Term 2

Snooping IoT devices with a Raspberry Pi

a UWC/CSIR project

Hi,

Name: Samuel Abu

Supervisor: Dr Michael Norman

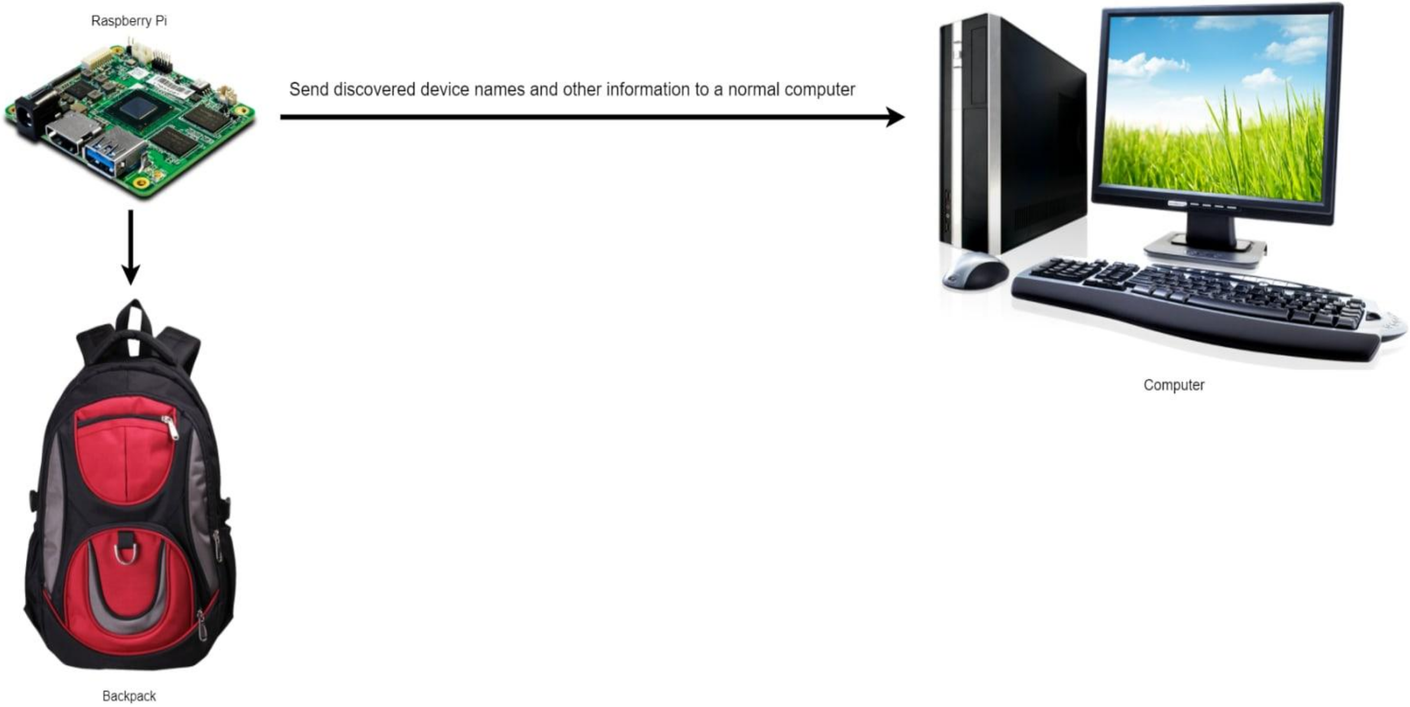
Co-supervisor: Muyowa Mutemwa (CSIR)

Co-supervisor: Francois Mouton (CSIR)

Overview

- Recap
- Interface Design
- High Level Design
- Data Design
- Low Level Design
- Prototype
- Project Plan
- References

