# Section C – Final Report

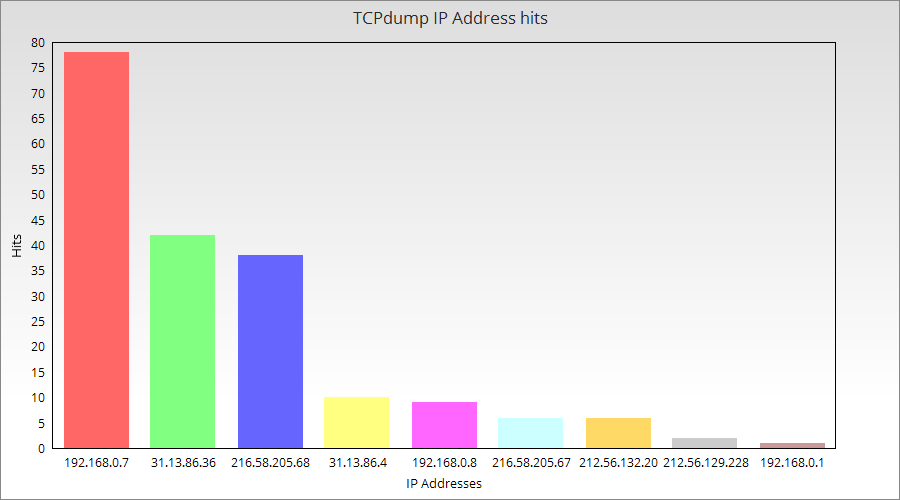
For the first attack in order to obtain the passphrase of the network two attacks was used to be able to compare results together. In the table below one can find what results where obtained from the attacks that was conducted. during the first phase of the script. These attacks were also researched 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.