4x72xxhd:~/hashcat-6.2.6$ ./hashcat.bin -m 22000 hash.hc22000 -w 3 -a 3 ?l?l?l?l?l?l?l?l
hashcat (v6.2.6) starting

* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
* Device #2: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
nvmlDeviceGetFanSpeed(): Not Supported

CUDA API (CUDA 12.2)
====================
* Device #1: NVIDIA H100 80GB HBM3, 80483/81230 MB, 132MCU

OpenCL API (OpenCL 3.0 CUDA 12.2.147) - Platform #1 [NVIDIA Corporation]
========================================================================
* Device #2: NVIDIA H100 80GB HBM3, skipped

Minimum password length supported by kernel: 8
Maximum password length supported by kernel: 63

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Brute-Force
* Slow-Hash-SIMD-LOOP

Watchdog: Temperature abort trigger set to 90c

Initializing backend runtime for device #1. Please be patient...
```

Finally, as shown below, hashcat will crack the hash and reveal the password within 30 hours. Although this wasn't carried out to completation, the cost can be calculated for cracking this hash. The paperspace H100 instance costs $6 per hour, over 30 hours is $180. This is a lot of money to the individual, but perhaps not so in the grander scheme of things. For instance, this $180 dollars can be used to gain the password and connect to the wireless network which could then be used for further exploitation and malcious activities.

```
Session..........: hashcat
Status...........: Running
Hash.Mode........: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target......: hash.hc22000
Time.Started.....: Thu Mar 14 22:48:09 2024 (13 secs)
Time.Estimated...: Sat Mar 16 05:06:31 2024 (1 day, 6 hours)
Kernel.Feature...: Pure Kernel
Guess.Mask.......: ?l?l?l?l?l?l?l?l [8]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1914.1 kH/s (69.86ms) @ Accel:8 Loops:1024 Thr:512 Vec:1
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 23789568/208827064576 (0.01%)
Rejected.........: 0/23789568 (0.00%)
Restore.Point....: 540672/8031810176 (0.01%)
Restore.Sub.#1...: Salt:0 Amplifier:18-19 Iteration:3072-4095
Candidate.Engine.: Device Generator
Candidates.#1....: wehgline -> wibhrerd
Hardware.Mon.#1..: Temp: 44c Util:100% Core:1980MHz Mem:2619MHz Bus:16

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit => s
```

Remediation

Introduction

This introduction to remediation using OpenWRT with WPA3 protocol will delve into the specifics of how these technologies work together to safeguard digital communications. We will explore the benefits of upgrading to WPA3, the challenges involved in the transition, and practical guidance on configuring OpenWRT to leverage WPA3 effectively. By the end of this discussion, readers will be equipped with the knowledge to enhance their network security and ensure their systems are resistant to modern cyber threats.

Requirements

Hardware	Software
Raspberry Pi 4 B with power supply	openwrt-23.05.0-bcm27xx-bcm2711-rpi-4-squashfs-factory.img
Raspberry Pi 5 B with power supply	openwrt-bcm27xx-bcm2712-rpi-5-ext4-factory.img
RJ45 Ethernet capable	Raspberry PI Imager
SD card 8GB minimum	

This figure illustrates the use of a Raspberry Pi 4 to install OpenWrt and configure the device as a router, intended for educational purposes.

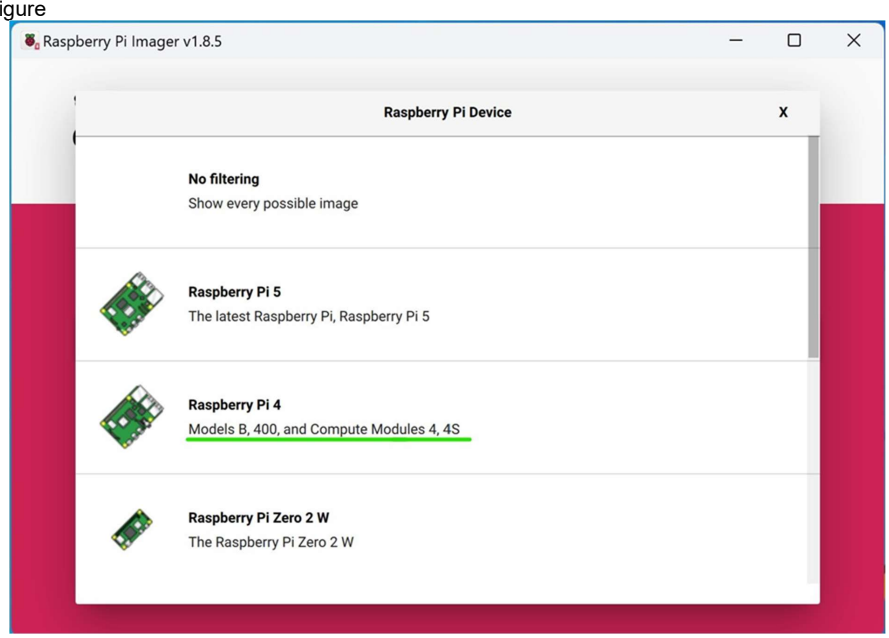
Walkthrough

After securing the necessary hardware (note that a single Raspberry Pi, either model 4 or 5, will suffice) download the compatible software for either Raspberry Pi 4 or Raspberry Pi 5, it is time to start the step-up process for OpenWrt. The group will use Raspberry Pi 4 as the hardware platform for this project. The initial step involves preparing the SD card by erasing and formatting it with OpenWrt, using the Raspberry Pi Imager tool.

