# Literature Review

## Wireless networks and Penetration testing

In the last decade, wireless networks became an essential part of our everyday life. To meet one’s everyday lifestyle, open spaces with networks are being offered to accommodate one’s lifestyle. Such open spaces include coffee shops, workplaces, and playgrounds amongst others. There has been a huge concern regarding public networks in such spaces due to the use of networks which transfer sensitive information to these public networks. Such transfer easies the burden for hackers. This is since hackers can gather data without authorisation from such public networks. As noted by Vemi, SG and Panchev (2015), the most used standard network in wireless networks security is WPA2 which is used in most homes and government entities. The demand for wireless devices that makes use of these wireless networks is rapidly expanding. In relation to such high demands, WIFI product vendors are facing a huge challenge where they need to produce high-quality technology. Similar to Vemi, SG and Panchev (2015), Vinjosh Reddy et al (2010) debated that one needs to keep the vulnerabilities of such devices in mind since such vulnerabilities are not yet known and patched. Hence, the method for implementation is still a cohesive issue. As discussed by Yevdokymenko, Mohamed and Onwuakpa (2017), there are multiple and various ways for an ethical hacker to access a network without authorisation. This is mainly done through the use of two different techniques which are analysis and investigation. The analysis technique for a penetration test is to think like a hacker and use the same steps that the hacker might use to get access to the network. In addition to this, when the investigation process is completed, the tester will find out the notion of the “holes” in the network. Such holes can lead to a disaster in an enterprise network if discovered by an unauthorised person. Abramov, Kobilev and Makarevich (2013) highlighted that without physical access to a network it is impossible to do a penetration test. This is why hackers are usually within the range of the network and connected directly instead of from another geographical position. With the use of drones this problem is eliminated as the drone can be placed in a hidden area where the signal range is reachable. This process can also be done without the need for the hacker to be on the premises.

## Known approaches for combining UAVs and Microcomputers.

There are many types of Microcomputers and UAV’s which are readily available on the market at a very low price. One of the most popular types of a microcomputer is the raspberry pi which comes in different models that offer different functions. Abramov, Kobilev and Makarevich (2013) emphasized that the most effective setup for penetration testing of a network is done through the use of quadcopters. This is done by using a raspberry pi integrated with the PwnPi which is a Linux based operating system. Such a system includes over two-hundred tools which can be used in this scenario. Furthermore, Abramov, Kobilev and Makarevich (2013) argued that this setup and software is easy to set up and use. In addition to this, Abramov, Kobilev and Makarevich (2013) also made use of a data collection card which was used to inject and analyse packets. The Wi-Fi card that was used throughout the process was the Alpha AWUS036NHR. This was beneficial and crucial for extending the range from the drone to the victim's access point. In relation to this, Westerlund and Asif (2019) also used a wireless adapter to be able to perform a similar type of attack. The adapter used by Westerlund and Asif (2019) was the Wifi Pineapple Nano 6th generation device. Such a device offers a user-friendly web interface which can be used to conduct a variety of attacks such as De-authentication attack, packet spoofing, denial of service attack and many more.

The unmanned aerial vehicles (UAV’s) are becoming more affordable and open-sourced. Abramov, Kobilev and Makarevich (2013) highlighted that the drone used in a penetration testing environment is one of the most effective ways which either the penetration tester or the hacker can get information and data from a network without being detected. From such studies, these researchers also evoked that this is the cheapest and most practical option to implement in inaccessible places. One drone which is hugely popular in multiple papers is an AR Drone 2 which can be easily used even by an unexperienced person which also provides a space where all the components can be connected to. This drone offers multiple modifications such as attaching and connecting the raspberry pi to the drone base and as a source of power supply. It also offers the compatibility to interact with API which can be found free online on the drone OS. Although this drone is one of the most practical for this kind of scenario, it has been discontinued and it is very challenging to acquire one. The most practical solution for this kind of penetration testing is building a custom-made setup which is effective and efficient.

## Maltese UAV Laws and restrictions

There aren’t any Maltese laws that specify any regulations regarding drones and UAV’s which are enforced by law. Malta has been issuing out recommendations on the use of drones that a user needs to follow to be able to fly the drone in a safe environment. Herrmann and Markert (2019) debated that a drone must fly in a place where the privacy of individuals is not breached, where there aren’t any crowds and in prohibited zones. Some restrictions that apply are that the drone must be flown in daylight and it cannot be flown further than 300 meters at a height of proximity 60 meters. In order to abide by these recommendations, the study which will be conducted will be in a controlled environment. All such regulations mentioned will be observed and met.

