OWASP SEASIDES

Building Your Hacker Black Box For Fun And Profit

VANSHIT MALHOTRA

HACKDOOR INDIA

BLACKBOX>>WHOAMI

- Former Cyber Security Consultant for Government of India UIDAI
- Cyber Security Consultant
    - Web | Mobile | Network Penetration Tester
    - WiFi Hacking Beyond Neighbours Free WiFi
    - Malware Analyst , Spam Fighter
    - Pentesting , Red Teaming Gadgets Enthusiast
- Presenter/ Speaker @ "HACKON-2016", "HACKTECH 2017", "National Cyber Safety and Security Standards (NCDRC) 2017", "c0c0n X 2017", "HAKON 2017"

DISCLAIMER

The Author of this Paper holds no responsibility of what so ever you do with the information provided or damages you cause to your own device or others. This white paper/presentation is purely for research and educational purposes.

MOTIVATION FOR CREATING THE PENTESTING ARSENAL

- The pentest community is always exited about custom boxes for pentesting ;
  - Pineapple WiFi Box
  - PwnPlug
  - Raspberry Pie etc.

- Using a hacker friendly hardware to perform pentesting exercises adds a Turing factor to the daily job.

THEN WHY BUILD YOUR OWN BLACKBOX

RASPBERRY PI

- EASILY IDENTIFIED !
- EXPENSIVE [3K INR]
- COSTS EVEN MORE WITH WIFI SUPPORT
- CLASS 10 SD CARD
- NO BOXING BY DEFAULT
- USB PORTS AND HDMI ARE USELESS DURING PENTESTS

PACKET SQUIRREL

- LIMITED TO NETWORK MITM
- 4K AND LONG SHIPMENT

PINEAPPLE WIFI

- EASILY IDENTIFIED !
- EXPENSIVE [7K - 14K INR]
- LIMITED CAPABILITY

AND WHAT IF YOU THINK OF A NEW ATTACK VECTOR OR A GREAT IDEA IN MONTHS TO COME ?

THE ROADBLOCKS

- CAN I REALLY DO IT
  - How to interface tools with hardware ?
  - Loading the custom firmware ?
  - Installing the tool support and services ? and many more ....

THE GOOD NEWS

- In this presentation I will be showing you that Building your own Hacker Pentesting Black Box is not difficult at all.
- It will be as simple as installing Linux on your device and configuring an internet router.
- My presentation will be highly technical and full of practical demonstrations so look closely.

WHAT IS PENTESTING BLACK BOX ? WHAT WILL I BUILD ?

- I will be building every Hackers Dream Gadget that allows me to carry on a lot of automated pentesting activities including but not limited to
    - Wifi Hacking
    - WiFi attacks
    - Karma Attack
    - Running NMAP based scans on network
    - Man in the Middle Attack
    - Exploitation of through Metasploit (or other exploits)
    - and all other capabilities of a usual laptop with a good pentesting distribution installed .

DESIGN GOALS

- Build Cheap : I built this device @ 1500 INR.
- Open Source: As much as I can.
- Custom OS with the following features :
  - Works easy with hardware with easy driver support
  - Easy Package management
  - Extensible in terms of Both Hardware and Software.
  - Easily Scriptable via Python , Ruby.

CHOICE OF HARDWARE

- Hardware Requirements :
    - Wifi Device with Monitor Mode and packet injection enabled .
    - USB support to interface more devices eg : wifi cards, pen-drives for storage etc.
    - Built-in battery or USB powered

TL - MR3020

- Has a USB interface to connect dongles .
- Has a Ethernet connection
- Is USB powered
- Switch to toggle between different modes.

In addition to TP-Link MR3020, we also need a USB key. (This is everything you need to build your Hacker Black Box :)