Figures 1 – 7 will show step-by-step how to erase and format the SD card: -

Figure 1 shows that the user interface is clean and straightforward, making it easy to create an SD card for various Raspberry Pi models. The group will choose the model of their Raspberry Pi, which will be Raspberry Pi 4 and then proceed to the next stages to select the precise OS image to flash onto their SD card.

Figure



1

Figure 2 shows that the SD card getting erased, and the SD card is formatted to the FAT32 file system using the Raspberry Pi Imager. FAT32 allows for high compatibility with various operating systems, meeting the Raspberry Pi's bootloader requirements to read the boot partition. FAT32's simplicity and reliability make it ideal for the SD card's boot process, even though other partitions may use various file systems, such as ext4, for the main operating system and storage due to its support for bigger files and more efficient space management.

Figure 2

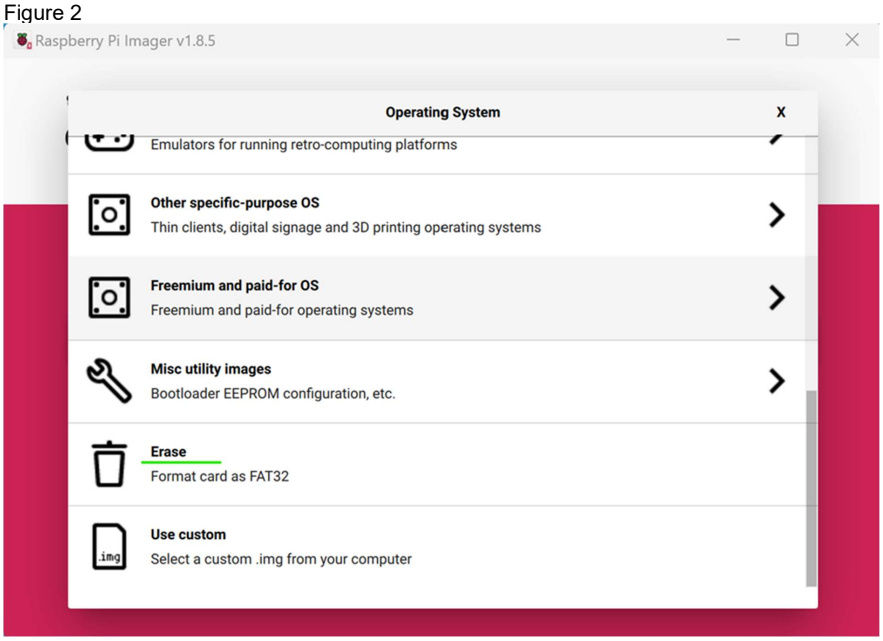


Figure 3 shows the selection of the particular SD card for erasing. by selecting the suitable SD card from a list of possible drives, ensuring that the correct one is erased and formatted for the project. This option is critical for preventing data loss from other discs that may be attached to the computer.

