# Research Methodology

The aim of this dissertation was to highlight the ability to complete a penetration test on an access point in which the network is far from reach. This is significant as most of the testing required physical access to the site where the network was located. The method of testing was split up into two sections.

The first phase was done through scanning of the network and data collection. The area that was scanned for any available access point tried to obtain the WPA password with the use of multiple and various tools. The most useful information needed for the first phase to be done consists of the BSSID, ESSID, IP address, Client MAC, Channel and most importantly the four-way Handshake.

The second stage evoked attacking of the access point as well as network analysis. A set of attacks took place where the vulnerabilities of the network were tested. This depended on the outcome of the first stage of scanning. In order to conduct such attack, minimal user interaction took place. The benefits of this was that the tests were conducted much faster and efficiently.

At the end of the testing, the user had a clear view of what was needed to be done to strengthen the network. The approach that was taken is based on previous studies that were conducted where all papers. Such papers were then analysed and identified. From the identifications, the best and suitable attack approach was then used. Previous research in the area show how a person can be able to collect, analyse and exploit wireless devices to obtain unauthorised information within the network.

## Hardware Tools

### Kali Linux Raspberry PI

The open-source kali operating system which was obtained from the kali official website was downloaded and installed on a raspberry pi. According to Watson (2020), the main purpose of the kali platform was to enhance and advance the penetration testing and security auditing. For this reason, kali platform was chosen for the penetration testing to be both effective and achievable. Watson, (2020) noted that the operating system contains hundreds of tools which are pre-installed with the possibility to install extra tools to one’s need. A bash scripting was used to enhance the system that allows a penetration tester to create a script. This is done in order to achieve the results much faster. The raspberry pie 3 was integrated with a Wifi chip that offered a frequency band of 2.4GHZ which was helpful in the testing to be done.

### X450 Drone with Pixhawk 2.4.5 controller

The custom-built drone was built with the purpose of lifting 300g of weight on top of its body mass. In addition to this, the use of GPS and live feed data from the telemetry device allows the penetration tester to view the exact location of the drone in real-time. The benefits of using a custom-made drone are limitless as it can be adapted to whatever scenario is best for this testing to be completed.

### Alfa AWUS1900 802.11ac 1900 Mbps Dual-band USB Wifi Adapter

Alfa AWUS1900 802.11ac is a device which can mainly be used as an external long-range wireless adapter with the frequency band of 2.4GHz and 5GHz. The attachment between the Raspberry pi and the drone enabled the possibility of the communication between the laptop to the Raspberry pi whilst in flight. This was done throughout this dissertation as it enabled the penetration tester to run bash scripts and commands as necessary. The Alpha AWUS1900 had the option to attach up to four dual-band antennas. For this reason, it evoked the possible to check the number of antennas needed for the according amount of weight.

### Core i5-7 Laptop with a minimum of 8GB RAM

Throughout this dissertation, the main purpose of the laptop was to enable one to view the results of the attack and decide on the further steps. Where possible, a VNC connection was used to establish the use of the raspberry pi as it was more effectively and easily.

## Setting up the UAV and Raspberry Pi

The Raspberry Pi was connected to the drone as shown in Figure 3.1 where the Raspberry Pi was connected with the 10,000mAh power bank and also the Alpha Wi-Fi Adapter. This set up was chosen to be the most effective since various other power banks used offered less usage time than the 10,000mAh power bank. The 10,000mAh power bank gave an approximate operation time of 2 hours from each charge. The Alpha Wi-Fi Adapter was using the power of the power bank to be more operational.