TL - MR3020

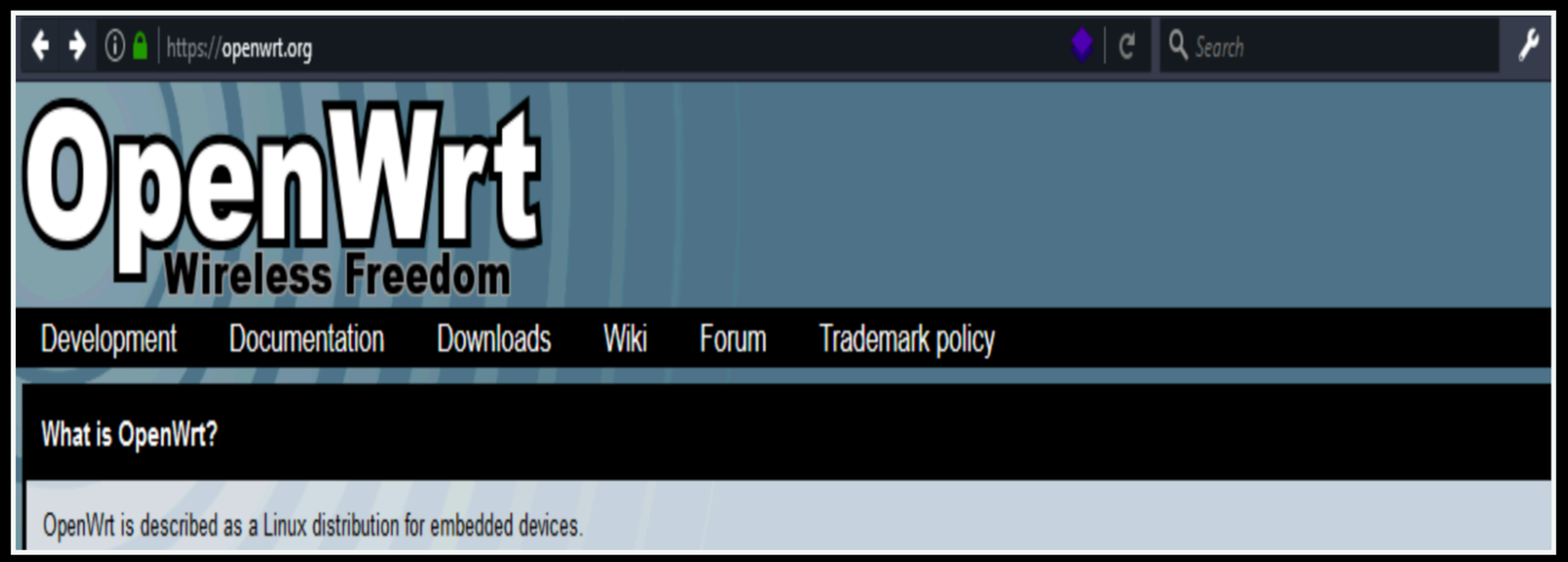

TP-LINK


TP-LINK
3G/4G
WISP
AP
WAN/LAN
POWER
3G/4G USB


TP-LINK
150Mbps TL-MR3020
WPS/RESET

CHOICE OF OPERATING SYSTEM

- OpenWrt : https://openwrt.org/.
- Fully Writable File System
- PackageManagement
- Fully Scriptable Interface



