Snooping IoT Devices with Raspberry Pi

SAMUEL GODWIN ABU

Thesis presented in fulfilment
of the requirements for the degree of
Bachelor of Science Honours
at the University of the Western Cape

Supervisor: **Dr Michael Norman**
Co-supervisor: **Mr Muyowa Mutemwa**(CSIR)
Co-supervisor: **Mr Francois Mouton**(CSIR)
version date: July 27, 2018

Declaration

I, Samuel Godwin Abu, declare that this thesis *"Snooping IOT Devices with Raspberry Pi"*, is my own work, it has not been submitted before for any degree or assessment at any other university, and that all the sources I have used or quoted have been indicated and acknowledged by means of complete references.

Signature:..... Date:.....

Acknowledgement

This thesis was done with the support of Dr Norman. The weekly meetings and updates were of immense help. Thank you for your patience and awesome communication skills. I will also like to thank the CSIR team of Muyowa Mutemwa and Francois Mouton. Grateful for the updates and support.

Abstract

This thesis investigates the process of snooping IoT devices using a Raspberry Pi. The purpose of the project is to create Cyber Security Awareness and to demonstrate how easy it is to identify IoT devices over a WiFi network. This project will build an IoT snooping tool on a Raspberry Pi and track how many IoT devices the snooping tool detects in the process. The hardware and software tools (Kali Linux Penetration Testing tools) necessary to carry out this project will be documented. The process flow of the project from setting up the snooping tool up until the exporting of information gathered, will also be clearly outlined. The scope of the project is restricted to devices connected to a WiFi network like the WiFi-Support(Limited-Period) or the UWC-Campus.

Key words

snoop or snooping

Command & Control center or C&C

Raspberry Pi

terminal

access points

MAC address

target

vendor

Aircrack-ng

airodump-ng

Contents

List of Figures

1 User Requirements Document

1.1 Introduction

The world today is a world filled with countless connecting devices. Every other adult and teenager has a phone with internet connecting capabilities. A lot of people quickly connect without a second thought to WiFi networks that are not password protected not knowing the security risks they expose their devices to. According to Anthony Spadafora [9] writing for 'IT Pro Portal', Electronics manufacturers, Samsung is working on integrating the company's offerings under one application that will allow for seamless connection experience at home, at the office and even in cars. Such announcements make it easier to believe that there will most likely be more connecting devices all around us in the future. This project will showcase some security risks people with devices can face over a WiFi network.

1.2 User's view of the project

This project is done in conjunction with CSIR (Council for Scientific and Industrial Research). Below is a direct quote from the CSIR team.
"The aim of this project is to have the candidate build an IoT snooping tool on a Raspberry Pi and track how many IoT devices the candidate comes into contact with as they walk around campus.

- *Step1: Build an IoT snooping tool on a Raspberry Pi. Build a Command and Control machine which will communicate with the Raspberry Pi and keep track of information that is found.*
- *Step 2: Power the Raspberry Pi using a Power Bank.*
- *Step 3: Test and confirm that the snooping tool functions as designed.*
- *Step 4: The candidate should walk around campus especially in busy areas such as the Student Centre during lunch or lecture halls. The snooping tool should get the name of the device and send the information back to the Command and Control machine. The Command and Control machine should keep track of how many distinct devices of a certain type were found. If possible remove duplicates.*
- *Step 5: Document findings and educate students around campus."*

