INSE6120 - Fall 2016 - Projects

1.- Team:

* Lino Antonio Nava Romero - Student ID: 27655975

2.- Project Proposal:

For my project I am going to work with an implementation (field study) project, precisely the option called “Free Wifi”. Everyday we find business offering free internet access as a additional services. Usually this connection are open and everybody who are near the place can access this but are we sure this free hotspot are totally secure?.

In this project I am not going to focus on how to perform attack against Wireless Access Point, the goal of this project is to evaluate how safe are these connection, We want to know if they are gathering information about us? Or injecting content to our browser? Additionally What can a malicious user can do? Can a malicious user eavesdrop our communication or alter it?.

There are some aspect to take in consideration:

1) Just perform my test in business wireless hotspots (restaurants, coffee shop, shopping malls, etc) and not against home private connections.

2) Wireless hotspots without password requirement (or with a captive portal that require a username and password) this is trying to mimic the behaviour of final user who requiere free internet. But hotspot that requiere personal information to give you access are ok (this count as an information gathering hotspot).

3) I am not going to execute any attack agains the AP (Access Point) or STA (Stations), that means Death, Man in the Middle or crack password. My goal is to test if my connection using these network are secure not crack them, but It’s valid to use scanners, change my wireless adapters settings, etc.

Into the goals of the projects are:

1) Categorize how grade of security have a wifi hotspot and describe how percentage of hotspot gather information, how many inject any kind of contents (ads, javascript files, etc), how many use any kind of proxy to alter https communication (man in the middle), etc.

2) Create an evaluation plan to use it for performing my test against different hotspot.

3) Propose some recommendation to make user connection more secure.

I am going to divide the project execution in different stages (and these are going to be describe it into the final report).

1) Stage 1 - Research, Lab Environment and Evaluation Plan: Here I am going to collect all the information possible and decide what cause makes a hotspot insecure, conduct different Labs test to simulate various hotspot condition and start to elaboration my evaluation plan.

2) Stage 2 - Field Studies - Wardriving: start collecting Wireless Networks location to later pre select which wireless networks audit by different criteria, discard home wireless network (maybe by SSID or by Zone). Additionally here I want to select a couple of hotspot from different Chain Stores

(McDonalds, Starbucks , etc) because I have a doubt is their wireless configuration is different by location or they have the same configuration.

3) Stage 3 - Field Studies - Conduct Test: Perform the different test against selected free wireless hotspots.

4) Stage 4 - Final Report: As stage name , write the final report.

3.- Tools and Hardware:

A list with different tools and hardware that I estimate I am going to use during my work, any additional tool should be mentioned in the report.

- **Kali Linux:** Preferred Linux distribution for audition and testing.
- **Python:** high-level programming language, use to automate tasks or scripting, its contain different libraries and toolkits as dnspython, python-wify, scapy, etc.
- **Kismet :** an open source Wi-Fi stumbler, to perform.
- **Wireshark**: network protocol analyzer.
- **Alfa Awus036NHA**: USB wireless adapter.
- **USGlobalsat BU-353-S4**: USB GPS Receiver.
- **Wifi Pineapple Mark V**: Wireless auditing box but for this project It's going to use it to perform wardriving stage.
- **Mikrotik Routerboard RB2011UiAS-2HnD-IN:** A highly customize router, that allow to create captive portal and it's going to use in lab test.

4.- References:

- Tunneling for Transparency: A Large-Scale Analysis of End-to-End Violations in the Internet. David Choffnes, Alan Misove, Taejoong Chung
- Wireless Hotspots: Current Challenges and Future Directions - Anand Balachandran, Geoffrey M. Voelker
- "Free" Wi-Fi from Xfinity and AT&T also frees you to be hacked - http://arstechnica.com/security/2014/06/free-wi-fi-from-xfinity-and-att-also-frees-you-to-be-hacked/
- Why I don't use Airplane WiFi - https://blog.joemanna.com/dont-use-airplane-wifi-security/
- Public Wi-Fi hotspots – know the risks - http://www.welivesecurity.com/2014/11/14/public-wi-fi-hotspots-know-risks/