A PRACTICAL GUIDE TO FLASHING OPENWRT ON TL-MR3020

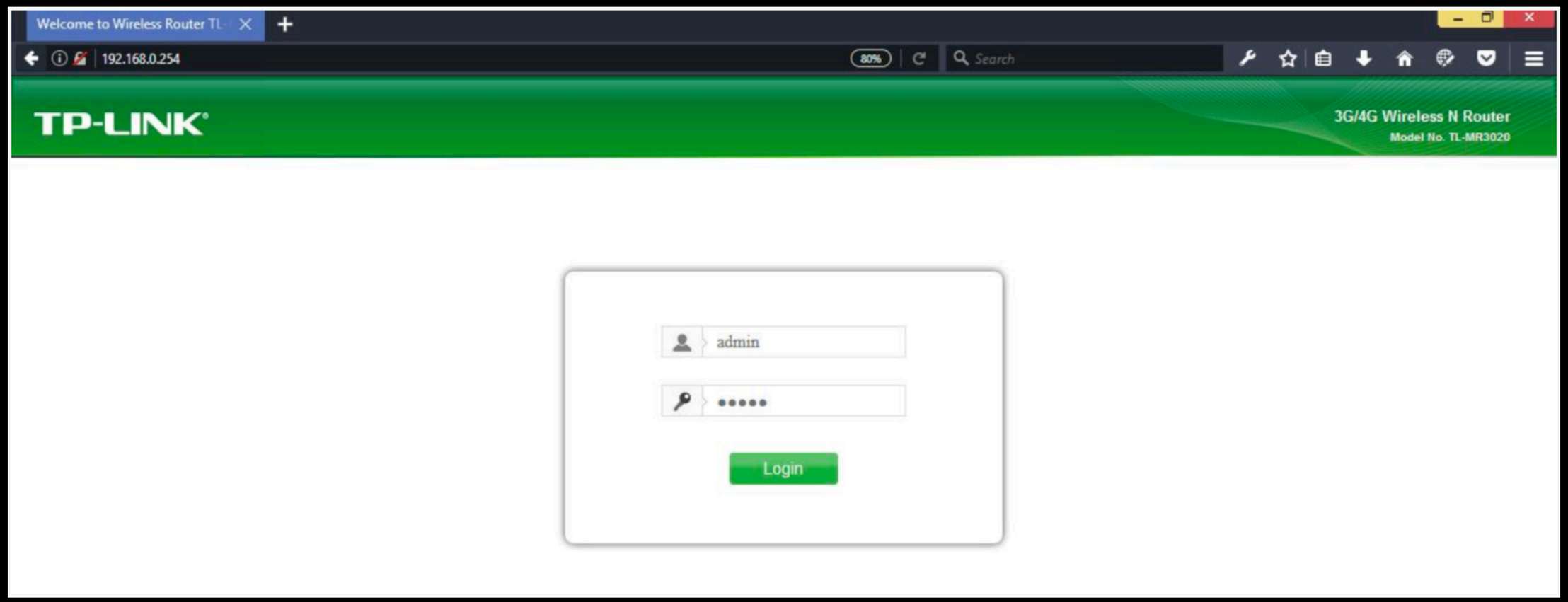
- Lab Set Up : Connect the Router to the Laptop through the Ethernet cable and power up the router via USB power. Let the router boot up.

- Unbox and Boot-up the router; TL-MR3020, and go to the admin login page;

    - The default url is : http://192.168.0.254 ; the default credentials : admin / admin (so secure :p)

