WI-FI HACKING WITH A RASPBERRY PI

NAME	***: ZUKISA***
SURNAME	***: DYANTYI***
STUDENT NO.	***: 3567302***
SUPERVISOR	***: DR. M NORMAN***
CO-SUPERVISOR	***: MR. M MUYOWA (CSIR)***

BACKGROUND

- ***Project is about cyber security and creating awareness of threats.***
- ***Build hacking prototype.***
- ***Retrieve hardware and software information and penetrate Wi-Fi network.***
- ***Objective is educate campus community.***
- ***Give suggestions to the Wi-Fi network owners found vulnerable.***

FUNCTIONAL REQUIREMENTS

- ***Detect available Wi-Fi networks and hidden networks.***
- ***Retrieve information about each network detected.***
- ***Convert Mac address to vendor names.***
- ***Where possible penetrate Wi-Fi network with weak encryption.***
- ***Document findings and educate the campus community the importance of strong passwords.***

TESTING STRATEGIES

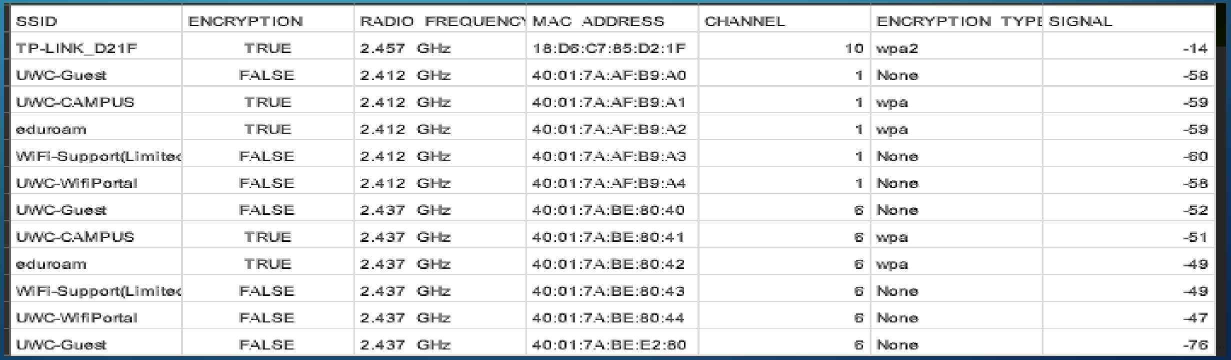
- ***Unit testing and system testing***
- ***Unit testing:***
  - ***Testing individual source codes.***
  - ***Five Python scripts***
- ***System testing:***
  - ***Hardware and Software integration***
  - ***Kali Linux, Raspberry Pi and Python.***

TESTING DESIGN

- ***Unit Testing:***
  - ***Run each script***
  - ***Then simultaneously, from scanning available networks to the hacking script.***
  - ***Each script function.***
- ***System Testing:***
  - ***All libraries installed in same directory***
  - ***Minimized time for penetration to avoid over heat on Raspberry Pi.***

TEST REPORT

- ***Tool built detects available networks and hidden ones.***
- ***Save all information on a CSV file.***
- ***Read Mac address column and convert to vendor names.***