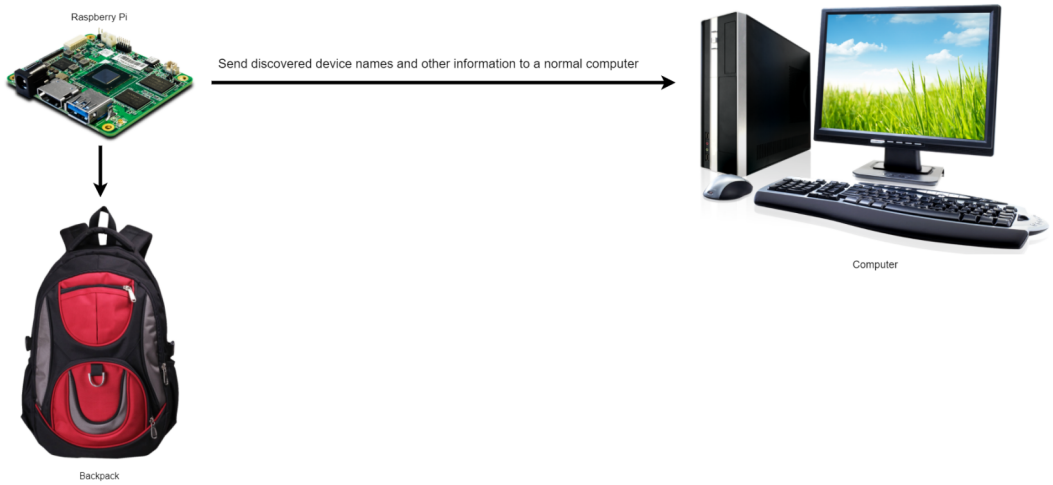

Figure 1: A simple illustration of the snooping tool

1.3 Description of project

The stakeholders (CSIR) require that an IoT snooping tool should be built on a Raspberry Pi. This Raspberry Pi will be used as a penetrating device to obtain safe information from penetrated devices over a WiFi network. This safe information will then be transmitted to a Command and Control center which is another computer. The stakeholder wants a list of encountered devices during the snooping. Figure 1 illustrates an overview of the task.

1.4 Limitations

A steady power supply is necessary to carry out this project. To be able to walk about campus (as required by stakeholders) with the snooping tool, a power bank and a small HDMI display monitor are necessary. The snooping tool thus comprises of the Raspberry Pi and a desktop monitor. These hardware tools require a power connection and thus limits the experiment to be conducted in one room, provided there are connected devices in the room. Another limitation might be setting up the Command and Control center but there might be a way around this hurdle.

2 Requirements Analysis Document

2.1 Purpose of project

The purpose of this project is to raise awareness about cyber security. Cyber security is not something users of devices often think about although some do. Functionality is what most users are more concerned about. The occurrence of data breaches has forced security to be an emerging priority. This project will show a scenario of how safe information can be obtained from IoT devices connected over a WiFi network with the intention of alerting users to issues of cyber security. This project will also show that a small device like the Raspberry Pi that can fit in a small backpack can be used as a penetration tool on connected devices over a WiFi network.

2.2 Scope of the system

The project will only cater for IoT devices connected over a WiFi network. The snooping tool will be implemented to function over a WiFi network. Snooping over a Vodacom or Telkom network should be considered outside the scope of this project. The snooping tool is not intended to perform in a malicious manner.

2.3 Objectives and Success criteria of project

The project will be deemed successful if the Raspberry Pi is successfully programmed to snoop connected devices over a WiFi network and keep track of some safe information about the devices encountered during the process. Another objective would be to set up the Raspberry Pi to send this collected and compiled safe information to another computer that will act as a Command and Control center.
The extent of snooping and the safe information currently is the type of discover-able IoT devices found over a network.

2.4 Designer's interpretation of user requirements

The stakeholders(CSIR team) listed a number of steps with which to proceed with the project. They are listed in the "User's view of the project" section of this document on page 1. Some of the hardware needed for a more accurate execution of the project are not currently available(such as Power Bank for USB Portable Power Supply). Hardware currently available are:
1. Raspberry Pi (see Figure 2)
2. 16GD micro SD Card (see Figure 3)
3. Desktop Computer at the Honours lab.

The Raspberry Pi does not have a display of its own. It is currently connected to a desktop monitor at the Honours lab. This means that the Command and Control center (Desktop Computer) and Raspberry Pi have to share the same monitor. So work cannot be carried out on both Raspberry Pi and Desktop computer (Command and Control center) at the same time. Internet access is also a necessity for the project and this is readily available at the Honours lab.

Figure 2: The Raspberry Pi

Software is also needed to execute this project. After meeting with the stakeholders, it was decided the Kali Linux operating system would serve best. Further research showed that the initial basic installation of Kali Linux OS on a 16GB micro SD card may not have all the functions required to commence with the experiment.

The 16GB micro SD card provided by the Department already had an operating system on it but the OS was not Kali Linux. The first task was to find a way to format the 16GB micro SD card and then install the basic Kali Linux OS which amounted to 4GB in size on that SD Card. See Figure 3 for a visual depiction of a micro SD card

Figure 3: The Micro SD card: the hard drive of the Raspberry Pi

2.5 Current System

Formatting the SD card was a success. Installation of Kali Linux and update to the full version was completed. The only drawback now is, the 16GB micro SD card is almost full. The full Kali Linux installation occupies 14GB of the 16GB micro SD card. This may not necessarily be a big issue but it is worth noting that the initial SD card is almost full and only installations have been done so far. The Raspberry Pi currently accesses the internet via the Ethernet cable at the lab. The Raspberry Pi is also WiFi capable.