A PRACTICAL GUIDE TO FLASHING OPENWRT ON TL-MR3020

A PRACTICAL GUIDE TO FLASHING OPENWRT ON TL-MR3020

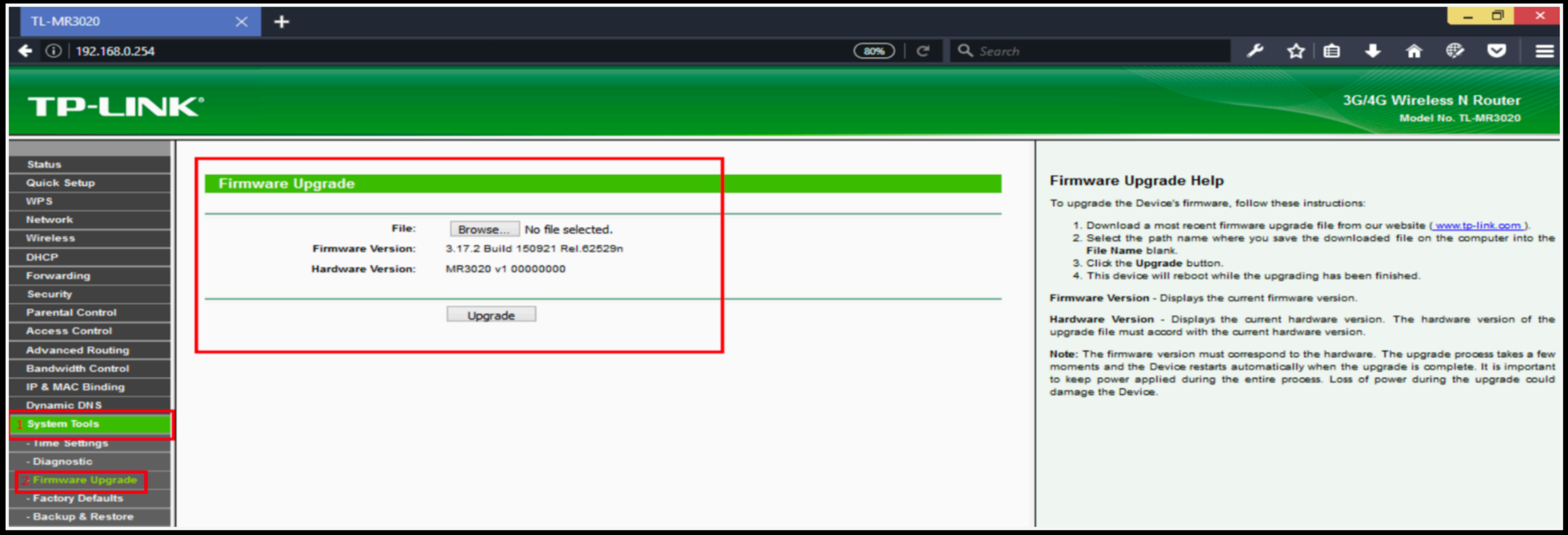


A PRACTICAL GUIDE TO FLASHING OPENWRT ON TL-MR3020

Before Flashing, make sure that the switch on the router is set to 3G/4G which is the default configuration.

A PRACTICAL GUIDE TO FLASHING OPENWRT ON TL-MR3020

Check firmware version , and hardware version and other details; System Tools -> Firmware upgrade



POWER OF WEB INTERFACE

- Logs
- Kernel Logs
- Wireless interface setup
- Installing and removing packages etc

SSH INTERFACE

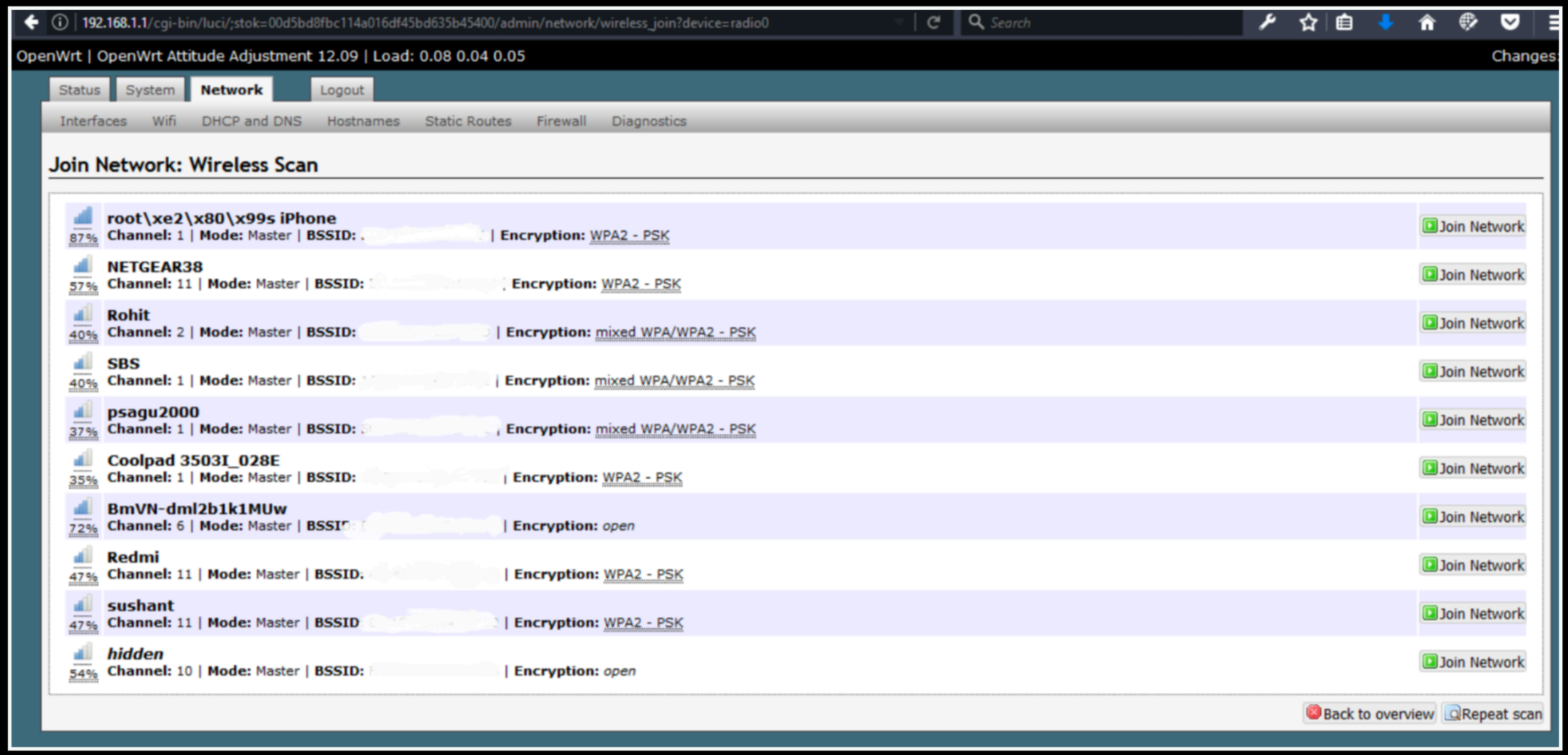
```
login as: root
root@192.168.1.1's password:


BusyBox v1.19.4 (2013-03-14 11:28:31 UTC) built-in shell (ash)
Enter 'help' for a list of built-in commands.

  _______                     ________        __
 |       |.-----.-----.-----.|  |  |  |.----.|  |_
 |   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
 |_______||   __|_____|__|__||________||__|  |____|
          |__| W I R E L E S S   F R E E D O M
 -----------------------------------------------------
 ATTITUDE ADJUSTMENT (12.09, r36088)
 -----------------------------------------------------
  * 1/4 oz Vodka       Pour all ingredients into mixing
  * 1/4 oz Gin         tin with ice, strain into glass.
  * 1/4 oz Amaretto
  * 1/4 oz Triple sec
  * 1/4 oz Peach schnapps
  * 1/4 oz Sour mix
  * 1 splash Cranberry juice
 -----------------------------------------------------
root@OpenWrt:~#
root@OpenWrt:~#
```

