Universiti Teknologi MARA

Proof of Concept: Attack on Wireless Environment through Wi-Fi Spoofing

Aizlan Nizam Bin Hamidon

Thesis submitted in fulfilment of the requirements for

Bachelor of Computer Science (Hons.) Data Communication and Networking

Faculty of Computer and Mathematical Science

July 2020

ACKNOWLEDEGMENT

Alhamdulillah praises and thanks to Allah because of His Almighty and His utmost blessings, I was able to finish this research within the time duration given. My special thanks goes to my supervisor, Mohamad Yusof Bin Darus for all the tips, encouragement and guidance throughout my Final Year Project that really helped me prepared this proposal with correct ways.

Special appreciation also goes to my beloved parents, who always gave me motivational support whenever I need them. Without their love and support, I might not able to finish up this proposal.

To those who I accidentally left out, my deepest sorry and gratitude for the support and encouragement shown to me with or without concerns.

ABSTRACT

This project aim is to proposed proof of concept of the vulnerability of public Wi-Fi network through spoofing of Access Point (AP). It is already 2020 but due network nature itself, user rarely able distinguish if he/she connect to legit AP while scanning for free public network provided at Café or Fast food restaurant. Worst scenario happen is rogue AP design with same parameters of real AP including ESSID, BSSID and Channel Number make it not too obvious as a medium for the attacker to sniff and capture sensitive data whenever user stroke the user and password credentials. This proof of concept needs to meet objectives of this project. The objectives of this project are to attack, spoofed a legit AP using same SSID information and sniff the deauth packet frame using sniffing tools. A scenario of attack simulation is recreated using Kali Linux and Rogue AP on same network. The attack simulation generate a result where packet frame are sniff and captured using Wireshark, giving credentials information of user and password login data. To help secure the connection of the user while browsing the website through public network, users are recommended to install and browsing using the VPN.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

In this chapter, research project objectives' and aim were identified by problem statements made. Project scopes were listed to give readers an overview of what will be covered in the research project. Then, significances of research project were included in this chapter.

1.1 Background of Study

According to Melanie Pinola (2020), Wi-Fi is a wireless local area network protocol that allows devices to access internet without direct cable connections based on the 802.11 IEEE network standard. Wi-Fi works by a router or any electronic mobile that have features to transmits an internet connection to nearby devices that can reach the wireless signal. A wireless access point (AP), allows wireless devices to connect wireless devices by taking the bandwidth from a router and stretched the network from farther distances away.

Based on an article written by Alison Grace Johansen (2020), most free public WI-FIs was not secured even we need a password to have access to the connection. Public Wi-Fis are mostly have flaws in terms of their security features due to encryption protocol that used by that wireless networks. Some wireless networks may use older protocol standard for encryption in which causes some 'holes' in network such as Wireless Encryption Protocol (WEP) and Wi-Fi Protected Access (WPA). Besides, user joined a spoofed or rogue AP might contributed to vulnerability in wireless environment. Free Wi-Fi lure unsuspecting victims to join fake AP created by attacker and next performing man-in-the-middle (MITM) attack.