IT-Project Report – Home assignment

Owen Scerri | IT-CSN-6.3B | 49399M

Link to Github Repo : <https://github.com/owen-scerri/Dissertation>

# Section A – Version Control

|  |  |  |
| --- | --- | --- |
| **Checkpoint** | **Deliverables** | **Commit Link** |
| 1 | Literature Review   * Should be documented in past tense * Circa 3000 words (recommended length) * References should be provided in context * Passive style of writing (no first person) * Tables and Figures might be added at this stage | <https://github.com/owen-scerri/Dissertation/commit/28aaa9a654fd41501c3b23deafed082cd30c070a>  **Comments :**  In this section a selection of papers was used in order to examine what past researches have conducted in a similar scenario. Various papers used different techniques in order to check weather penetration testing can be conducted using a Raspberry PI and a drone. Various attacks were discussed to outline the best solution to be conducted in this dissertation |
| 2 | Methodology   * Should be documented in past tense * Circa 2000 – 2500 words (recommended length) * Should include a description of the main test, details of the prototype being used (if applicable) , details of the experimental variables (if applicable), sampling techniques, details related to subjects being studied (if applicable) * Passive style of writing (no first person) * Tables and Figures might be added at this stage | <https://github.com/owen-scerri/Dissertation/commit/03f5addb0849d4d9ccdbbd071e742543392763b4>  **Comments :** The methodology on how the testing was done in order to obtain the desired results. This methodology includes details on how various scripts where created. Tools such as Aircrack-ng , Evil twin script , Nmap , macchanger , Arpspoof and tcp dump were used in order to obtain all the information needed where a final report will be represented with all the results joined together. |
| 3 | Interim Report (See Section B) | <https://github.com/owen-scerri/Dissertation/commit/995064da5c7a1caaee73fe47fd19bb7a6b83ce39> |
| 4 | Results and Discussion   * Should be documented in past tense * Circa 3000-3500 words (recommended length) * Results should be presented in the form of tables and graphs (no given fixed number – varies per dissertation) * References should be provided in context * Ability to compare and contrast your findings with existing empirical data and or existing literature should be demonstrated * Passive style of writing (no first person) * Tables and Figures might be added at this stage | <https://github.com/owen-scerri/Dissertation/commit/5025d7ed74e9dc2f64e0a1c29f93fb3cd334424e>  **Comments :**  In this document the results that were obtained during the tests were discussed and analysed in detail. Tables and a Graph was used to compare each test more easily and point out various important factors that were evident during the testing phase. The findings found from the results where compared to other researchers’ paper. It was found that some papers had similar results which confirmed that the results obtained were correct. Furthermore, the prototype was discussed where it was stated that the two technologies can be integrated and used together. In order to answer the research question in the concluding part of this section it was stated that with various tools it was able to conduct such research possible. |

|  |  |  |
| --- | --- | --- |
| 5 | Conclusion, Introduction, Abstract   * Should be documented in past tense with some possible use of present / present continuous * Introduction should contain (a) a definition of the problem (b) motivation behind the research (c) a definition of the research objectives (d) a section describing the various chapters in your study. * Conclusion should contain (a) summary of the findings (b) recommendations for future research (c) an evaluation of the findings outlining the strengths/weaknesses of the research * Abstract should contain a summary of the dissertation with highlights from the study. (500 words – recommended length) * References should be provided in context * Passive style of writing (no first person) * Tables and Figures might be added at this stage | Introduction  <https://github.com/owen-scerri/Dissertation/commit/7aa4b1b6f0cc8a3329acf30588fda59b23dd0e1b?diff=split>  Abstract  <https://github.com/owen-scerri/Dissertation/commit/fbe528912cf1994899be20cea3e7a380732c6424>  Conclusion  <https://github.com/owen-scerri/Dissertation/commit/dc796223912e199f0c6fdf4906a500d1e2e0f432>  **Comments :**  The introduction , conclusion and recommendation section includes a summary of all the findings that were found during the tests conducted. It outlines that the hypothesis question was addressed and verified that it was true. The strengths of the results found is that most of the tests conducted were successful and also shows that a drone and a Raspberry PI can be used in order to conduct penetration testing on a system. Limitations were noted and discussed.  A short summary of the dissertation was written were the scripts created were mentioned with their main functionality. This allows a reader to know what is expected from the dissertation and a quick view of what was the methodology used and results obtained. |
| 6 | * Final Report (See Section C) * Completed Implementation (if a prototype was created) | <https://github.com/owen-scerri/Dissertation/commit/c64902d7f677e589245c650442599d6ae525ecb3>  Implementation  <https://github.com/owen-scerri/Dissertation/commit/600e18255c1f3832d0ddcc5698c12757fb085b49> |