CONNECTING TO INTERNET/NETWORK

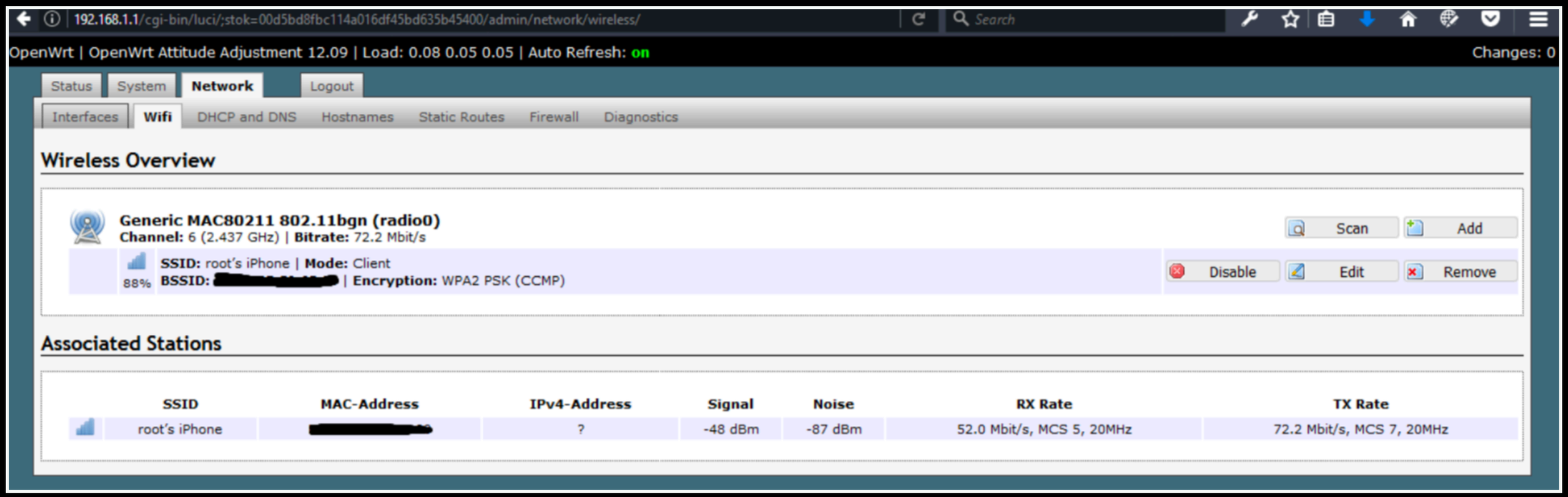
- Need to have internet/network connectivity on this device :
  - Initially to install packages
  - Latter to run Pentest on the network

CONNECTING TO INTERNET/NETWORK

- Network -> Wifi -> Scan ;
- his will return a list of available wireless networks in the vicinity. Connect to the network and submit.