Figure 3

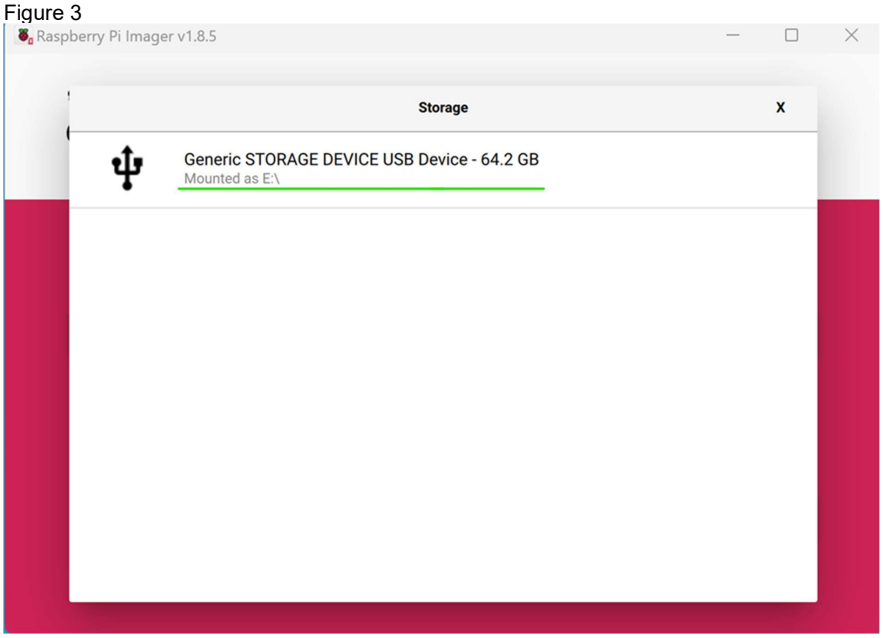
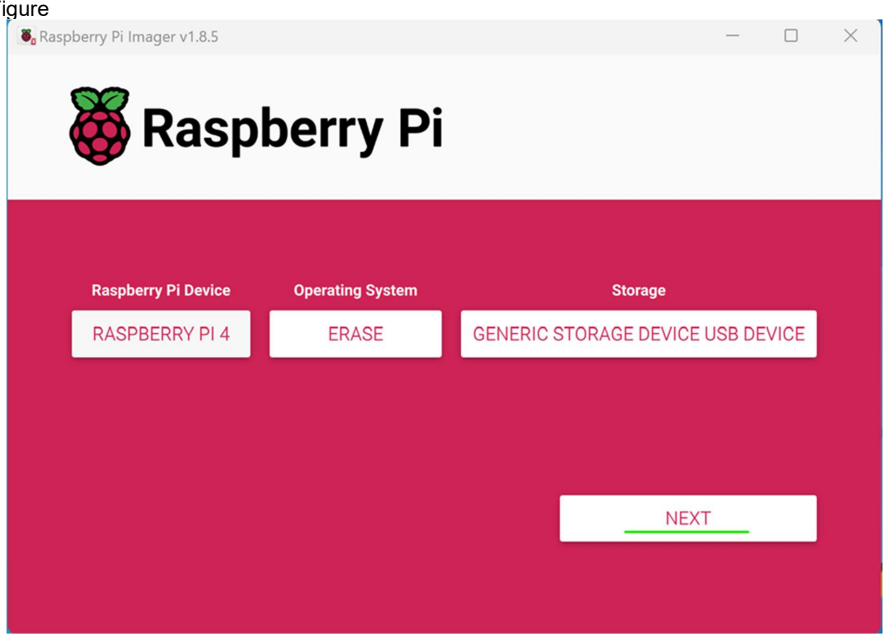


Figure 4 shows the correct option has been selected, and ready to be erase SD card.

Figure



4

Figure 5 shows after the SD card is ready to be written, go to option use custom and choose OpenWrt.

Figure 5

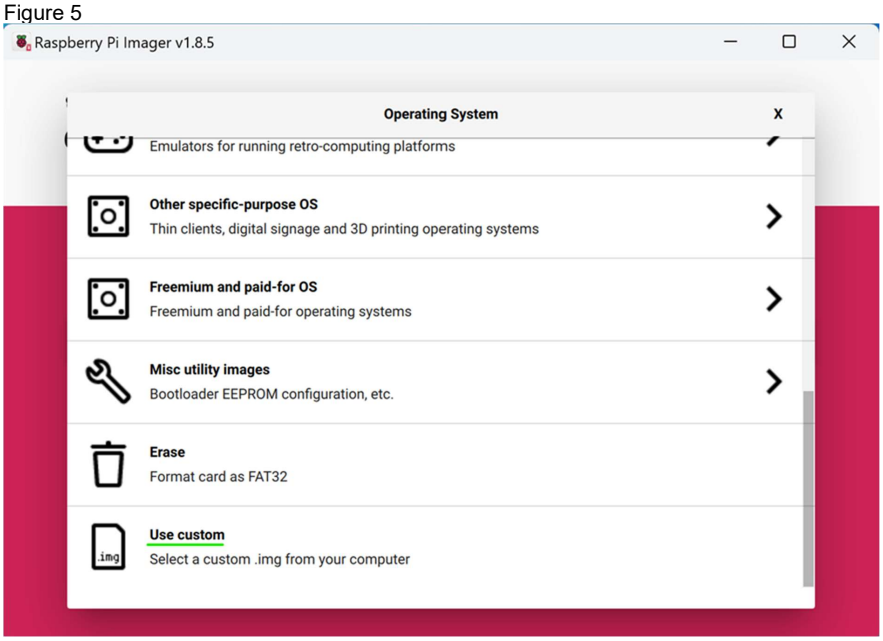


Figure 6 - Figure 6 shows the OpenWrt OS ready for the installation.