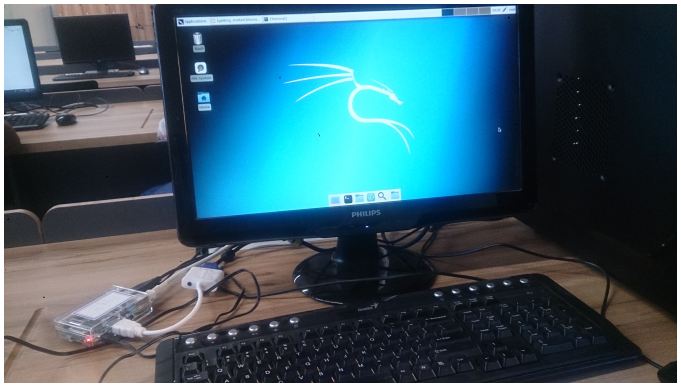

Figure 4: Current state of snooping tool

2.6 Proposed System

The snooping tool should be able to detect access points in a network. It should also detect connected devices on a network. The snooping tool should also be able to communicate with the Command and Control center (a desktop machine).

2.7 Requirements Analysis Conclusion

Current requirements gathered are for a simple implementation of the project. This simple implementation would be a snooping tool most likely without a power bank. Chances are if the tool can snoop while plugged to power(electricity), snooping on battery power can become a possibility.

3 Design Model

3.1 Data Design

The project requires that when snooping is being carried out, network access points should be discovered. These access points (e.g UWC-Campus) are the first piece of data encountered in a snoop operation. These access points can be described for the sake of this project as entry points for this snooping project. Upon discovering access points, the next step in the snoop process is finding out which access points are currently servicing connected devices or clients. For the access points that have connected devices or clients, the following step is choosing which of the access points to target.

The result of a successful snoop operation for this project is the MAC addresses of connected devices to targeted access points. These discovered MAC addresses will be converted to the names of the vendors that created the devices (e.g Apple Inc which is the vendor for Apple devices).

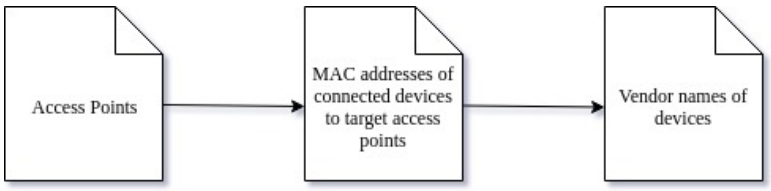

Figure 5: Data progression during course of project

3.2 Interface Design

There are quite a number of tools available in the Kali Linux OS library [4] that can be used for this project. Some of these applications have a designed UI (user interface) but a simple terminal based application would suffice. Initial testing done with a Kali Linux application named Wifite yielded very acceptable results. The interface of this project will be the terminal display of the Kali Linux OS.

