# Conclusion and Recommendations

The main objective of this dissertation was to investigate and analyse whether microcomputers and UAV’s can be used with one another to penetration test a physically inaccessible access point.

The major concern and struggle of having a hacker who wants to break into a specific system are to keep up with a high level of security. Hence, one needs to adopt certain precautions in order to minimize such an attack from happening. One of the precautions one can take is to conduct a penetration test. This is done to highlight any weaknesses that can cause the access point to allow a malicious user into the network.

Throughout this dissertation, the network was chosen on purpose. The reason being is that such network setup is available and accessible in most households both locally and internationally. In addition to this, the network setup also emerges a list of most and common vulnerabilities in which a specific household Wi-Fi would contain.

The tests were conducted as expected. One of the reasons being is that such tests were conducted through the use of a GPS antenna. The GPS antenna-maintained stability throughout the process and kept a steady position at a fixed altitude. Moreover, the location was also stable throughout such a process. Hence, the tests were done without any drawbacks.

The penetration tester used the scripts that were conducted. For this reason, the time required to conduct these tests where minimized. Hence, the tests were conducted more efficiently.

The Drone and the Raspberry PI network tested an access point. Both devices produced a successful outcome in which they obtained any vulnerabilities which existed. These vulnerabilities produced where then addressed and fixed. In order to check for any vulnerabilities, the access point was used. The access point was used as a base of testing in order to gather necessary data and information. Apart from this, it was also used to identify and analyse any backdoors which might have been open due to a hazardous attack.

## Hypothesis :

In conclusion to the testing conducted it can be concluded that the hypothesis has been proved true where it was possible to test a network that the penetration tester has no physical access for vulnerabilities that it might have. Furthermore, it was also proven that secure access points can be scanned and exploited if using a microcomputer.

## Evaluation of work:

During one of the initial phases, the password was collected. This was done via two tools which were the air crack u evil twin. These two tools resulted that they are two of the most effective tools one can use to obtain the hash of the network and find out the password.

If the password is complex and so it could be difficult to find, one is suggested to use the evil twin method. The reason being is that such method is used to help minimize the testing time. Once the password was found, the penetration tester was able to enter the network. This gives the ability to the penetration tester to conduct further tests.

During such stage of the process, a network scan was very crucial in order to obtain much-needed topology of the network. Hence, two network scans were conducted. Throughout such scans, the clients and ports which were being used where listed. In the second run of the scan, the vulnerabilities of the hosts were found and saved in a text file. This was needed to be able to allow the user to check what vulnerabilities the network has.

The conduct the second phase of the process, the gathered information from the first phase was needed. A man-in-the-middle attack was done through the use of the access point and the host. This was done in order to be able to intercept traffic between these nodes. All activity on the network was monitored and focused more on the servers used. Hence, the penetration tester had a solid result which could be verified if the results obtained were true or not.

A further test was conducted on an open network which was configured with MAC address filtering. In this test, a script was produced in order to automate a tool named macchanger. This tool gives the option to the penetration tester to change the MAC address of a network adapter. In addition to this, the tool would also allow the user to join the network with the Spoofed MAC address. Apart from this, it could be recognised as a legitimate client where both phases could take place to construct a vulnerability testing analysis of the whole network. After the completion of the testing, the MAC address of the Raspberry PI was then reverted back to its original state.

## Future recommendation and discussion:

Once the tests were conducted and completed, number and several limitations of the study were outlined. For this reason, such limitations can be researched to enhance this dissertation in the near future.

In order to reduce the limitations and further improve the scripts, one can join the scripts together into one. Throughout this process, the penetration tester would be given the possibility to choose on the attack one needs to conduct. This can be done from the same script rather than executing the scripts one by one. Another limitation of the study is that at times, the scripts were restarted. Hence, one needs to remove any previous configuration that was done on the Raspberry PI which was not taking part in the testing. To make the testing more reliable and effective, more hosts could be connected to the specific network. The mentioned hosts could be able to conduct further investigation.

This study highlights that the Aircrack-ng was completed quite smoothly. A limitation is that the handshake which captured it took a lot of time to figure out the password required to enter the network. Other diverse word lists which can be obtained online could be used. This is so that it would make it a possibility to find a more efficient wordlist rather than the one used to conduct the tests.

Another recommendation of the study is that a man-in-the-middle attack could be used with a different approach. This would have allowed this dissertation to be developed and analysed further. In addition to this, different and various attacks could also be tried with the same method. A larger selection of tools could be used to make the penetration test much more applicable.