CONNECTED TO WIRELESS HOTSPOT FROM MY I PHONE



Other Way Of Connecting to Internet

The other way of providing the network connectivity is through the Ethernet interface which is as simple as connecting the 2 ends of Ethernet cable.

INSTALLING USB SUPPORT FOR PENDRIVE

Why USB Support :

- Limited Storage on Embedded Systems
- Our BlackBox only has 680.00 KB available. This is too less for a Hacker's Black Box.
- Need a-lot of memory space for installing Pentesting tools/ packages and scripts
- Additional Space for Storing Scan Results , Data collected while Pentest.

Solution : Utilise the USB interface

INSTALLING USB SUPPORT FOR PENDRIVE - **PACKAGE NAMES**

Install Basic Packages for USB Support

- opkg update
- opkg install kmod-usb-support
- opkg install kmod-fs-ext4
- opkg install kmod-fs-vfat
- opkg install block-mount

PENTESTING ? PACKAGES MISSING

basic packages missing !

```
root@OpenWrt:~# iwconfig
-ash: iwconfig: not found
root@OpenWrt:~# airmon-ng
-ash: airmon-ng: not found
```

opkg install package_name

START BUILDING BLACKBOX

installing iwconfig support

```
 _______                     ________        __
|       |.-----.-----.-----.|  |  |  |.----.|  |_
|   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
|_______||   __|_____|__|__||________||__|  |____|
         |__| W I R E L E S S   F R E E D O M
-----------------------------------------------------
ATTITUDE ADJUSTMENT (12.09, r36088)
-----------------------------------------------------
 * 1/4 oz Vodka      Pour all ingredients into mixing
 * 1/4 oz Gin        tin with ice, strain into glass.
 * 1/4 oz Amaretto
 * 1/4 oz Triple sec
 * 1/4 oz Peach schnapps
 * 1/4 oz Sour mix
 * 1 splash Cranberry juice
-----------------------------------------------------
root@OpenWrt:~# opkg update
Downloading http://downloads.openwrt.org/attitude_adjustment/12.09/ar71xx/generic/packages/Packages.gz.
Updated list of available packages in /var/opkg-lists/attitude_adjustment.
root@OpenWrt:~# opkg install wireless-tools
Installing wireless-tools (29-5) to root...
Downloading http://downloads.openwrt.org/attitude_adjustment/12.09/ar71xx/generic/packages/wireless-tools_29-5_ar71xx.ipk.
Configuring wireless-tools.
root@OpenWrt:~# iwconfig
lo        no wireless extensions.

wlan0     IEEE 802.11bgn  ESSID:"root's iPhone"
          Mode:Managed  Frequency:2.462 GHz  Access Point: BE:F4:8E:59:0F:80
          Bit Rate=72.2 Mb/s   Tx-Power=15 dBm
          RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=70/70  Signal level=-25 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:4   Missed beacon:0

eth0      no wireless extensions.

br-lan    no wireless extensions.

root@OpenWrt:~#
```

INSTALLING AIRCRACK-NG SUITE

```
root@OpenWrt:~# opkg install aircrack-ng
Installing aircrack-ng (1.1-3) to root...
Downloading http://downloads.openwrt.org/attitude_adjustment/12.09/ar71xx/generic/packages/aircrack-ng_1.1-3_ar71xx.ipk.
Installing libpthread (0.9.33.2-1) to root...
Downloading http://downloads.openwrt.org/attitude_adjustment/12.09/ar71xx/generic/packages/libpthread_0.9.33.2-1_ar71xx.ipk
Installing libopenssl (1.0.1h-1) to root...
Downloading http://downloads.openwrt.org/attitude_adjustment/12.09/ar71xx/generic/packages/libopenssl_1.0.1h-1_ar71xx.ipk.
Installing zlib (1.2.7-1) to root...
Downloading http://downloads.openwrt.org/attitude_adjustment/12.09/ar71xx/generic/packages/zlib_1.2.7-1_ar71xx.ipk.
Installing libpcap (1.1.1-2) to root...
Downloading http://downloads.openwrt.org/attitude_adjustment/12.09/ar71xx/generic/packages/libpcap_1.1.1-2_ar71xx.ipk.
Configuring libpthread.
Configuring zlib.
Configuring libopenssl.
Configuring libpcap.
Configuring aircrack-ng.
root@OpenWrt:~#
```