## Past Approaches for penetration testing using UAV’s

Past approaches for penetration testing using UAV’s has highlighted that to be able to implement such test one needs a small computer which can be carried by the drone and two Wi-Fi networks interfaces. As evoked by Vemi, SG & Panchev (2015), these types of attacks are dependent on the password being used on the access point or router. To further strengthen this argument, if passwords are very complex and contain a good mixture of letters, numbers and symbols, the process will be longer. Hence, it would take a lot of time to enter the system and perform the attacks due to the limitation of the battery life of the drone. Vemi, SG & Panchev (2015) noted that to be able to perform this test, a raspberry pie model 3+ with a Linux operating system was used with two network interfaces. One of the wireless interfaces was used to scan for the available access points and identify the connected targets to these access points. This was done by the use of “airmon-ng” where the interface was set to monitor mode and the packets began to be captured. The other interface was used to apply the attack on the selected target which was identified by the use of the first adapter. This interface was also used to inject packets into the network where a de-authentication attack would take place.

Similar to Vemi, SG & Panchev (2015), Abramov, Kobilev and Makarevich (2013) used a similar setup that was used to test the setup by first scanning and collecting data and performing an attack to check whether the network is secure or not. The initial part of the process was done by guiding the drone into the attack, which was scanned for available access points and tried to locate the weakest part of the network. This was required so that the attack could be more effective.

Unlike these researchers, Vemi, SG & Panchev (2015) had also set up the drone with a GPS antenna to allow the user to locate and point all the access points. This was done through the use of the wifi signal strength in order to be able to understand the network structure. In addition to this, these researchers also noted that the useful information is stored from scanning and data collection which includes the location, best strength of a signal, BSSID, SSID, MAC address and encryption type. Furthermore, multiple drones were used to be able to cover an immense area in a smaller timeframe to make the simulated attack more useful. When all the data was gathered, the attack was tested on open networks with no password. This was done quickly, effectively and successfully. The test was conducted also on WEP and WPA which are types of basic protection that will offer. Abramov, Kobilev and Makarevich (2013) emphasised that to be able to access the WEP secured network, a PTW attack needs to be done by the use of aircrack-ng. For the WAP secured network, a dictionary attack needs to be used with the use of a brute force attack. This made it possible to obtain the password and enter the network.

Westerlund and Asif, (2019) highlighted that a Wi-Fi pineapple could be used to coordinate an attack with a set of tools already pre-configured where one can perform a man-in-the-middle attack, denial of service and de-authentication attacks. A similar system which is very useful in this kind of scenario is ‘Fruity-Wifi’. This is a tool which can be implemented on a raspberry pi without the need for extra hardware like WI-Fi pineapple which is a device on its own. Such a tool has multiple and various benefits such as that the attacks are more flexible, and it has less payload to the drone’s weight.

## Tools for penetration testing

### WPA/WPA2 Password Cracking

The unauthorised access to access points is becoming a huge barrier. This is since such encryptions are becoming much more demanding to bypass. Due to the complexity that the WPA2 offers, such a method of hashing is challenging the penetration tester when conducting the tests. Murphy (2013) noted that a primary tool which conducts the possibility of such an attack is the Air-crack-ng. In addition to this, this primary tool is a network software which encapsulates a network detector, WEP, WPA/WPA2 cracker, a packet sniffer as well as an analysis tool. Aircrack-ng can support both Windows and Linux environments for both 2.4GHZ and 5GHZ. Murphy (2013) added that a four-way handshake is required to be able to obtain the key. In relation to this, Carranza et al (2018) noted that Aircrack-ng uses Airodump-ng which allows any wireless network to be set up in monitor mode. This allows the penetration tester to use the desired network adapter to obtain the ESSID. Apart from this, the penetration tester will also obtain the MAC address of the access point as well as any client which is connected to the access point. Without obtaining this information, and Aircrack-ng attack would not be possible. Following the process of the four-way handshake, the penetration tester needs to conduct a dictionary attack Figure 2.1. Carranza et al (2018) emphasized that with the use of the Aircrack-ng command, there is a probability for one to use a wordlist which can be pre-defined or constructed with another command. This is done in order to be able to find the password of the access point. Sometimes, this process may be seen as a burden due to the amount of time needed to conduct such complex tests. This researcher stated that when the passwords are very complex or uncommon, the time might range from either an hour to days.