Figure 6

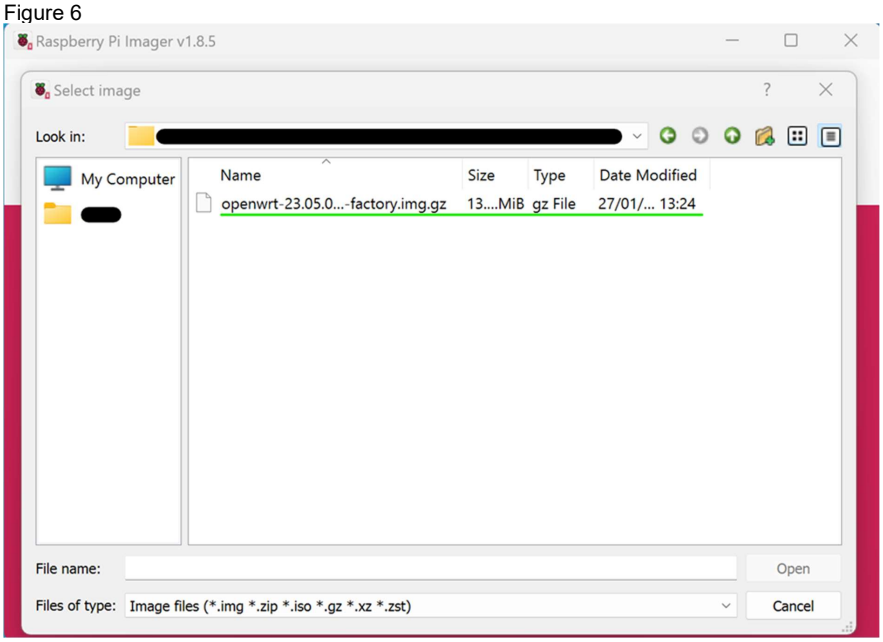
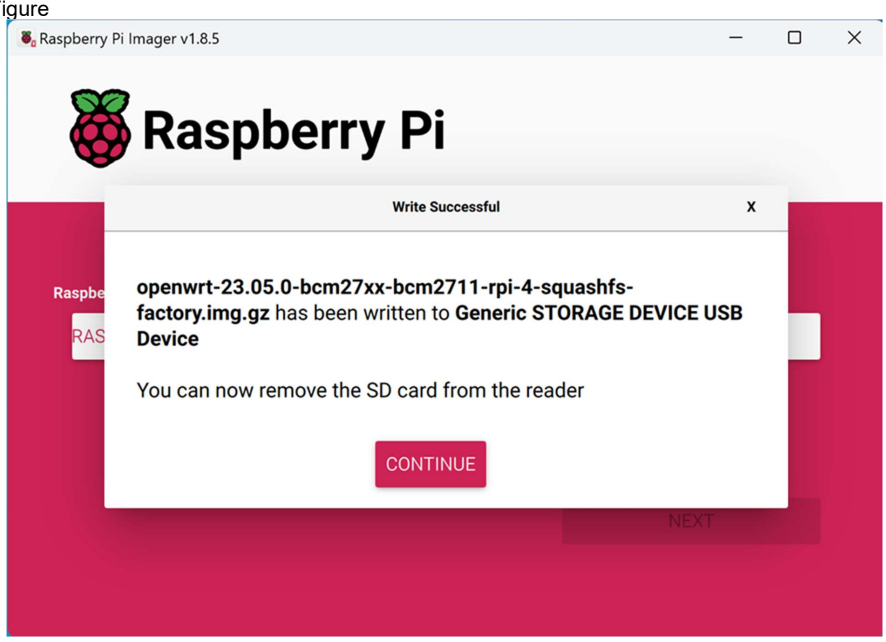


Figure 7 - Figure 7 shows OpenWrt has been installed successfully.

Figure 7



This step shows the network setup required to connect the Raspberry Pi to the computer for configuring OpenWrt.
