

1. Introduction

Due to the increase of home users that are connected to the internet, the author had focused this project on home security vulnerabilities. This let to investigate security issues to provide protection to secure a user data on home networks. In order to secure a network, it requires two methods to complete it. Research on previous studies to understand and carry out experiment to test network to provide solutions to address vulnerabilities, threats and risks targeting a home network technology. In completion of the project, the author hoping to achieve target and this has had achieved because all the experimentations completed with success.

2. Aim & Objectives

The aim is to conduct an experiment to address security vulnerabilities, threats and risks targeting a home network technology.

- Literature review of books, journals and articles
- Identify vulnerabilities, attacks and threats
- Critical review of previous studies on network security problems
- Design and implement a network
- Experiment with a combination of software and hardware equipment to test
- Test and evaluate findings & make recommendations for future improvements.

3. Sources

Books, journals, articles and any other sources that related to home network security. This helps to understand the type of vulnerabilities, threats, attacks and risks that home user faces on daily basis when connected to the internet to provide solutions [1-4].

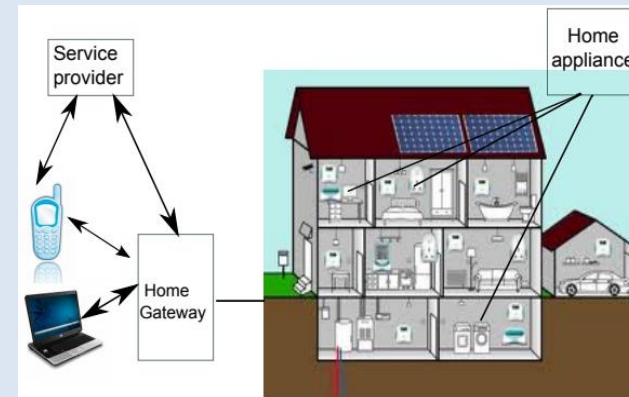


Figure 1: Smart Home Design [5]

4. Design & Implement

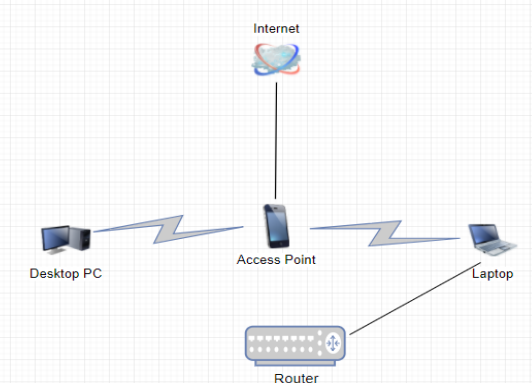


Figure 2: Smart Home Design

5. Experiments

The author conducted 3 methods of experimentations. The results shows on 6, 7 & 8 section. The methods which are WPA2 password crack, man in the middle attack and port scanning. All carried via Kali Linux operating system.

6. WPA2 Crack

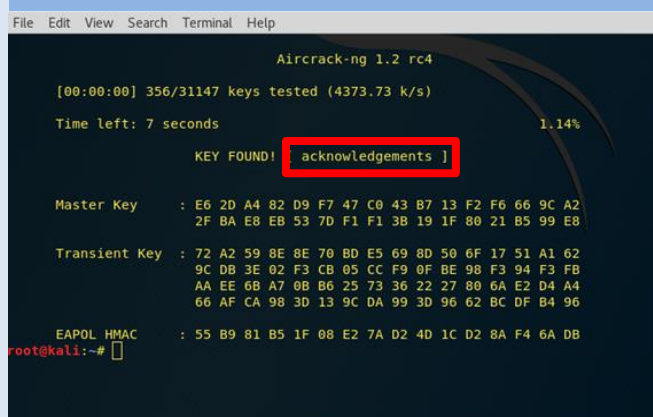


Figure 3: Smart Home Design

Figure 3 shows result of Key found which is as “acknowledgements”.

7. MITM Attack

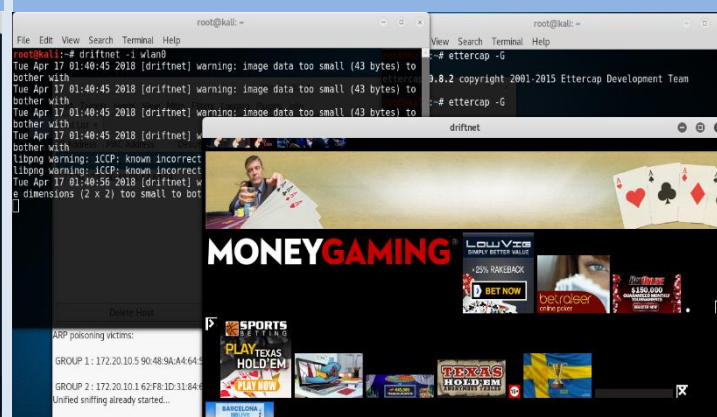


Figure 4: Smart Home Design

Figure 4 shows result of sniffing and capturing images from targeted device via driftnet.

8. Port Scanning

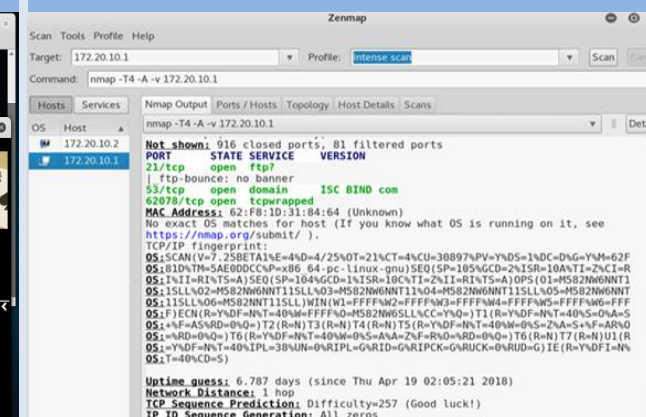


Figure 5: Smart Home Design

Figure 5 shows port scanning results which conducted via ZenMAP method.

9. Conclusion

Overall, this project has completed successfully. As the author being able conduct three different types of experimentations. Which shows in the results on figures 3-5, all of them were successful. In the future, the author is aiming to learn more about home network in order to provide better network to project home user data. As home networks have greater risk the business according to research findings during this project.

10. References

- [1] Z. C. Schreuders and A. M. Bhat, “Not All ISPs Equally Secure Home Users An Empirical Study Comparing Wi-Fi Security Provided by UK ISPs,” *2013 Int. Conf. Secur. Cryptogr.*, pp. 1–6, 2013.
- [2] C. Routh, B. Decrescenzo, and S. Roy, “Attacks and Vulnerability Analysis of E-Mail as a Password Reset Point.”
- [3] M. M. Najafabadi, T. M. Khoshgoftaar, C. Calvert, and C. Kemp, “Detection of SSH brute force attacks using aggregated netflow data,” *Proc. - 2015 IEEE 14th Int. Conf. Mach. Learn. Appl. ICMLA 2015*, pp. 283–288, 2016.
- [4] N. Gelernter, S. Kalma, B. Magnezi, and H. Porcilan, “The Password Reset MitM Attack,” *Proc. - IEEE Symp. Secur. Priv.*, pp. 251–267, 2017.
- [5] S. Ruj, A. Nayak, and S. Naik, “Securing home networks using Physically Unclonable Functions,” *ICUFN 2012 - 4th Int. Conf. Ubiquitous Futur. Networks, Final Progr.*, pp. 288–293, 2012.