INSTALLING PYTHON FOR SCRIPTING

```
root@OpenWrt:~# opkg install python
Installing python (2.7.3-1) to root...
Downloading http://downloads.openwrt.org/attitude_adjustment/12.09/ar71xx/generic/packages/python_2.7.3-1_ar71xx.ipk.
Installing libffi (3.0.10-1) to root...
Downloading http://downloads.openwrt.org/attitude_adjustment/12.09/ar71xx/generic/packages/libffi_3.0.10-1_ar71xx.ipk.
Installing python-mini (2.7.3-1) to root...
Downloading http://downloads.openwrt.org/attitude_adjustment/12.09/ar71xx/generic/packages/python-mini_2.7.3-1_ar71xx.ipk.
Configuring libffi.
Configuring python-mini.
Configuring python.
root@OpenWrt:~# opkg install python-crypto
Installing python-crypto (2.0.1-1) to root...
Downloading http://downloads.openwrt.org/attitude_adjustment/12.09/ar71xx/generic/packages/python-crypto_2.0.1-1_ar71xx.ipk.
Installing libgmp (4.3.1-2) to root...
Downloading http://downloads.openwrt.org/attitude_adjustment/12.09/ar71xx/generic/packages/libgmp_4.3.1-2_ar71xx.ipk.
Configuring libgmp.
Configuring python-crypto.
root@OpenWrt:~# python
Python 2.7.3 (default, Mar 14 2013, 12:12:59)
[GCC 4.6.3 20120201 (prerelease)] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
>>>
>>> print "Python Installed on OpenWrt
```

INSTALLING SECURITY TOOLS TCPDUMP, ETTERCAP, NETCAT …. ….

```
root@OpenWrt:~#
root@OpenWrt:~# opkg install tcpdump
Installing tcpdump (4.2.1-3) to root...
Downloading http://downloads.openwrt.org/attitude_adjustment/12.09/ar71xx/generic/packages/tcpdump_4.2.1-3_ar
Configuring tcpdump.
root@OpenWrt:~#
root@OpenWrt:~#
root@OpenWrt:~#
root@OpenWrt:~# opkg install ettercap
Installing ettercap (NG-0.7.3-2) to root...
Downloading http://downloads.openwrt.org/attitude_adjustment/12.09/ar71xx/generic/packages/ettercap_NG-0.7.3-
Configuring ettercap.
root@OpenWrt:~#
```

```
root@OpenWrt:/# opkg install netcat
Installing netcat (0.7.1-2) to root...
Downloading http://downloads.openwrt.org/attitude_adjustment/12.09/ar71xx/generi
c/packages/netcat_0.7.1-2_ar71xx.ipk.
Configuring netcat.
root@OpenWrt:/#
```

CHECKING FOR PACKET INJECTION

```
root@OpenWrt:~# aireplay-ng --test mon0
08:56:58  Trying broadcast probe requests...
08:56:58  Injection is working!
08:57:00  Found 1 AP

08:57:00  Trying directed probe requests...
08:57:00  50:2B:73:1D:B7:78 - channel: 1 - 'psagu2000'
08:57:02  Ping (min/avg/max): 1.607ms/9.842ms/83.314ms Power: -76.67
08:57:02  18/30:  60%

root@OpenWrt:~#
```

PENTESTING WITH HACKER'S BLACK BOX - W!-SPY

Goal: Building the Ultimate Wifi Spy (Wi-SPY) Gadget

- The capabilities of the Hacker's Black Box($25) is same as a WiFi Pineapple device($100).I can use my Hacker Black Box as an ultimate WiFi Spy (Wi-SPY) device.

- Wi-SPY is an automated device that broadcasts the Wireless networks probed by the Laptops, Tabs, Phones etc in the vicinity and allows these devices to connect to itself. Once we get the IP level connectivity with our victim, we are able to perform range of attacks which include but not limited to DNS poisoning, Cafe Latte Attack, MITM, Browser Applet attacks etc.

INJECTION MODE FOR WIRELESS INTERFACE

- The first step is to bring my wireless interface into monitor mode.