Figure . - Drone with Raspberry PI

The drone was flown to the location of attack where an access point and a small network infrastructure was set up to be used for testing purposes. The Raspberry PI was configured with OpenSSH-server so that the tester was able to connect via SSH using Putty to it on port 22. Then X11VNC was installed so that the tests could be run on the Raspberry PI. The GUI was also used to allow the test to be done faster. The setup is shown in figure



## Scanning and Data Collection

Figure . – An experiment Scenario

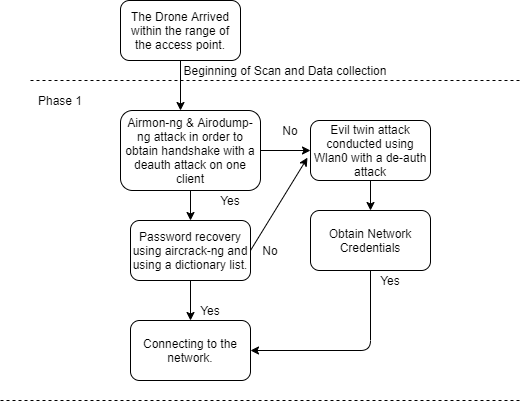
Once the drone arrived at the location of attack, the GPS co-ordinates were taken so that the second part of the attack could be done from the same location. The drone was left to hoover until a safe landing spot was discovered where the access point signal was reachable. The first phase of the scanning and data collection section took place as indicated in figure 3.3.

Figure . - Flow of scanning done

### Phase 1: Obtaining access to the secured Access point.

By making use of the available software which was widely used and also was very well documented, the first part of the methodology was based on two main tools which where Aircrack-ng and an Evil twin attack which could be conducted using an evil twin attack.

#### Four-way handshake approach

A Bash script shown in figure 3.3 was written to automate the WPA2-PSK attack. The bash script allowed the attack to happen much faster and even collected the data in the least possible time frame. Wlan0 was reset from any other previous configuration to conduct this test without any problem. As shown in Figure 3.4, this command was used with the addition of many parameters to be able to store the ESSID of the strongest signal in a text file. With the strongest signal access point being the first in the results table, this was chosen for the attack to take place. Airmon-ng was used to set the network adapter into promiscuous mode. Whilst, as seen in Figure 3.5 this was used to grep all the traffic of that ESSID and discover the BSSID and channel number being used.

After the discovery of the BSSID Airodump-ng, the access point under attack was focused with the command as shown in Figure 3.6 A client was identified, and the Bssid of Mac address of the station was stored in a text file. This was used in a replay attack that was done to de-authenticate a legitimate user and obtain the handshake needed. Five replay attacks were conducted using the command shown in Figure 3.7 so that the legitimate client would have to connect to the network once again. Once the user tried to connect, the four-way handshake was captured. F. Murphy (2013) stated that the handshake is composed of unique packets that can be used to obtain the passphrase needed to be able to log into the network under test. At the end of this bash script, Aircrack-ng was used to retrieve the password of the network. The time taken to retrieve the passphrase depended on the complexity and whether it can be found in pre-defined dictionary lists. An example of this is the rockyou.txt. If the password is complex to obtain, it will take numerous hours to crack the drone. Hence, the drone will flow back to the penetration tester where the Raspberry Pi was connected to a power supply. The drone will be left running for a while until the password would be successfully found.

Figure . - Scanning for the best Essid



Figure . - Checking ESSID to obtain BSSID & channel



Figure . - Using the channel and BSSID to capture traffic



Figure . - Replay attack on the client

#### Evil Twin approach

The evil twin attack was used when the dictionary attack could not find the password. With the use of this attack, the tester set up an interface on the Raspberry PI to act as a legitimate access point. This was done so that it will trick the legitimate clients into thinking that the password for wireless access is needed to be inserted again. To be able to perform this attack two scripts were used. The first script was airgeddon which was used in a similar way to the four-way-handshake approach. Airgeddon was set up with the parameters needed to capture a handshake with the access-point under test. Then, Fluxion a script developed by MPX4132 was used in order to set up the wireless adapter as a rogue access point, create a fake webpage and collect the password needed. The script scanned for targets and listed them. The preferred access point was selected and configured the Raspberry PI network card which was needed to be used for the attack. After this, an SSL certificate was created in order to make the webpage look legitimate. In the following screen, all the webpages that could be created were listed where the access point manufacturer’s brand were selected. When the configuration was done, the attack was then conducted with a de-authentication attack so that clients connect to the rogue access point. When the first client connected and entered the passphrase for the access point the script ended and the password was saved into a text file.

