# Introduction

Due to the emerging technologies found nowadays, one can easily construct an attack. This area of study was chosen to enhance the knowledge of how various and numerous attacks can be done without nobody noticing.

As mentioned above, the wireless network revolution has increased rapidly and has brought major and crucial changes. Due to such a revolution, the devices are becoming portable and makes it easier for the user to use both wireless network devices and the network at any time of day. For such reasons, wireless networks have become part of one’s daily life. Millions of individuals are using wireless networks all the time for various purposes. Wi-Fi Access Points have been installed to both indoor and outdoor environments to facilitate user connectivity with the network.

The method of research is based on multiple attacks which can be created and used by script kiddies and hackers. The main aim of this research is to verify whether is it possible to penetration test access points which are located far away from an attacker without any authorisation. Another objective that needs to be answered is whether a microcomputer can be used in order to gather data from a secured network device without using complex scripts. Furthermore, any limitations which might produce a challenging scenario will be outlined and discussed.

Wi-Fi Access Points offers an environment where people can share resources without being connected directly via cable to a network. This scenario makes it possible for the hacker to hack and access the network without having physical access to the network infrastructure.

During recent years, UAV’s have become much cheaper and simpler to use. There are multiple options on how one can obtain UAVs. Such devices can be bought ready to use or one can create such a device with little knowledge required. The hacker can decide to make use of a microcomputer such as a Raspberry PI. The Raspberry PI can be attached to the drone where it could be configured to attack a physically unreachable access point. Moreover, if the attack happens to a small or an enterprise network, it could lead to loss of data. Apart from this, the hacker could also gather sensitive and important information which might lead to multiple circumstances. The setup of the attachment of the Raspberry PI and the drone can be beneficial to the penetration tester. This is since it could be used to test these kinds of access points and fix any vulnerabilities that the network might have. Since there are multiple access points within a network, it might be challenging to keep track of all the security issues that these might have. If left unattended, such access points could be vulnerable to hacking. This is since unauthorised access is gained to collect data without any permission from the owner.

With rapidly emerging technologies, one can never underestimate a hacker’s ability to conduct an attack even on places where physical access is prohibited. The technologies being used in order to conduct such a hacking scenario is inexpensive. It also can be easily used with various scripts which can be written by the hacker or obtained from online sources. Network security testing is one of the most effective and interesting cases when it comes to penetration testing. This is since it minimizes the possibility of a hacking attack being conducted where it is least expected. With the use of various tools, back doors identification allows the network users with a protected environment that can defend such attacks.

The prototype includes the building of a contraption where a custom-made drone with a GPS antenna and a Raspberry PI using the Kali operating system. The next step after the device is made is to create scripts which automate attacks and network scans with the minimum user input needed. Different attacks will try to exploit the security implemented in access point and networks and verify if such a scenario can be conducted by a hacker. The final part of this dissertation will be a discussion of results obtained when the tests were being conducted. Different methods of data collection will be tested in order to compare the results of different tests together.