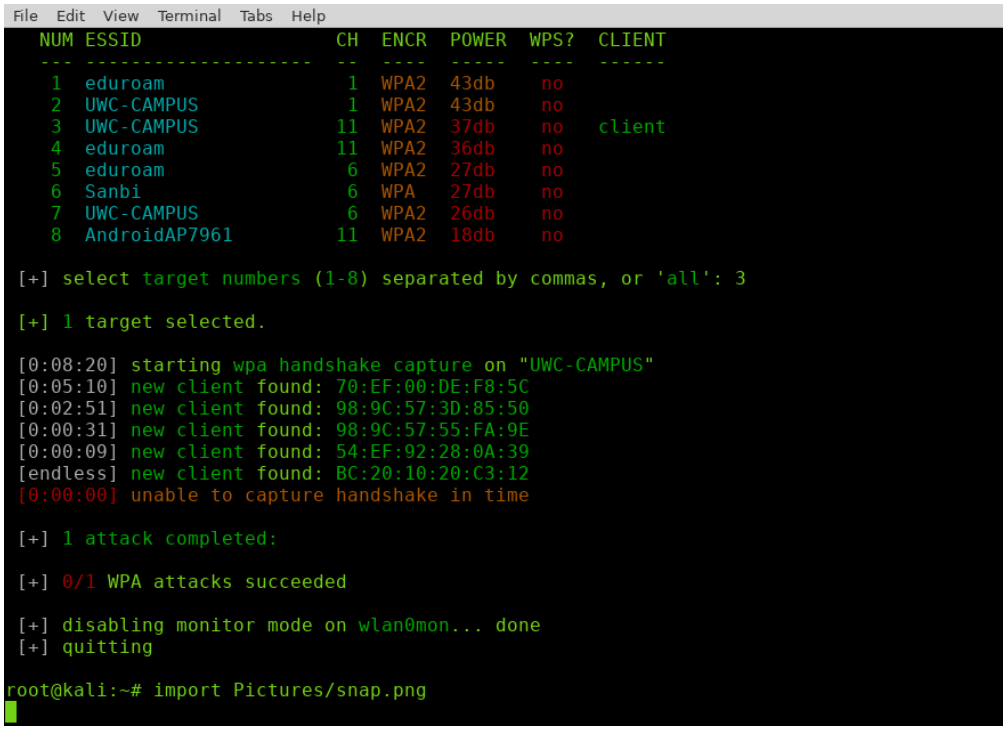

Figure 6: Interface of Prototype

3.3 High-Level Design

There are a couple of steps that need to occur for completion of the project. This steps begin with starting the snoop operation and concludes with the final formatted list of vendor names of devices discovered. Here are the steps necessary to complete a non malicious snooping operation(as shown in Figure 7):

- Begin Snoop Operation: *The Raspberry Pi is turned on and a Kali Linux ethical hacking application (e.g Wifite) is turned on. Discovered access point is selected to be targeted.*
- Save Findings: *The MAC Addresses of discovered devices on target access points are saved in a file*
- Run Python Script: *A python HTTP Requests script is used to send each MAC address to www.macvendors.com API which hosts an IEEE Standards Association list of vendors*
- Save formatted version of findings: *All returned responses from www.macvendors.com (which are now vendor names of discovered devices) are saved in a file*
- Run Python Script that sends formatted findings to Command & Control center

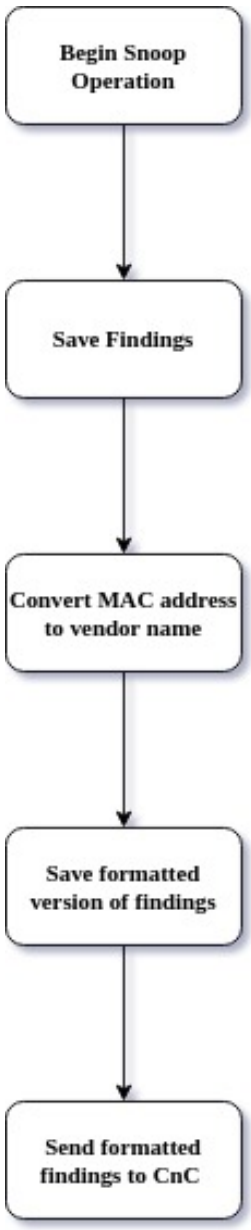

Figure 7: High Level Design of project.

3.4 Low-Level Design

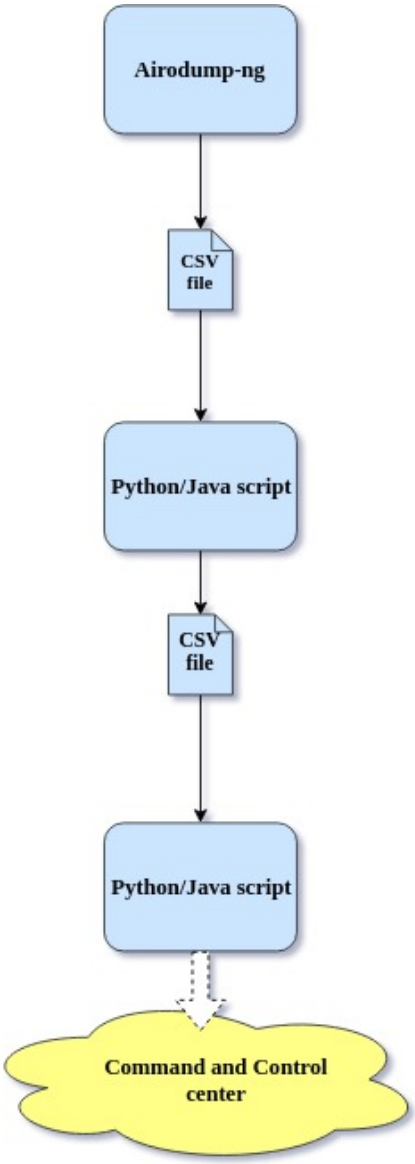

Figure 8: Low Level design of project.

A complete execution of this project includes the functionality of saving important data discovered during the course of a snoop operation. Kali Linux provides a plethora of tools to choose from to perform this project. These tools are known as **HCXtools**[4]. The HCXtool of choice for this project is **Aircrack-ng**[10].