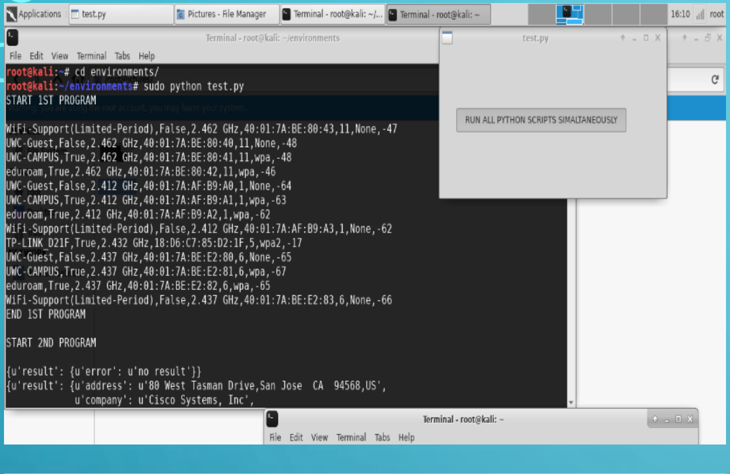


SSID	ENCRYPTION	RADIO FREQUENCY	MAC ADDRESS	CHANNEL	ENCRYPTION TYPE	SIGNAL
TP-LINK_D21F	TRUE	2.457 GHz	18:D6:C7:85:D2:1F	10	wpa2	-14
UWC-Guest	FALSE	2.412 GHz	40:01:7A:AF:B9:A0	1	None	-58
UWC-CAMPUS	TRUE	2.412 GHz	40:01:7A:AF:B9:A1	1	wpa	-59
eduroam	TRUE	2.412 GHz	40:01:7A:AF:B9:A2	1	wpa	-59
WiFi-Support(Limited	FALSE	2.412 GHz	40:01:7A:AF:B9:A3	1	None	-60
UWC-WifiPortal	FALSE	2.412 GHz	40:01:7A:AF:B9:A4	1	None	-58
UWC-Guest	FALSE	2.437 GHz	40:01:7A:BE:80:40	6	None	-52
UWC-CAMPUS	TRUE	2.437 GHz	40:01:7A:BE:80:41	6	wpa	-51
eduroam	TRUE	2.437 GHz	40:01:7A:BE:80:42	6	wpa	-49
WiFi-Support(Limited	FALSE	2.437 GHz	40:01:7A:BE:80:43	6	None	-49
UWC-WifiPortal	FALSE	2.437 GHz	40:01:7A:BE:80:44	6	None	-47
UWC-Guest	FALSE	2.437 GHz	40:01:7A:BE:E2:80	6	None	-76

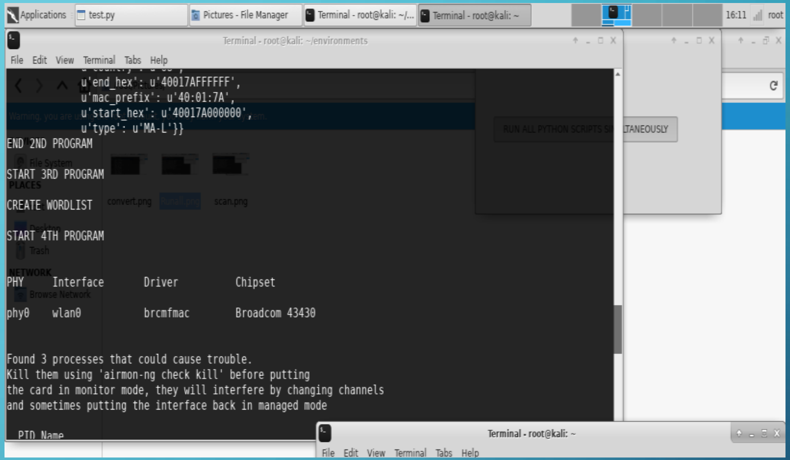
TEST REPORT

- ***Testing has been conducted on three networks.***
- ***With different passwords in length and difficulty level.***
- ***passwords:***
  - ***First password contain numbers only.***
  - ***second password contain numbers and alphabet characters.***
  - ***Third password has numbers, alphabets and special characters e.g. %_134Zdyou.***

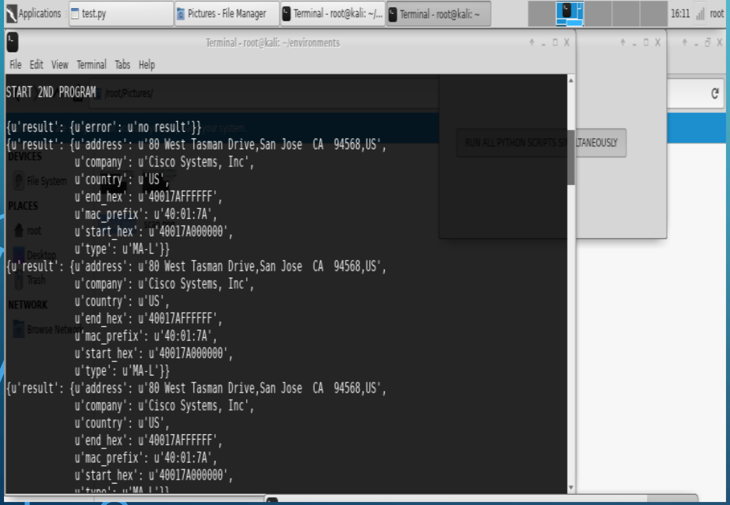
TEST REPORT


Applications
test.py
Pictures - File Manager
Terminal - root@kali: ~/...
Terminal - root@kali: ~
16:10
root
Terminal - root@kali: ~/environments
File Edit View Terminal Tabs Help
test.py
RUN ALL PYTHON SCRIPTS SIMALTANEOUSLY
Terminal - root@kali: ~
File Edit View Terminal Tabs Help