- Running Airmon-ng on TL-MR3020 to turn the Wifi card into monitor mode

>> airmon-ng start wlan0

```
usage: airmon-ng <start|stop|check> <interface> [channel or frequency]

root@OpenWrt:~# airmon-ng start wlan0
ps: invalid option -- A
BusyBox v1.19.4 (2013-03-14 11:28:31 UTC) multi-call binary.

Usage: ps

Show list of processes

        w       Wide output


Interface       Chipset         Driver

wlan0           Atheros         ath9k - [phy0]
                                (monitor mode enabled on mon0)

root@OpenWrt:~# airodump-ng mon0
```

SCANNING THE AIR

- Running airodum-ng to scan for the wireless networks in the vicinity

airodump-ng mon0

```
CH  1 ][ Elapsed: 24 s ][ 2017-08-06 08:55

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

E8:94:F6:4A:43:F4   -1        0        1    0 108  -1   WPA                <length:  0>
BE:F4:8E:59:0F:80  -33      258       31    0   1  54e  WPA2 CCMP   PSK  root▒..s iPhone
50:2B:73:1D:B7:78  -78      212      136    3   1  54e  WPA2 CCMP   PSK  psagu2000

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

E8:94:F6:4A:43:F4  38:A4:ED:C1:5D:0B  -127    0 - 0e     0        1
(not associated)   E8:4E:06:1D:EE:7D  -33     0 - 1      0        2
E8:94:F6:4A:43:F4  C4:0B:CB:6F:28:51  -74     0 - 6      0       11
```

SETTING UP FAKE ACCESS POINT

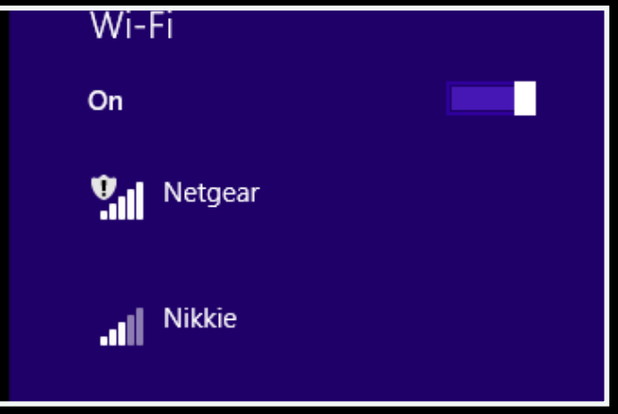
```
root@OpenWrt:~# airbase-ng --essid Netgear -c 6 mon0
15:47:21  Created tap interface at0
15:47:21  Trying to set MTU on at0 to 1500
15:47:21  Trying to set MTU on mon0 to 1800
15:47:21  Access Point with BSSID 98:DE:D0:90:D6:9E started.
15:47:30  Client B8:76:3F:F3:58:69 associated (unencrypted) to ESSID: "Netgear"
15:47:40  Client B8:76:3F:F3:58:69 associated (unencrypted) to ESSID: "Netgear"
```

airbase-ng --essid <network-name> -c 6 mon0

THE EVIL TWIN

- Connected to the Fake AP being broadcasted by the Hacker's Black Box

```
root@OpenWrt:~# airbase-ng --essid Netgear -c 6 mon0
15:47:21  Created tap interface at0
15:47:21  Trying to set MTU on at0 to 1500
15:47:21  Trying to set MTU on mon0 to 1800
15:47:21  Access Point with BSSID 98:DE:D0:90:D6:9E started.
15:47:30  Client B8:76:3F:F3:58:69 associated (unencrypted) to ESSID: "Netgear"
15:47:40  Client B8:76:3F:F3:58:69 associated (unencrypted) to ESSID: "Netgear"
15:47:53  Client B8:76:3F:F3:58:69 associated (unencrypted) to ESSID: "Netgear"
15:48:05  Client B8:76:3F:F3:58:69 associated (unencrypted) to ESSID: "Netgear"
15:48:16  Client B8:76:3F:F3:58:69 associated (unencrypted) to ESSID: "Netgear"
15:49:14  Client B8:76:3F:F3:58:69 associated (unencrypted) to ESSID: "Netgear"
15:49:26  Client B8:76:3F:F3:58:69 associated (unencrypted) to ESSID: "Netgear"
```



THANKS !

@vanshitmalhotra

/vanshitmalhotra