Recap



Raspberry Pi

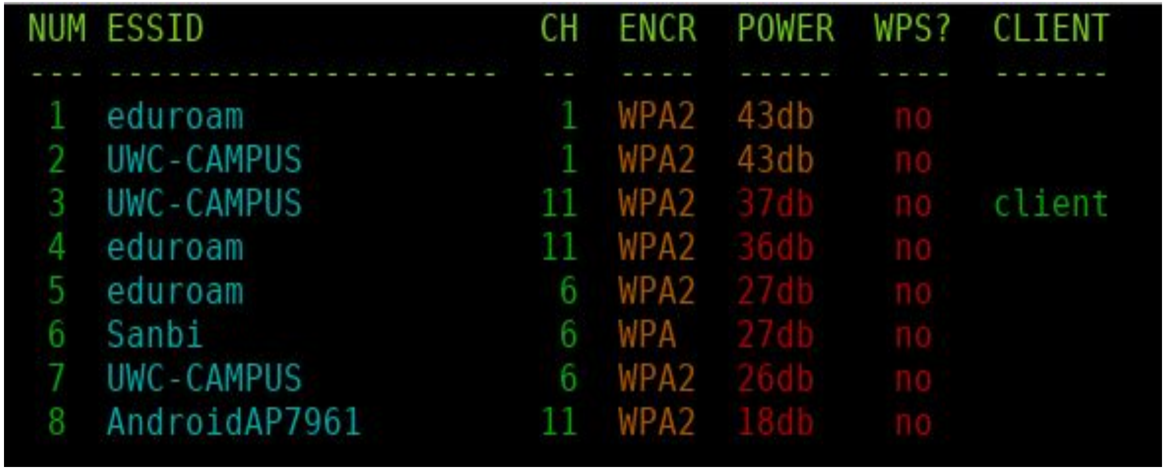
Send discovered device names and other information to a normal computer

Computer

Backpack

Interface Design

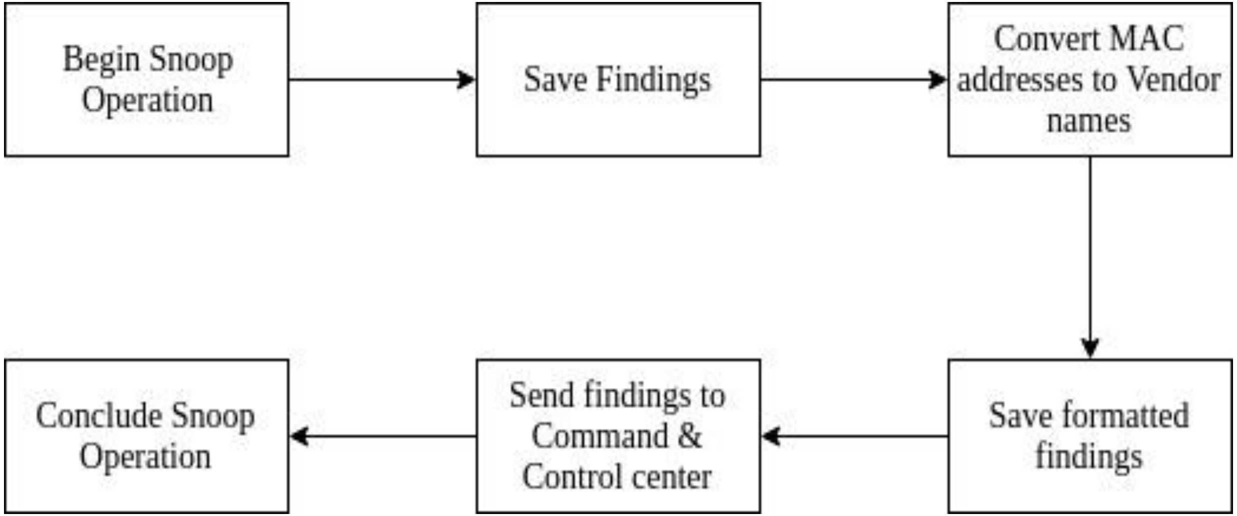
Current research and testing with Wifite have been carried out via terminal on the Kali Linux OS



```
NUM ESSID                 CH  ENCR  POWER  WPS?  CLIENT
--- --------------------  --  ----  -----  ----  ------
 1  eduroam                1  WPA2  43db    no
 2  UWC-CAMPUS             1  WPA2  43db    no
 3  UWC-CAMPUS            11  WPA2  37db    no   client
 4  eduroam               11  WPA2  36db    no
 5  eduroam                6  WPA2  27db    no
 6  Sanbi                  6  WPA   27db    no
 7  UWC-CAMPUS             6  WPA2  26db    no
 8  AndroidAP7961         11  WPA2  18db    no
```