### Phase 2: Collecting IP addresses and port information

#### Network Scanning

In order to perform penetration testing, one needs a necessary tool which conducts a network scan. This is an important tool which must be used to get the maximum amount of information possible from the network. With such a tool, the tester can be able to see which TCP and UDP ports are left open which might be vulnerable to an attack. Yevdokymenko, M., Mohamed, E., & Onwuakpa, P. (2017) highlighted that in the reconnaissance stage of penetration testing is another description of network scanning. Furthermore, by scanning the target access point, it gives a clear interpretation of what can be done to test the network with maximum efficiency. For network scanning, a bash script was coded through the use of an IP address which was discovered by the previous attack using Aircrack-ng. Two Nmap scan was conducted and done. The first scan, as evoked in Figure 3.8 performed a simple network scan which outputs all the IP addresses that were being used in the network and also showed what type of operating system is being used. This information was useful to perform various attacks such as a man-in-the-middle attack. The second scan focused on the vulnerabilities of the devices. Each connected device effected the final output which is clearly shown through the command in Figure 3.8. All the outputs will be saved in text files for the user to view them when needed.

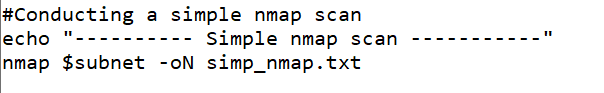


Figure . - Simple Nmap Scan

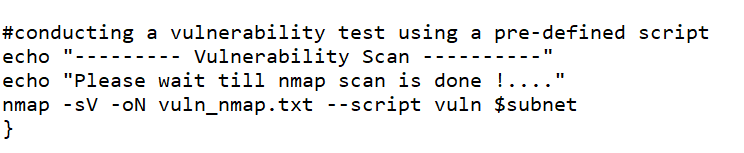


Figure . - Vulnerability Nmap scan

## Penetration testing and Attack assessments

### Phase 3: Vulnerability testing

#### Man-in-the-middle

When the ports where scanned, Nmap a man-in-the-middle attack was used. This is a test which offers a clear output of what the clients and what network traffic are being generated. Moreover, the Raspberry pi will act as a malicious device between the access point and a client. The script created for this attack will require the user to input the IP address of both devices that needs to be used manually so that any desired access point or client device can be put under test. Furthermore, the test was done using Arpspoof as depicted in Figure 3.10. This was used to establish the rouge device between the legitimate network. Three tests were performed in this man-in-the-middle attack. The Urlsanrf which is shown in Figure 3.11 was used to store any websites that the user visited. TCPdump was then used to conduct two trials.

As seen in Figure 3.12 the use of the command used was that any activity from the network which uses the port 80 was stored in a text file. As evoked in Figure 3.12, the conducted final test showed the IP addresses in various websites which where stored.