Figure 8 shows how to setup the network for OpenWrt, by right clicking and selecting properties
Figure 8

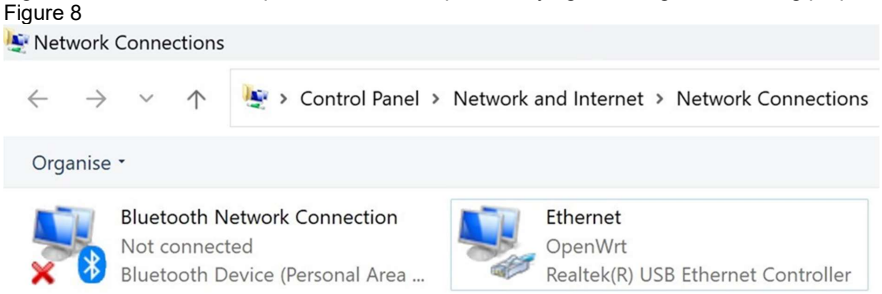


Figure 9 shows the network settings, clicking on Internet Protocol Version 4 and changing the IP Address with the following configuration, will allow the team to log into the OpenWrt admin page the default gateway.

Figure 9

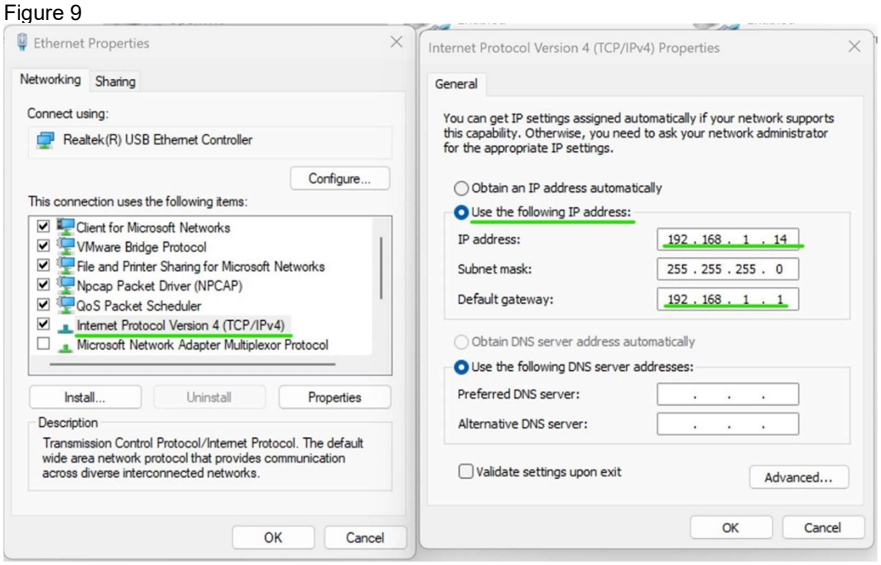


Figure 10 shows a Raspberry Pi 4 connected via an Ethernet cable, through which a group accesses the OpenWrt login page by navigating to the default gateway IP address using a web browser. The login page requires authorization and prompts for a username and password. The username is "root," which is the default for OpenWrt administrative access. This step is crucial for the team to log in and begin configuring the OpenWrt installation.

Figure 10

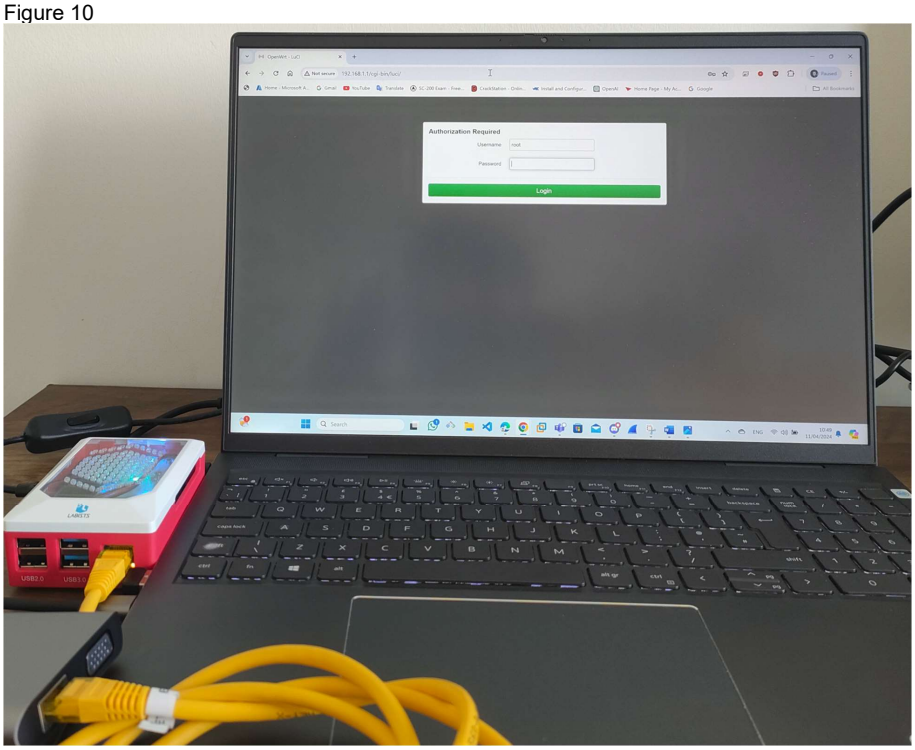


Figure 11 shows OpenWrt's web interface after a successful login, details about the system is shown, such as the hostname being "OpenWrt," the model as a Raspberry Pi 4 Model B Rev 1.4, and various software versions and statuses. Memory usage is detailed, showing a total available memory close to 7.64 GB. The group navigate to the 'Wireless' section, accessible via the 'Network' dropdown menu, where they will have the option to activate the wireless adapter and configure wireless security, including the WPA3 protocol.