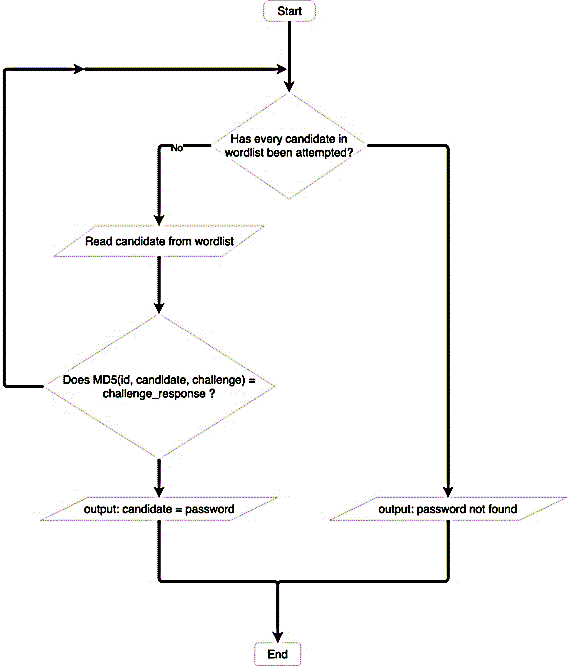


Figure . - Dictionary attack Procedure

### Network Scanning

One of the most crucial things in relation to penetration testing is a network scanning. The network scanning allows the tester to gather the necessary information regarding open ports, operating systems, and more vital information. Such information and access can lead to either a back door or a vulnerability. To strengthen this point, Westerlund, O., & Asif, R. (2019) debated that in order to find any ports which might hinder this obstacle, one needs to make use of special software. Such software gives additional help to the user in both network discovery and network auditing. Moreover, the results of such test will display a list of any open ports on the target network. Similar to Westerlund, O., & Asif, R. (2019), Yevdokymenko, M., Mohamed, E., & Onwuakpa, P. (2017) also emphasised the importance of network scanning. Yevdokymenko, M., Mohamed, E., & Onwuakpa, P. (2017) also described how scanning will be used to construct and shape the attack that will be conducted on the internal network.

### Man-in-the-middle attack

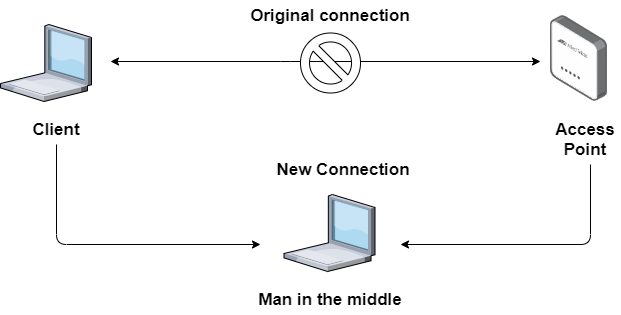
In a man-in-the-middle attack, the tester will act as an intermediate connection between the access point and the client. This will allow the tester to capture any data which will be transferred from the legitimate client to the network. Westerlund, O., & Asif, R. (2019) states that first the network is scanned, and the network is mapped with all the clients that are connected. As can be seen in Figure 2.2 the device between the legitimate client and access point will mimic the mac address of the legitimate device so that the administrators will not know that they are being monitored.

Figure . - Man-in-the-middle attack

**2.5.4 Mac Spoofing**

Another tool which is used when doing penetration testing is macchanger. This benefits the user with hiding its identity to the network so that the traffic generated will be captured as a legitimate client. As discussed by Cangea, O. (2018) the identity of the attacker is very hard to find because this attack makes the attacker invisible. Even open Access network with Mac address filtering is vulnerable to such attack since the user will imitate a client and gain access using it’s MAC address where afterwards attacks can be done accordingly.

### Evil Twin / Café latte attack

The use of this attack is mainly to trick users into using the device which is set up by the penetration tester to get as much information about the network as needed. This can be done even without the need of a password for the network under test. Sharma et al. (2015) compered this attack to a phishing attack where users data is being collected by the evil twin. The attack uses genuine access points and clones their settings to make the client think that the network is not being hacked. According to Ghering, M., & Poll, E. (2016) an evil twin attack uses a rogue access point to be able to imitate another wireless network. This method tricks lots of devices to think that they are connecting to a legitimate client.

