# Abstract

Hackers have always been analysing and discovering new ways on how to exploit a networking system for malicious purposes. Through the use of emerging technologies, hackers have benefited in creating and constructing new gadgets which allow an attack to occur. Such an attack would be much more efficient and faster. The main aim of conducting such research was to be able to conduct penetration testing by making use of unmanned aerial vehicle and microcomputers. Usually, the attacks conducted by a hacker would require a direct connection to the network. In order to be able to connect directly the attack, the network would require physical access to the premises. UAV’s and Microcomputers offers the opportunity to locate a wireless signal from an access point which is part of the network. One can ask himself regarding the possibility of using flying computers as a method to hack into a network and conduct various attacks. This can cause serious damage to a system and even data could be stolen from servers, computers and other gadgets. The area of study chosen will allow penetration testers to gain knowledge regarding the damages that could be done to a network if this type of scenario emerges.

To be able to conduct this penetration testing, the Raspberry PI device was set up with the operating system named Kali Linux. The drone was equipped with a GPS antenna in order to hold a position during an attack. Scripts were produced and executed in order to automate multiple tests and decrease the time of testing significantly. The results which were obtained were the password of the wifi in order to access the network. The network scan was able to identify potential targets that are connected to the network and a man-in-the-middle attack which produced a network trace of what was the client doing on the network. Furthermore, the network scan also provided a list of potential vulnerabilities that each device has in order to have a clear guide of that attack should be tested in the future. Finally, all the results were saved in a text file. This was done for the benefit of the penetration tester to have a report of all the results of the attacks that were conducted. The second setup was used in which an open access point with MAC filtering rules was used. This access point allows only certain MAC address devices to connect to the network whilst others will see the ESSID but will not be allowed to connect. In addition to this, the script helped to simplify the macchanger commands. This is since it was possible to scan the network and see what clients are connected to the mac filtered access point and clone the mac address of a legitimate client on the Raspberry PI. This allowed the wireless adapter to connect to the network without a problem and conduct further testing, as necessary.

Improvements outlined including the creation of a script which can encapsulate all the scripts written for this dissertation. Furthermore, a suggestion was made for researching various other tools in order to obtain the encrypted wireless password called the handshake excluding the once used and researched to minimize the amount of time needed for the password to be cracked and found. Furthermore, various other tools could be tested using the setup which will widen the awareness and knowledge on this scenario of attacks.