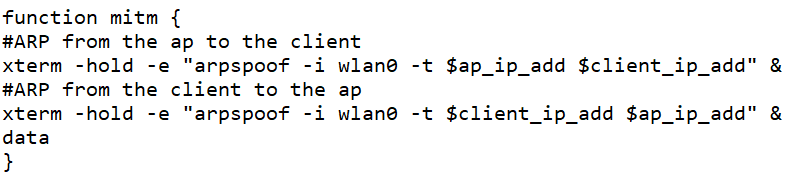


Figure . - Arpspoof to conduct MITM

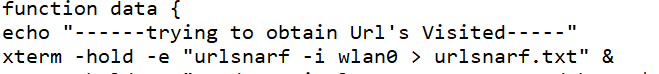


Figure . - Urlsnarf command



Figure . - First TCPdump command

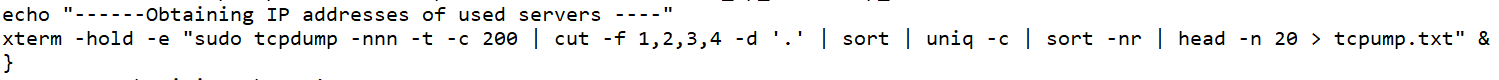


Figure . - Second TCPdump command

#### MAC Spoofing

With the use of the tool macchanger, a script was written with the purpose of bypassing MAC filtering and also protecting the attacker’s identity. The benefits of using MAC Spoofing is that one can connect to multiple networks which have MAC Address filtering. Apart from this, one can conduct Scanning and do vulnerability testing without authorisation. Furthermore, this will hide one’s hardware identity which makes attacks as if they were being developed in a legitimate client. A script was written where it would scan all available networks and show their Bssid as shown in Figure 3.14. After this, a client was chosen so that the MAC of wlan0 on the Raspberry PI became the same as the MAC of the client. This is depicted in Figure 3.15. In Figure 3.16 the macchanger command was used in order to perform the MAC address to Change.



Figure . - Capturing all available networks

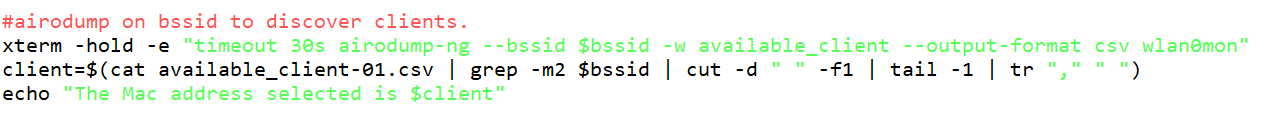


Figure . - Capturing the client MAC

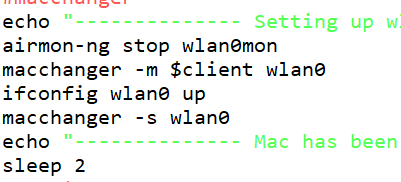


Figure . - Changing the MAC

## Conclusion

After all the tests and scanning that have been performed, a report was displayed with all the tests combined. These where then further inspected by the tester and the company that where being under test. This is beneficial to the businesses. This is since it enables the companies to see any vulnerabilities which might occur in the system and where forgotten. From all the scripts which were conducted, a clear and vivid view was given to all the vulnerabilities in the testing setting.

**References**

Watson, J. (2020). *Kali Linux on the Raspberry Pi: 3, 2, 1, and Zero | ZDNet*. ZDNet. Retrieved from <https://www.zdnet.com/article/kali-linux-on-the-raspberry-pi-3-2-1-and-zero/>.

*Online-iT How To Install ALFA AWUS1900 Kali Linux 2018.4*. Online-iT. (2020). Retrieved from <https://online-it.nu/how-to-install-alfa-awus1900-kali-linux-2018-4/>.

F.Murphy, B., 2013. Network Penetration Testing and Research. *Nasa USRP- Internship Final Report*, Program USRP Summer.

Yevdokymenko, M., Mohamed, E., & Onwuakpa, P. (2017). Ethical hacking and penetration testing using raspberry PI. 2017 4th International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S and T 2017 - Proceedings, 2018-Janua, 179–181. <https://doi.org/10.1109/INFOCOMMST.2017.8246375>

Wang, S.-L., Wang, J., Feng, C., & Pan, Z.-P. (2016). Wireless Network Penetration Testing and Security Auditing. ITM Web of Conferences, 7, 03001. https://doi.org/10.1051/itmconf/20160703001

Gergovemi, S., & Panchev, C. (2015). Vulnerability testing of wireless access points using Unmanned Aerial Vehicles (UAV). European Conference on Information Warfare and Security, ECCWS, 2015-Janua(February), 425–428.