## Network Monitoring and Packet Analysis

Packet sniffing is a technique which captures packets that are passing through the network. Tools such as Wireshark, TCPdump are used to monitor all network data. As described by Gandhi, C., Suri, G., Golyan, R. P., Saxena, P., & Saxena, B. K. (2014) a packet sniffer captures frames from the Transport, Network, Link, and physical layers of the open systems interconnection model. As argued by Gandhi, C., Suri, G., Golyan, R. P., Saxena, P., & Saxena, B. K. (2014) TCPdump is one tool which works only with the Linux operating system, with the ability to use the command line to capture packets it makes it possible for one to run a script and conduct network monitoring easily. In contrary to TCPdump, Wireshark offers a GUI interface that offers information in a much more meaning full manner whilst also offers much more filtering options that work on more than one thousand one hundred protocols. Furthermore, Gandhi, C., Suri, G., Golyan, R. P., Saxena, P., & Saxena, B. K. (2014) discussed how neither Wireshark nor TCPdump offered an intrusion detection function or can manipulate data.

## Command-line Attacks vs GUI attacks

The use of the command line offers a faster rate of attack rather than using GUI. Some tests require the use of a GUI which then is done manually by the tester. When a tester is using a command-line interface, one has the possibility to write English like codes. This is done in order to create a small program that offers the use of multiple tools at a faster rate with minimal help from the penetration tester. In the study conducted by Westerlund and Asif (2019), the use of CMD is visible throughout all tests performed. This improved the quality of the attack so that the legitimate client would not recognise that an attack is being done. Similar to Westerlund and Asif (2019), Vinjosh Reddy et al (2010) noted that the use of command-line offers more flexibility on the way that the attack is performed and done.

**Bibliography**

Herrmann, S., & Markert, F. (2019). Drone rules and laws in Malta - current information and experiences. Drone Traveller. Retrieved 23 April 2020, from <https://drone-traveller.com/drone-laws-malta/>.

Farik, M., & Ali, A. (2015). Analysis Of Default Passwords In Routers Against Brute-Force Attack. INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, Volume 4(issue 09).

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>

Westerlund, O., & Asif, R. (2019). Drone Hacking with Raspberry-Pi 3 and WiFi Pineapple: Security and Privacy Threats for the Internet-of-Things. 2019 1st International Conference on Unmanned Vehicle Systems-Oman, UVS 2019, c, 1–10. <https://doi.org/10.1109/UVS.2019.8658279>

Ghering, M., & Poll, E. (2016). Evil Twin vulnerabilities in Wi-Fi networks. <http://www.cs.ru.nl/bachelorscripties/2016/Matthias_Ghering___4395727___Evil_Twin_Vulnerabilities_in_Wi-Fi_Networks.pdf>

Gandhi, C., Suri, G., Golyan, R. P., Saxena, P., & Saxena, B. K. (2014). Packet Sniffer – A Comparative Study. International Journal of Computer Networks and Communications Security, 2(5), 179–187.

Abramov, E., Kobilev, M., & Makarevich, O. (2013). Using quadrocopter as a pentest tool. SIN 2013 - Proceedings of the 6th International Conference on Security of Information and Networks, 404–407. https://doi.org/10.1145/2523514.2527019

Cangea, O. (2018). to Defeat Cyber Attacks. LXX(2), 29–37.

Čisar, P; Čisar, S. M. (2018). 9 Ethical Hacking of Wireless Networks in Kali Linux Environment. Annals of the Faculty of Engineering Hunedoara; Hunedoara, 16(3), 181–186.

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.

He, D., Chan, S., & Guizani, M. (2017). Drone-Assisted Public Safety Networks: The Security Aspect. IEEE Communications Magazine, 55(8), 218–224. https://doi.org/10.1109/MCOM.2017.1600799CM

Murphy, B. F. (2013). Network Penetration Testing and Research Major : Computer Science Program USRP Summer Network Penetration Testing and Research. 0–11.

Pesce, L. (2015). Drones for Pentesting ?

Stiawan, D., Idris, M. Y., & Abdullah, A. H. (2013). Attack and vulnerability penetration testing: FreeBSD. Telkomnika, 11(2), 399–408. https://doi.org/10.12928/telkomnika.v11i2.942

Sweigart, C. (2003). Interested in learning more ? In sti tu te , A ut ho ins ll r igh. Security 401, 1–39. https://www.giac.org/paper/gsec/3907/introduction-computer-security-incident-response/106281

Vinjosh Reddy, S., Sai Ramani, K., Rijutha, K., Mohammad Ali, S., & Pradeep Reddy, C. H. (2010). Wireless hacking-a WiFi hack by cracking WEP. ICETC 2010 - 2010 2nd International Conference on Education Technology and Computer, 1, 189–193. https://doi.org/10.1109/ICETC.2010.5529269

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

Warrior, C. (2014). New hacking scenario emerges : Wi-Fi signal-sniffing drones.