Wifite terminal interface showing list of discovered Access Points

High Level Design



Begin Snoop Operation

Save Findings

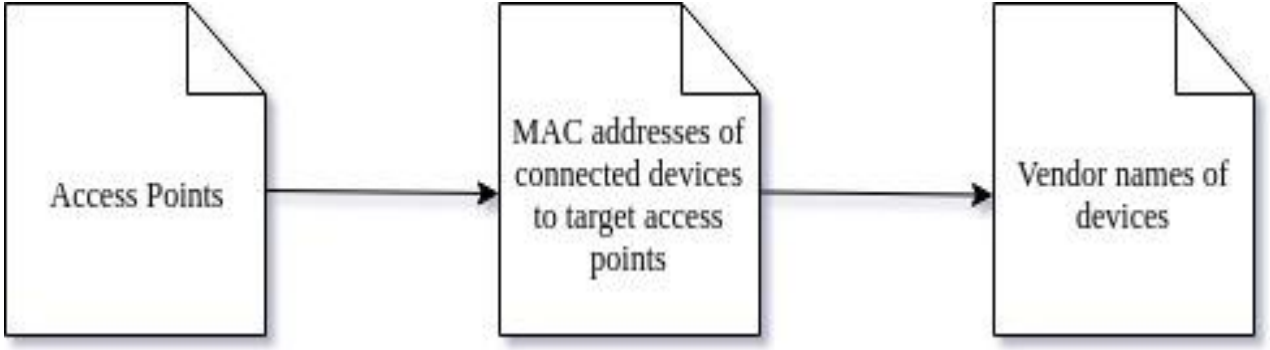
Convert MAC addresses to Vendor names

Save formatted findings

Send findings to Command & Control center

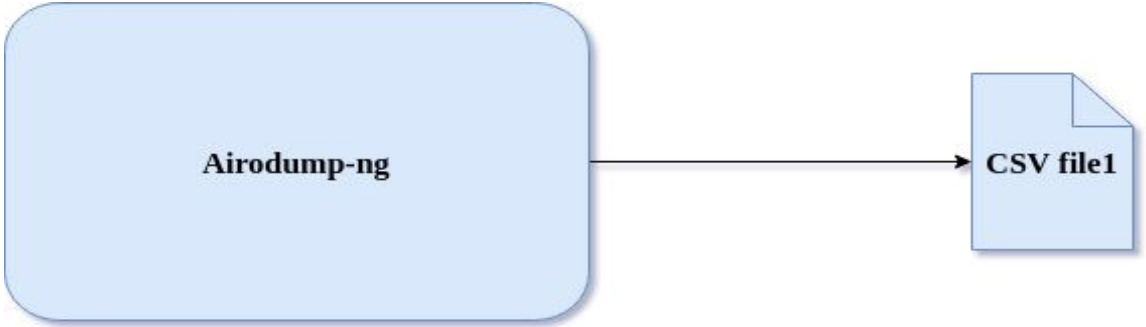
Conclude Snoop Operation