# Section B – Interim Report

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

# Section C – Final Report

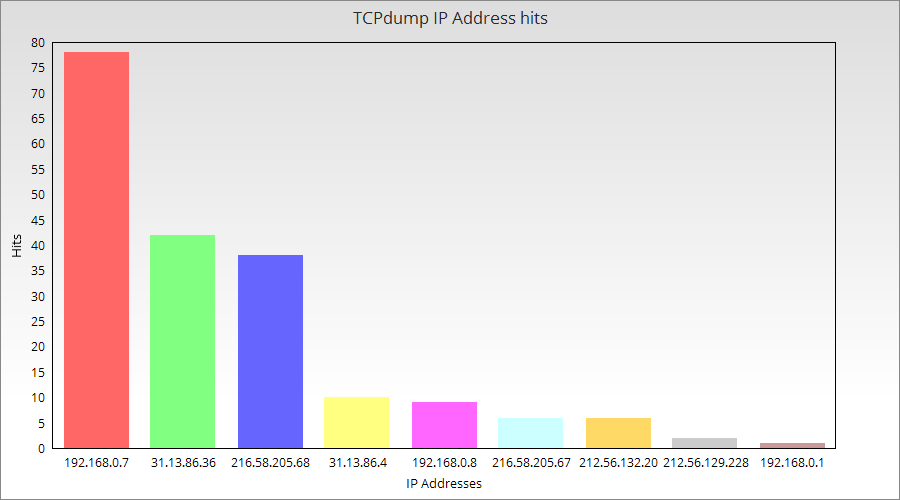
For the first attack in order to obtain the passphrase of the network two attacks was used to be able to compare results together. In the table below one can find what results where obtained from the attacks that was conducted. during the first phase of the script. These attacks were also researched by Murphy (2013) noted that a primary tool which conducts the possibility of such attack is the Air-crack-ng. 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 was also visible in the method of experiment used in this dissertation where the key was obtained from the handshake that was captured.

|  |  |  |
| --- | --- | --- |
|  | **Aircrack-ng (Dictionary attack)** | **Evil Twin Attack** |
| **Script Setup** | The script was initiated where the strongest AP was chosen automatically | The script was deployed, and the penetration tester had to choose the desired AP |
| **Access Point BSSID** | 2C:99:24:65:84: A9 | 2C:99:24:65:84: A9 |
| **Client MAC** | FC:DE:90:79:64:A9 | FC:DE:90:79:64:A9 |
| **Success?** | It was successful | It was successful |
| **Time is taken for an attack** | To obtain handshake 5 minutes, the time taken for an attack to crack the password took around 9 hours | The total time taken for the evil twin attack to crack the password was around 7 minutes. |
| **Efficiency** | Such an attack is more efficient as it is much simpler and is user friendly.  A downside of this attack is that although it is efficient, it takes a lot of time to construct such an attack. | Such an attack is much more complex to obtain the password.  In comparison to the Aircrack-ng, the Evil Twin attack took fewer minutes to perform. |
| **Output Password** | The output password was displayed on the screen | The output password was saved in a log file |
| **Handshake needed?** | Handshake is required | Handshake is required |

During the second attack a Nmap scan was conducted in order to obtain vulnerabilities and hosts in the network as can be seen in the table below. Similar to, Westerlund, O., & Asif, R. (2019) the tool used for this attack was the same tool used by this researcher. Furthermore, the importance of scanning was noticed in , Westerlund, O., & Asif, R. (2019) and Yevdokymenko, M., Mohamed, E., & Onwuakpa, P. (2017) papers. Both tests were success full and the time taken for each scan to be conducted was dependent on the complexity of the scans.

|  |  |  |
| --- | --- | --- |
|  | **Simple Nmap Scan** | **Vulnerability Nmap Scan** |
| **Test successful?** | Yes | Yes |
| **Time** | The simple Nmap scan takes minimum time. Hence, the penetration tester could use the information obtained in the next attacks. | The vulnerability Nmap scan takes more time to check and establish all vulnerabilities. |
| **Looking for targets** | In order to look for targets, such scan created a simple list of all the required hosts and ports. | In order to look for targets, this scan created a list with known vulnerabilities of the hosts. |
| **Use** | This scan is used to identify the topology of the network behind the access point. | This scan is used by a penetration tester. This tester can conduct any suggested tests on the host indicated in this scan. |
| **All hosts discovered?** | Yes | Yes |

The results obtained from the Man-in-the-middle attack was given out network captures where it is not possible to be translated into tables. In the screenshot below one can see that the user was using Facebook whilst the attack was ongoing. The paper written by Westerlund, O., & Asif, R. (2019) offered a brief example of how a man in the middle attack can be used where an attacker is acting as a middle node for the connection between 2 devices.

The graph below shows the IP addresses vs hits amounts in order to see which server was being used the most.

In conclusion the these results the testing was successfully done where the drone was able to be used as a penetration testing device. This kind of device offers a new way of hacking where it can be researched further in order to outline what can be done to avoid such a hacking to happen.