Figure 11

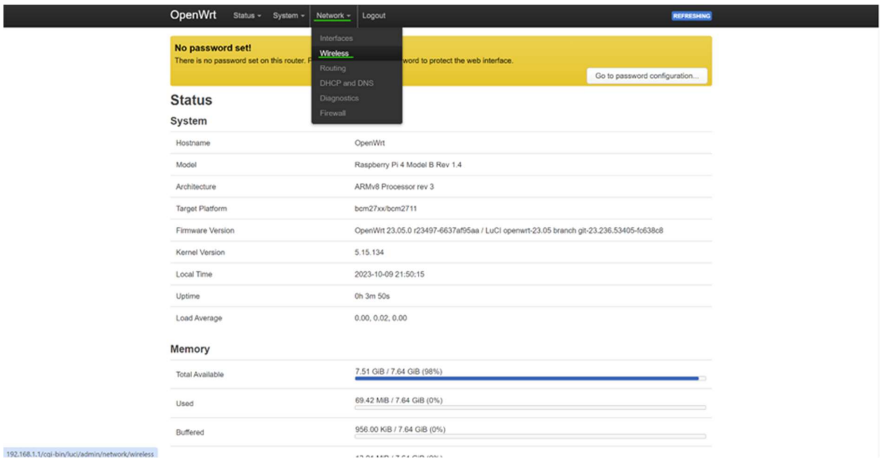


Figure 12 shows that the wireless network interface, named Cypress CYW43455 and supporting the 802.11ac/b/g/n standards, is shown as "not active" and the SSID, "OpenWrt," is as disabled. For the device to broadcast the SSID and become visible to other devices for wireless connectivity, the group will enable the wireless function by clicking the "Enable" button.

Figure 12

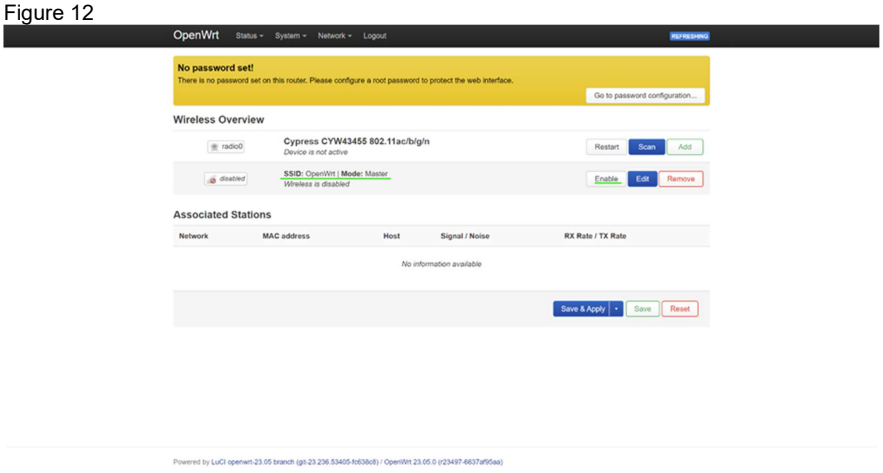


Figure 13 shows the General Setup tab of a wireless network configuration, it shows that the wireless network is enabled, as indicated by the option to "Disable" a sign that the wireless functionality is enabled. The ESSID, which stands for Extended Service Set Identifier, is set to "OpenWrt." This ESSID serves as the network name, and by being set, it allows other wireless-enabled devices to detect and identify this specific OpenWrt network when scanning for

available Wi-Fi connections. The details also confirm the network mode as "Access Point," indicating that the device is configured to act as a Wi-Fi hotspot that other devices can connect to.