Data Design



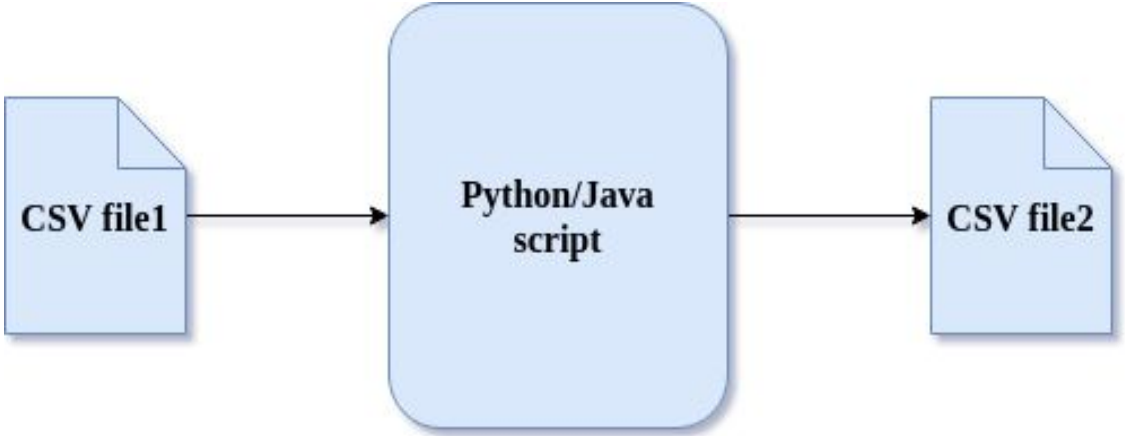
Plan includes the possibility of saving all the necessary pieces of data and compiling it into meaningful information.

Low Level Design



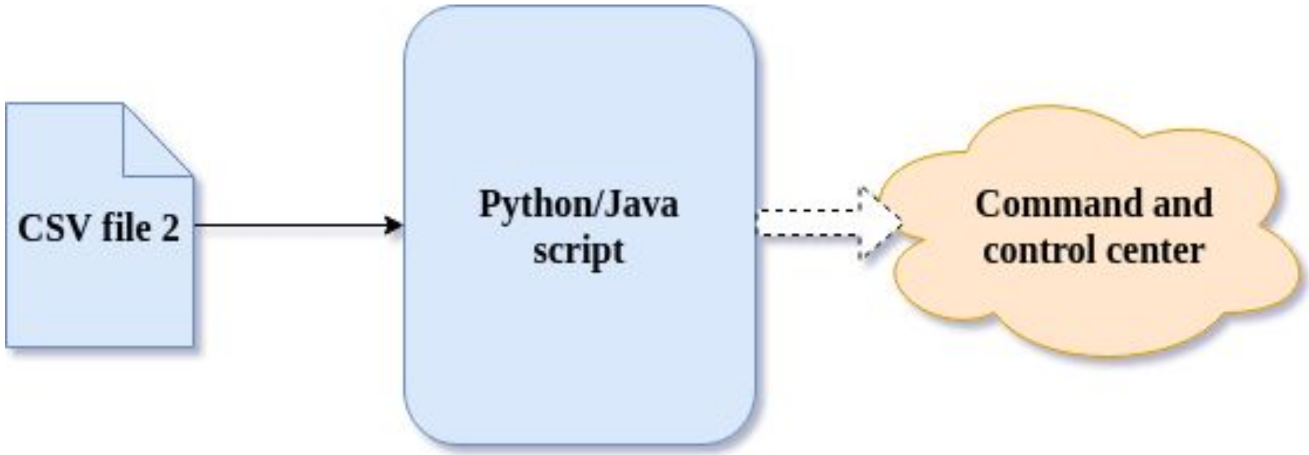
Airodump-ng will detect access points and MAC addresses of client devices connected to access points.