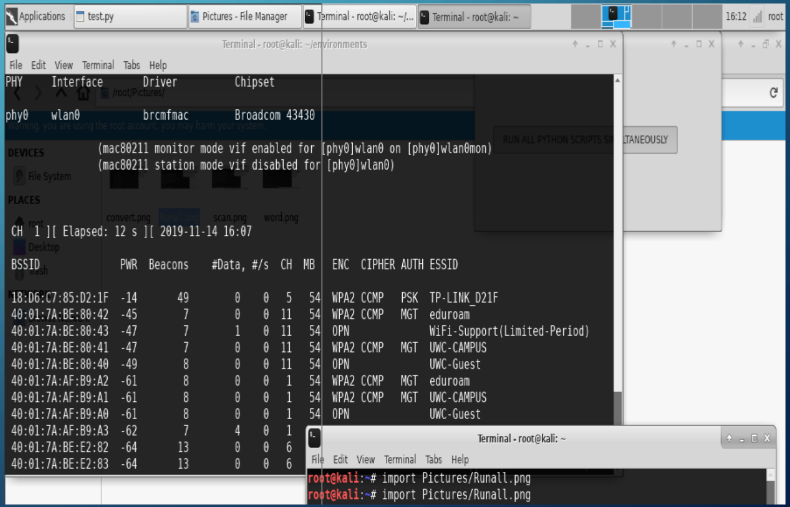
```
root@kali:~# cd environments/
root@kali:~/environments# sudo python test.py
START 1ST PROGRAM

WiFi-Support(Limited-Period),False,2.462 GHz,40:01:7A:BE:80:43,11,None,-47
UWC-Guest,False,2.462 GHz,40:01:7A:BE:80:40,11,None,-48
UWC-CAMPUS,True,2.462 GHz,40:01:7A:BE:80:41,11,wpa,-48
eduroam,True,2.462 GHz,40:01:7A:BE:80:42,11,wpa,-46
UWC-Guest,False,2.412 GHz,40:01:7A:AF:B9:A0,1,None,-64
UWC-CAMPUS,True,2.412 GHz,40:01:7A:AF:B9:A1,1,wpa,-63
eduroam,True,2.412 GHz,40:01:7A:AF:B9:A2,1,wpa,-62
WiFi-Support(Limited-Period),False,2.412 GHz,40:01:7A:AF:B9:A3,1,None,-62
TP-LINK_D21F,True,2.432 GHz,18:D6:C7:85:D2:1F,5,wpa2,-17
UWC-Guest,False,2.437 GHz,40:01:7A:BE:E2:80,6,None,-65
UWC-CAMPUS,True,2.437 GHz,40:01:7A:BE:E2:81,6,wpa,-67
eduroam,True,2.437 GHz,40:01:7A:BE:E2:82,6,wpa,-65
WiFi-Support(Limited-Period),False,2.437 GHz,40:01:7A:BE:E2:83,6,None,-66
END 1ST PROGRAM

START 2ND PROGRAM

{u'result': {u'error': u'no result'}}
{u'result': {u'address': u'80 West Tasman Drive,San Jose  CA  94568,US',
           u'company': u'Cisco Systems, Inc',
```


Applications
test.py
Pictures - File Manager
Terminal - root@kali: ~/...
Terminal - root@kali: ~
16:11
root
Terminal - root@kali: ~/environments
File Edit View Terminal Tabs Help
RUN ALL PYTHON SCRIPTS SI LTANEOUSLY
Terminal - root@kali: ~
File Edit View Terminal Tabs Help

```
           u'end_hex': u'40017AFFFFFF',
           u'mac_prefix': u'40:01:7A',
           u'start_hex': u'40017A000000',
           u'type': u'MA-L'}}
END 2ND PROGRAM

START 3RD PROGRAM

CREATE WORDLIST

START 4TH PROGRAM

PHY     Interface       Driver          Chipset

phy0    wlan0           brcmfmac        Broadcom 43430


Found 3 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

  PID Name
```


