**Section B**

The research conducted for this thesis has been collected in all similar experiments conducted by various authors all used the quantitative approach. This was also used in my thesis where multiple scripts were created to conduct a penetration test on an access point. The scripts created gave out multiple results which were then all joined together to form a result report. The papers used offered multiple aspects and methods of how other people conducted similar ideas.

In a paper written by Abramov et al. (2013) the objectives of this paper are to describe how a small prototype was done by using UAVs as part of the penetration testing. This paper showed that the best possible way to conduct this type of attack was by conducting the experiment split into two parts. The first part was the scanning and data collection and the second part was the testing of the network. The author also emphasised that the use of a GPS in this kind of scenario very helps full in conduction the testing required. The paper proved that a test using drones can be success full when trying to test or hack an access point. In research done by Abramov et al. (2013), it has been noted an external battery source would be useful for the microcomputer to preserve the battery life of the drone. The research question for this paper was focused on if it was possible to conduct a network pen test using drones.

The research conducted by Murphy, B. F. (2013) mainly focused on testing and researching network penetration on devices. It is noted that multiple tools can be used to create an efficient attack which might lead to a vulnerability in a system. Murphy, B. F. (2013) emphasised that the most important test that needs to be done is network scanning due to this test exposing lots of information about the network under test. From Murphy, B. F. (2013) findings the most appropriate tools to be used for this test is Aircrack-ng, Metasploit, Nessus and Nmap.

Gergovemi, S., & Panchev, C. (2015) describes how our everyday life depends on wireless networks. It is noted that many of these devices can be vulnerable to dictionary attacks. With the use of a raspberry pi and a drone similar to the set up used by Abramov et al., (2013). By using Aircrack-ng which was also suggested by Murphy, B. F. (2013) it allowed the tester to collect the WPA passphrase and use it to connect to the network. The methodology used in this paper also contained a Man-in-the-middle attack which was done to capture, alter and inject messages in different hosts and clients. The conclusions of this test show that a cheap solution can be used to collect such data and it will cause a great impact if implemented with the use of a drone.

Yevdokymenko, M., Mohamed, E., & Onwuakpa, P. (2017) mainly focuses on ethical hacking and penetration testing with the use of a Raspberry PI with a similar testing scenario to previous works done by Gergovemi, S., & Panchev, C. (2015). Also as suggested by Murphy, B. F. (2013) the phase of reconnaissance and vulnerability scanning makes it evident that it is the most important phase for a vulnerability test to be useful and with the correct results. In the conclusion of the paper, it is emphasised that for a network to be secure penetration testing must be conducted to close all backdoors and fix any vulnerabilities.

The research was done by Wang, S.-L., Wang, J., Feng, C., & Pan, Z.-P. (2016) offers a clearer view of what attacks were needed to conduct a vulnerability assessment. The use of a man-in-the-middle attack is stressed since from the network traffic that is generated one can be able to discover passwords, URL surfing and also hosts that are being mostly used. From the testing conducted the Password discovery and the man-in-the-middle attack where successful. It was also noted that an external wireless adapter would be needed if the SSH connection would be required.

Westerlund, O., & Asif, R. (2019), with a difference from other studies the use of a wifi pineapple was included in the research question where it was used to conduct network auditing and investigation. The main attacks being done where DDOS, DE authentication and a man-in-the-middle attack. Apart from this one difference also stands out where telnet is mentioned as a vulnerability in a system that might be under attack. Seven experiments were conducted in total with the results being that all where successful.

Stiawan, D., Idris, M. Y., & Abdullah, A. H. (2013) the approach used by this study was done by using a pc to obtain data via Wireshark, TCPDump and NetMon where it was connected to a switch directly to LAN. This was done used to discover various servers and hosts which were used to conduct multiple attacks. Similar to Murphy, B. F. (2013) the research used similar to Nmap which provides similar results of the study of Murphy, B. F. (2013).

**Bibliography :**

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>

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

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.

Yevdokymenko, M., Mohamed, E., & Onwuakpa, P. (2017). Ethical hacking and penetration testing using raspberry PI. 2017 4th International Scientific-Practical Conference Problems of Infocommunications

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>

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>

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