Low Level Design



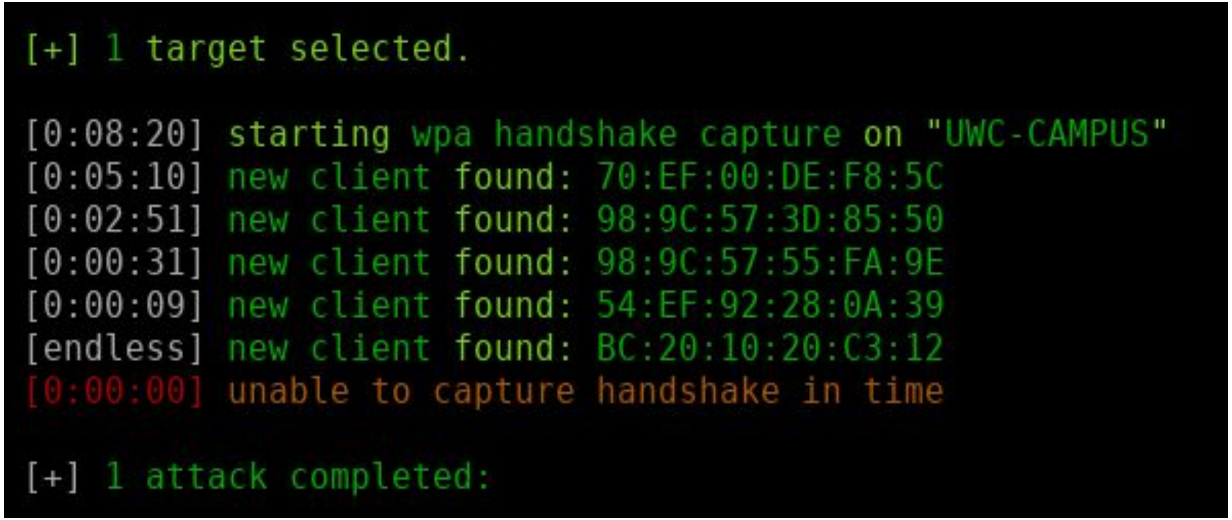
CSV file 1 contains MAC addresses of devices found. This data is transformed into vendor names using a third party API and the vendor names are dumped into a new CSV file

Low Level Design



CSV file 2 which contains the vendor names of devices found during Snoop operation is sent to Command and control center

Prototype

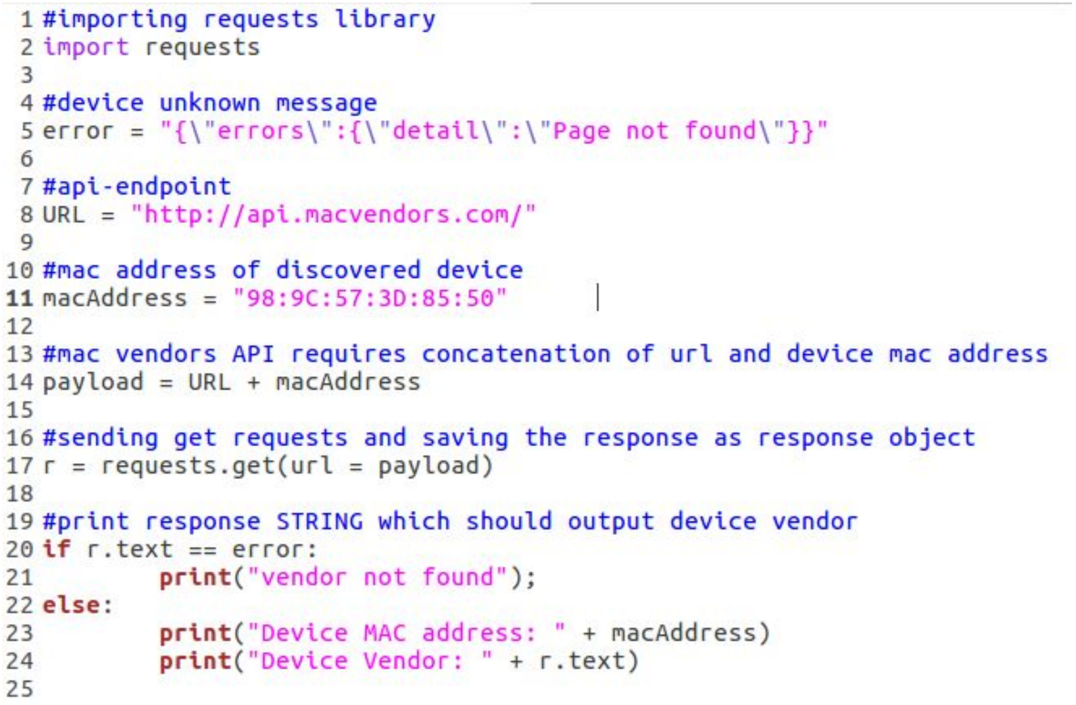


```
[+] 1 target selected.

[0:08:20] starting wpa handshake capture on "UWC-CAMPUS"
[0:05:10] new client found: 70:EF:00:DE:F8:5C
[0:02:51] new client found: 98:9C:57:3D:85:50
[0:00:31] new client found: 98:9C:57:55:FA:9E
[0:00:09] new client found: 54:EF:92:28:0A:39
[endless] new client found: BC:20:10:20:C3:12
[0:00:00] unable to capture handshake in time

[+] 1 attack completed:
```