Applications
test.py
Pictures - File Manager
Terminal - root@kali: ~/...
Terminal - root@kali: ~
16:11
root
Terminal - root@kali: ~/environments
File Edit View Terminal Tabs Help
RUN ALL PYTHON SCRIPTS SI LTANEOUSLY

```
START 2ND PROGRAM

{u'result': {u'error': u'no result'}}
{u'result': {u'address': u'80 West Tasman Drive,San Jose  CA  94568,US',
           u'company': u'Cisco Systems, Inc',
           u'country': u'US',
           u'end_hex': u'40017AFFFFFF',
           u'mac_prefix': u'40:01:7A',
           u'start_hex': u'40017A000000',
           u'type': u'MA-L'}}
{u'result': {u'address': u'80 West Tasman Drive,San Jose  CA  94568,US',
           u'company': u'Cisco Systems, Inc',
           u'country': u'US',
           u'end_hex': u'40017AFFFFFF',
           u'mac_prefix': u'40:01:7A',
           u'start_hex': u'40017A000000',
           u'type': u'MA-L'}}
{u'result': {u'address': u'80 West Tasman Drive,San Jose  CA  94568,US',
           u'company': u'Cisco Systems, Inc',
           u'country': u'US',
           u'end_hex': u'40017AFFFFFF',
           u'mac_prefix': u'40:01:7A',
           u'start_hex': u'40017A000000',
```


Applications
test.py
Pictures - File Manager
Terminal - root@kali: ~/...
Terminal - root@kali: ~
16:12
root
Terminal - root@kali: ~/environments
File Edit View Terminal Tabs Help
RUN ALL PYTHON SCRIPTS SI LTANEOUSLY
Terminal - root@kali: ~
File Edit View Terminal Tabs Help

```
PHY     Interface       Driver          Chipset

phy0    wlan0           brcmfmac        Broadcom 43430

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)


 CH  1 ][ Elapsed: 12 s ][ 2019-11-14 16:07

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 18:D6:C7:85:D2:1F  -14       49        0    0   5  54  WPA2 CCMP   PSK  TP-LINK_D21F
 40:01:7A:BE:80:42  -45        7        0    0  11  54  WPA2 CCMP   MGT  eduroam
 40:01:7A:BE:80:43  -47        7        1    0  11  54  OPN              WiFi-Support(Limited-Period)
 40:01:7A:BE:80:41  -47        7        0    0  11  54  WPA2 CCMP   MGT  UWC-CAMPUS
 40:01:7A:BE:80:40  -49        8        0    0  11  54  OPN              UWC-Guest
 40:01:7A:AF:B9:A2  -61        8        0    0   1  54  WPA2 CCMP   MGT  eduroam
 40:01:7A:AF:B9:A1  -61        8        0    0   1  54  WPA2 CCMP   MGT  UWC-CAMPUS
 40:01:7A:AF:B9:A0  -61        8        0    0   1  54  OPN              UWC-Guest
 40:01:7A:AF:B9:A3  -62        7        4    0   1
 40:01:7A:BE:E2:82  -64       13        0    0   6
 40:01:7A:BE:E2:83  -64       13        0    0   6
```

```
root@kali:~# import Pictures/Runall.png
root@kali:~# import Pictures/Runall.png
```

REFERENCE

[1] CISCO, “Security,” CISCO/Security, 2018. [Online]. Available: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html. [Accessed: 14-Feb-2019].

[2] hash3liZer, “No Title,” 2018. [Online]. Available: https://www.shellvoide.com/python/how-to-code-a-simple-wireless-sniffer-in-python/. [Accessed: 05-Aug-2019].

[3] A. L. and J. Muniz, Penetration Testing with Raspberry Pi. Birmingham,UK: Packt Publishing Ltd., 2015.

[4] V. Kumkar, A. Tiwari, P. Tiwari, A. Gupta, and S. Shrawne, “Vulnerabilities of Wireless Security protocols (WEP and WPA2),” Int. J. Adv. Res. Comput. Eng. Technol., vol. 1, no. 2, pp. 2278–1323, 2012.

[5] J. F. and S. A. Tyler Williams, “security of the internet of things(iot),” Digitalcommons.murraystate.edu, 2017. [Online]. Available: https://www.google.com/search?rlz=1C1AVFC_enZA833ZA833&ei=myOCXMrnCeGU1fAPkqOooAI_&q=security+of+the+internet+of+things%28iot%29+murray+state+university&oq=%22security+of+the+internet+of+things%28IoT%29%

DEMO

- ***Run two Python scripts.***
  - ***First script run two scripts simultaneously.***
    - ***Detect available networks, then convert Mac addresses of detected networks to vendor names.***
  - ***Last script crack passwords.***
    - ***Weak password, has digits only.***
    - ***Strong password, has digits, alphabets and special characters.***

THANK YOU