Figure 13

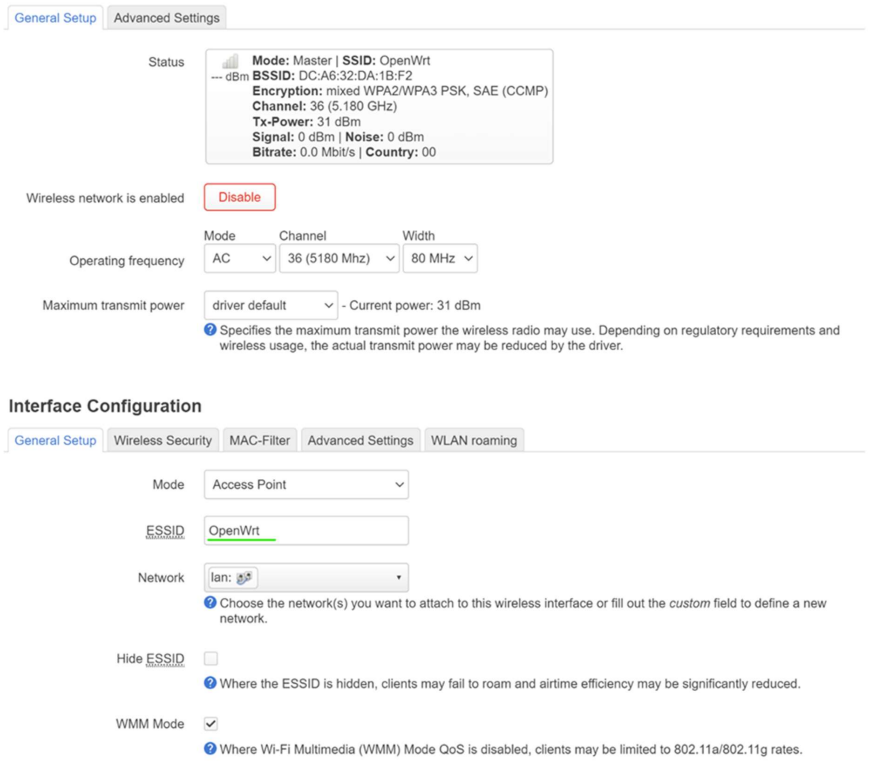


Figure 14 shows that by selecting 'Wireless Security' tab will allow for configuration on the encryption method. The encryption to a mixed mode of WPA2-PSK/WPA3-SAE, which allows for a transition phase accommodating devices that support either encryption standard. Additionally, the wireless password (or key) has been updated to "Ed1nbUrgHN@p13r1964". This new password will be required by devices attempting to connect to the network to verify authorised access, which will enhance the networks.

Figure 14

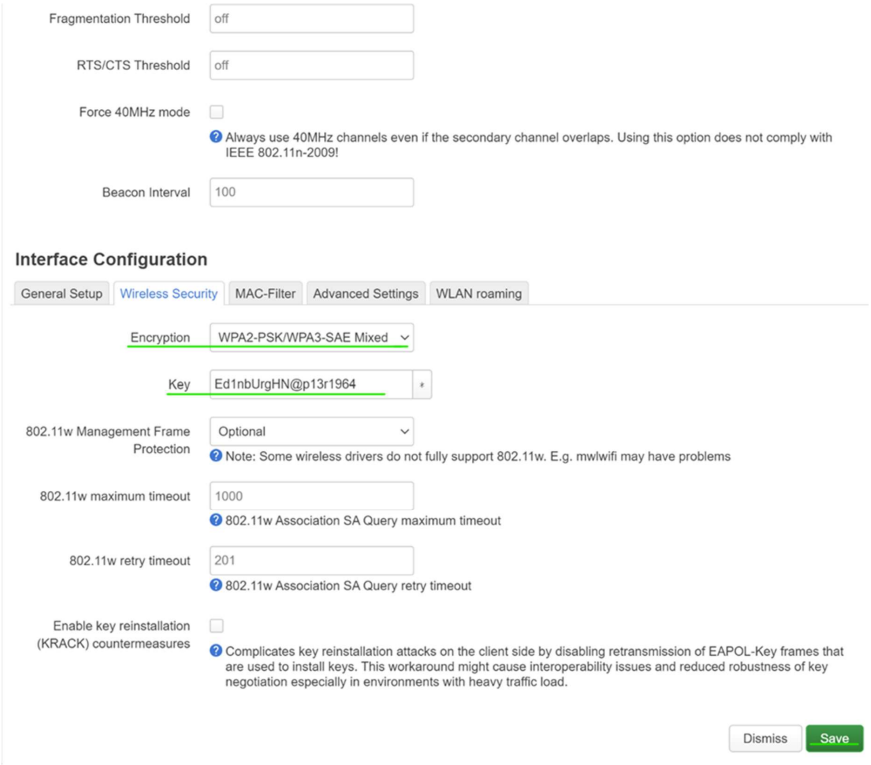


Figure 15 shows the OpenWrt web interface, where the group has made configurations to the wireless settings and by selecting the "Save & Apply" button will make the changes have been made. The wireless summary section shows the SSID as "OpenWrt" with the mode set to "Master," and the encryption as "mixed WPA2/WPA3 PSK, SAE (CCMP)," that the network will use a secure encryption method. To ensure that these adjustments take effect, the group will need to save and apply them.