5 MAC addresses of devices connected to UWC-Campus access point are discovered using Wifite.

Snoop lasted approximately 8mins 20secs

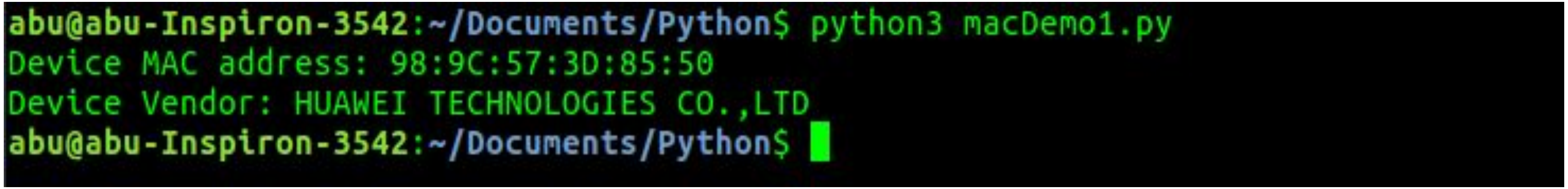
Prototype



```
#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)

```

Using a python HTTP request script, the MAC addresses are turned into vendor names which indicate the device makers.

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$
```

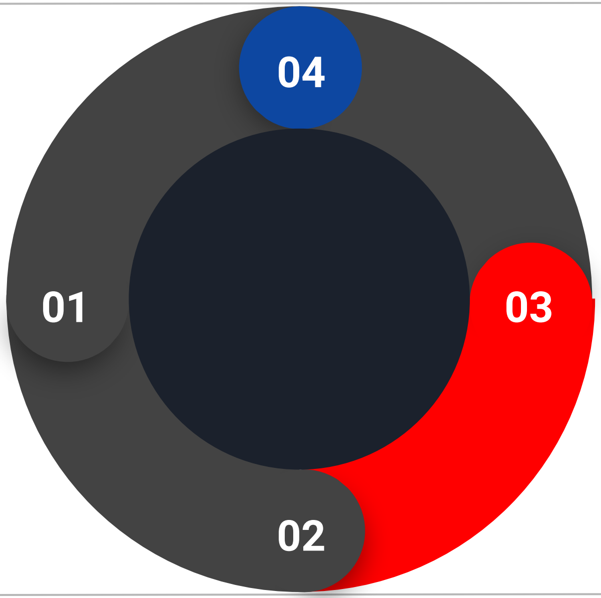
Using a python HTTP request script, the MAC addresses are turned into vendor names.

Project Plan

Term 1: Requirements Gathering and Requirements Analysis

Term 2: Prototyping

- More research of Kali Linux tools
- Some testing



Term 4: Final Presentation

Term 3: Implementation

- Storing data encountered
- Compile data to information
- Set-up C&C

References

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

[2] Kali Tools, “Wifite, Wifite Package Description,” Feb. 2014, https://tools.kali.org/wireless-attacks/wifite, Last accessed on 2018-07-13.

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

[4] Penetration Testing Tools, “Airodump-ng,” Mar 2017. https://en.kali.tools/?p=367, Last accessed on 2018-07-13.

Thank you for listening

Questions?