Is your Wi-Fi really protected?

Author: Johnathan R. Santiago Laguna
Advisor: Prof. Jeffrey Duffany
Electrical and Computer Engineering and Computer Science Department

Abstract

The purpose of this project will be testing a tool called 'aircrack-ng suite' and performed a penetration test to a private network. This suite is a collection of tools that allows you to assess the strength of your Wi-Fi security. This suite includes the tools airmon-ng, airodump-ng and aircrack-ng that are used to penetrate a home network cracking the key. For the project, I selected a small home network that only connect computers, smart tv, phones and printers. The owners of this network were aware of the attack and gave necessary permissions. This project intends to test how secure using WP2 protocol could be for a home network, create security awareness for people to protect their privacy and information.

Introduction

For this project, I decided to use is the capture the 4-way handshake between the target host and the network router. What it's a handshake? A handshake is when a device connects with an AP there's where the 4-way handshake is executed. The handshake shares information between the AP and the device that is trying to connect to it. In Figure 1, we show the topology of the network select to attack in this project. The diagram shows how the devices are connected and the information of each connected host. The host Apple Computer is the victim who once I'm inside the network, uninvited, I'm going to sniff, monitored and capture the traffic that allow to be examined and possible extract credentials in plain text from it.

In wireless security exists 3 major security protocols that are used in variety of networks. The wireless security protocols are WEP, WPA and WPA2, serving the same purpose but being different at the same time. As explained by IPCisco [1], has developed in 2006. It was advanced version of first WPA. Vulnerable parts of WPA become stronger with WPA2. WPA2 offered new encryption and authentication mechanisms to provide more secured networks. These mechanisms were AES (Advanced Encryption Standard) and CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol). These mechanisms were being used instead of previous mechanism TKIP. For interoperability, TKIP was also used but as a fallback. Dictionary Attacks are the most vulnerable part of WPA2 for passwords. For this purpose, the network we selected for this project is currently using WPA2. Theatrically speaking WPA2 is the hardest and tedious protocol to crack and access a network using it. Performing the dictionary attack to this network, in this project we can proof the point that WP2 has its vulnerability and is not secure for enterprise networks.

Background

The main topic for this research are cybersecurity, networking, Linux operating system and hacking. This could be helpful for students or professional in the field of computer science, cybersecurity and networking. Also, could serve as a case studies for nontechnology users and the best use of the technology.

Problem

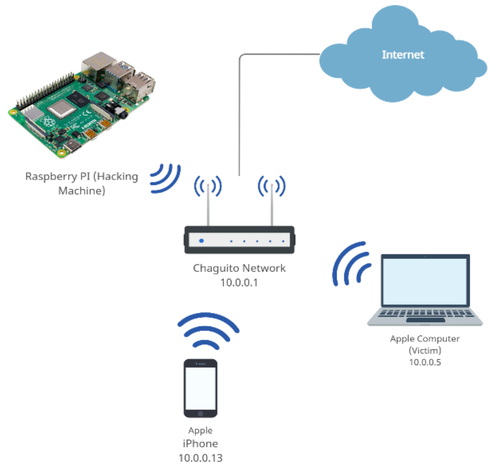
This research expand the knowledge to people about what is wireless security, the importance of it. Create awareness on the use and creation of complex password. Regular users rely on defaults password or avoid using complex password worrying of forgetting. Showing how traffic can be control and manipulated to gather arbitrary information could demonstrate to users we are not that secure, even though we think we are.

Methodology

The methodology used on this project was an exploratory research. I select a home private network to try to crack the password using a complete suite of Wi-Fi cracking tool. I didn't have any previous knowledge of the targe network regarding topology, architecture or configuration nor the tools tested in this experiment. All information was gathered during the recognition process.

Results and Discussion

The results of this project were impressive from a network security perspective. We successfully crack the password of a home private network, manipulate the traffic for one of the connected devices and almost gather accounts credentials from the user. We proved that the tools I tested are powerful, robust, and accurate. I think this project can demonstrate that any security is not perfect security nor can be trusted. The password "santiago1405" was used to enter to the network. The connected host selected to manipulate was the apple computer.



Being inside the network let me to recreate the network topology as show above, this led me to analyze how the network was configured and how the traffic is managed.

Conclusions

From the non-technical user standpoint, a project like this can opened their mind to be more serious and aware about things they can do to reinforce their security. The digitalization is transforming the world in light speed, network security and other aspect of computer security are in the highest demand being the number one treat to any business, person or entity. Security professionals are making the best effort to create awareness in the people in how important security is and what are the best practices to implement in our lifestyle. But most importantly is our responsibility to keep learning and give security the importance in should have.

As a lesson learned from this project, we see the importance of creating complex password for any digital account or device. A complex password must be created containing combination of letter, numbers, symbols and a length of more than 10 characters.

Future Work

This project fulfilled the purpose of demonstrating that WP2, being the most secure of all network protocols, can be vulnerable and cracked. Most importantly, the results of this project serve as inspiration and open new opportunity in research and investigation in newer protocols being in develop like WP3 and that will be the new standard in a near future. We are living in a world that just one single vulnerability is all an attacker needs.

Acknowledgements

This project was possible with the help of my mentor Prof. Jeffrey Duffany

References

[1] Ipcisco. "Wireless security protocols." Ipcisco.com. Sept. 15, 2020. [Online]. Available: https://ipcisco.com/lesson/wireless-security-protocols/

[2] S. Klimaszewski. "Raspberry pi." Kali. Oct. 14, 2021. [Online]. Available: https://www.kali.org/docs/arm/ raspberry-pi/

[3] Aircrack-ng. "Aircrack-ng." Aircrack-ng.org. Sept. 18, 2019. [Online]. Available: https://www.aircrack-ng.org/doku.php?id=aircrack-ng

[4] Hoffman, C. "What Is an SSID, or Service Set Identifier?" How-To Geek. Dec. 5, 2017. [Online]. Available: https://www.howtogeek.com/334935/what-is-an-ssid-or-service-set-identifier/

[5] Nmap.org. "Nmap network scanning." Nmap.org. 2000. [Online]. Available: https://nmap.org/book/man-host-discovery.html

[6] Wireshark. "Go Deep." Wireshark. 2020. [Online]. Available: https://www.wireshark.org/index.html#about WS