Figure 15

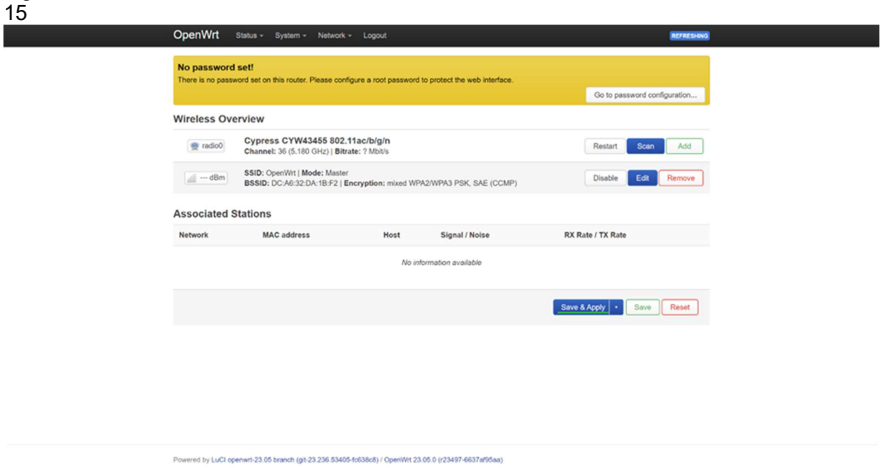


Figure 16 shows that a device with WPA3 compatibility has connected to the OpenWrt access point. The device is "Connected" to the network named "OpenWrt." It is set to automatically reconnect whenever it's within range of this network. The network's signal strength is excellent at -46 dB, and the link speed is reported as 325 Mbps. The security section confirms the use of WPA3-Personal, this proves that the device is using the latest WPA3 security protocol for a secure connection.

Figure 16

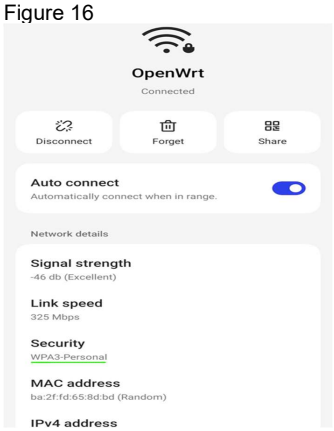


Figure 17 shows that the login password has not yet been established. The group needs to fix this by clicking on the "Go to password configuration" option, which will guide the group through the process of setting a secure password to protect the router's administrative interface. It is very simple.

Figure 17

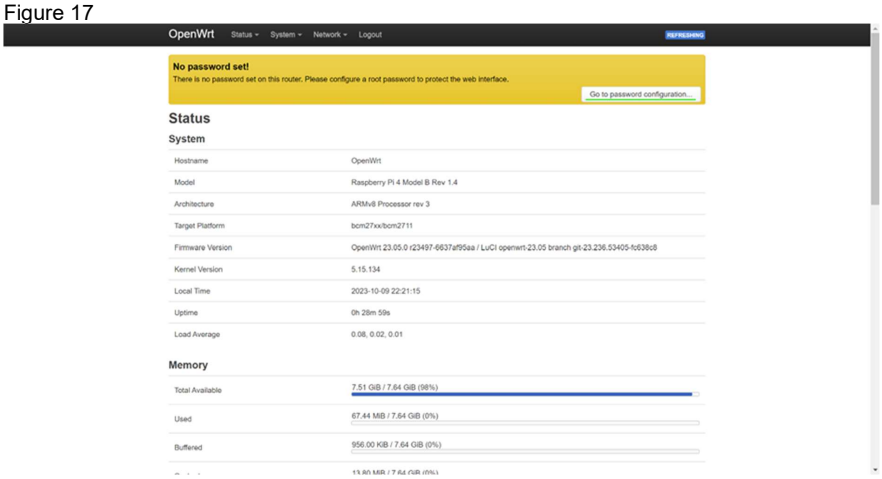


Figure 18 shows the password configuration page, the group has entered a new password for the login page on OpenWrt. The password 'Pr0j3ctWPA3p@2024' has been entered twice for verification and the system agrees the password is secure by stating that the password is 'Strong', its complexity and strength. With 18 characters including upper- and lower-case letters, numbers, and special characters, it provides robust protection against unauthorised access. Once this password is saved, it will serve to fortify the device's web interface security. Once this password is saved, it will help to strengthen the device's web interface security.

Figure 18