Aircrack-ng is a set of tools that can be used to access WiFi security. Its functions include Monitoring, Attacking, Testing and Cracking. This project falls under the Monitoring category of functions that Aircack-ng provides. The goal is to monitor access points, capture packets and export important data for further processing. Aircrack-ng provides a tool named **airodump-ng**[8] and it is airodump-ng that allows for the exporting of data. Airodump-ng has a **-write** option that exports important data information to a CSV file. Data in the exported CSV file will include the MAC addresses of discovered devices. These MAC addresses in turn will then be used with a third party API to transform the MAC addresses to the name of the vendor that produced the device.

4 Prototype

The project is implemented using an evolutionary prototype. The prototype comprises of hardware components, software components and a python script.

4.1 Hardware

The hardware components consist of the following:

1. Raspberry Pi 3
2. Micro SD card
3. Desktop Monitor

The hardware components remain the same from prototype till final product.

4.2 Software

An application known as Wifite[5] which is available on the Kali Linux OS is the application in use for the prototype. Wifite is able to detect access points and also discover MAC addresses of devices on a target access point. The MAC addresses detected would then be converted into the vendor name of the device.
The software components for the prototype are:

1. Kali Linux Operating System
2. Wifite

The conversion of MAC addresses is done using an API provided by Nivel Technologies Ltd[7]. The API provided by Nivel Technologies uses HTTP requests to their server. If the vendor is found in their list of IEEE Standards Association list, a string is returned with the name of the vendor of the MAC address that was sent with the HTTP request.

Nivel Technologies run a website www.macvendors.com and they provided a PHP GET example which for the sake this project has been converted to the Python language. Below is what a simple Python HTTP request to the API looks like:

```python
#importing requests library
import requests

#device unknown message
error = "{\"errors\":{\"detail\":\"Page not found\"}}"

#api-endpoint
URL = "http://api.macvendors.com/"

#mac address of discovered device
macAddress = "98:9C:57:3D:85:50"

#mac vendors API requires concatenation of url and device mac address
payload = URL + macAddress

#sending get requests and saving the response as response object
r = requests.get(url = payload)

#print response STRING which should output device vendor
if r.text == error:
        print("vendor not found");
else:
        print("Device MAC address: " + macAddress)
        print("Device Vendor: " + r.text)

```

Figure 9: Prototype Python HTTP request script converting MAC address to vendor name

Figure 10 shows the display from the Python HTTP request script written and used with the prototype.

```
abu@abu-Inspiron-3542:~/Documents/Python$ python3 macDemo1.py
Device MAC address: 98:9C:57:3D:85:50
Device Vendor: HUAWEI TECHNOLOGIES CO.,LTD
abu@abu-Inspiron-3542:~/Documents/Python$
```

Figure 10: Python HTTP request script returns vendor name

References

[1] Ethical Hacking and Penetration Testing. *How to Hack Wifi*. https://miloserdov.org/?p=659, Last accessed on 2018-07-10.

[2] Ethical Hacking and Penetration Testing. *Programs for Hacking Wifi*. https://miloserdov.org/?p=674, Last accessed on 2018-07-9.

[3] Hack Method. *Wireless Hacking Tutorial*. https://hackmethod.com/wireless-hacking-tutorial/, Last accessed on 2018-07-19.

[4] Kali Tools. *Kali Linux Tools Listing*. https://en.kali.tools/, Last accessed on 2018-07-13.

[5] Kali Tools. *Wifite, Wifite Package Description*. https://tools.kali.org/wireless-attacks/wifite, Last accessed on 2018-07-13.

[6] Kamil's Lab. *How to perform a Pixie Dust WPS attack using the Raspberry Pi*. http://kamilslab.com/2016/01/01/how-to-perform-a-pixie-dust-wps-attack-using-the-raspberry-pi/, Last accessed on 2018-07-11.

[7] Nivel Technologies. *MAC vendors API*. https://macvendors.com/api, Last accessed on 2018-07-13.

[8] Penetration Testing Tools. *Airodump-ng*. https://en.kali.tools/?p=367, Last accessed on 2018-07-13.

[9] Anthony Spadafora. *Samsung lays out its vision for the future of IoT*. https://www.itproportal.com/news/samsung-lays-out-vision-for-future-of-iot//. Accessed: 2018-04-15.

[10] Penetration Testing Tools. *Air-crack-ng*. https://en.kali.tools/?p=57, Last accessed on 2018-07-15.