



Deception Firmware

www.HackerArsenal.com

PENTESTER
ACADEMY



Getting Started: Deception

The Deception firmware allows you to use your device as a portable Wi-Fi Honeypot. The firmware has different captive portal splash pages which you can select and demo for security awareness.

Deception Firmware: Connecting

We will be communicating with the device using its serial port which is available over the USB interface. We will use the Serial Monitor in the Arduino IDE as it allows us to send and receive using a simple interface. ***We are assuming the device has already been flashed using the Deception firmware downloaded from our website.***

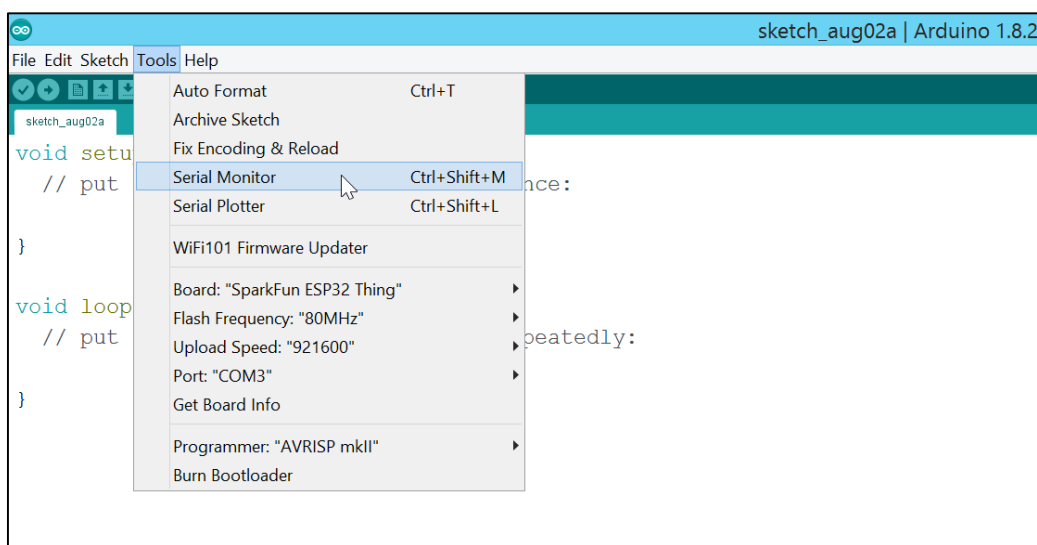
Step 1: Download and install Arduino IDE by following the instructions given below:

Windows: <https://www.arduino.cc/en/Guide/Windows>

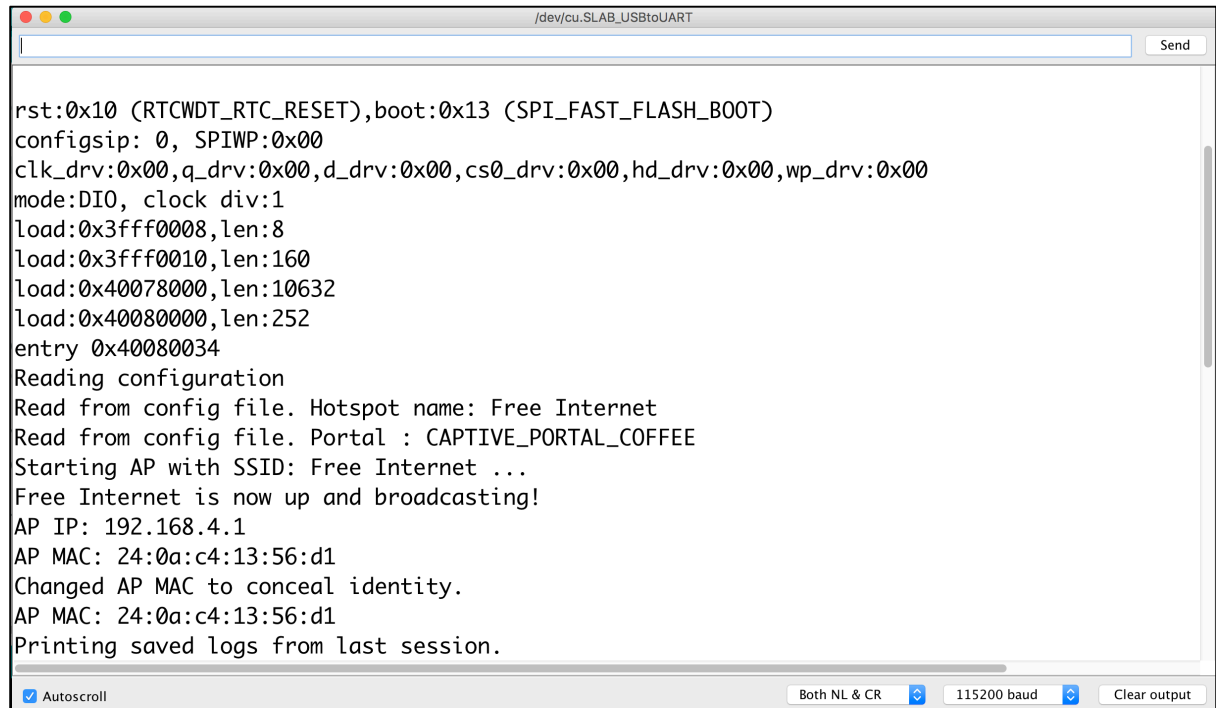
Linux: <https://www.arduino.cc/en/Guide/Linux>

Mac OSX: <https://www.arduino.cc/en/Guide/MacOSX>

Step 2: Connect the device to your laptop, start the Arduino IDE, make sure that the **Port** is selected correctly as per your environment and then open the **Serial Monitor**.



Step 3: In the Serial Monitor, please ensure that the baud rate is set to 115200.



The screenshot shows a Serial Monitor window titled "/dev/cu.SLAB_USBtoUART". The main text area displays the following log output:

```
rst:0x10 (RTCWDT_RTC_RESET),boot:0x13 (SPI_FAST_FLASH_BOOT)
configsip: 0, SPIWP:0x00
clk_drv:0x00,q_drv:0x00,d_drv:0x00,cs0_drv:0x00,hd_drv:0x00,wp_drv:0x00
mode:DIO, clock div:1
load:0x3fff0008,len:8
load:0x3fff0010,len:160
load:0x40078000,len:10632
load:0x40080000,len:252
entry 0x40080034
Reading configuration
Read from config file. Hotspot name: Free Internet
Read from config file. Portal : CAPTIVE_PORTAL_COFFEE
Starting AP with SSID: Free Internet ...
Free Internet is now up and broadcasting!
AP IP: 192.168.4.1
AP MAC: 24:0a:c4:13:56:d1
Changed AP MAC to conceal identity.
AP MAC: 24:0a:c4:13:56:d1
Printing saved logs from last session.
```

At the bottom of the window, there is a status bar with the following controls:

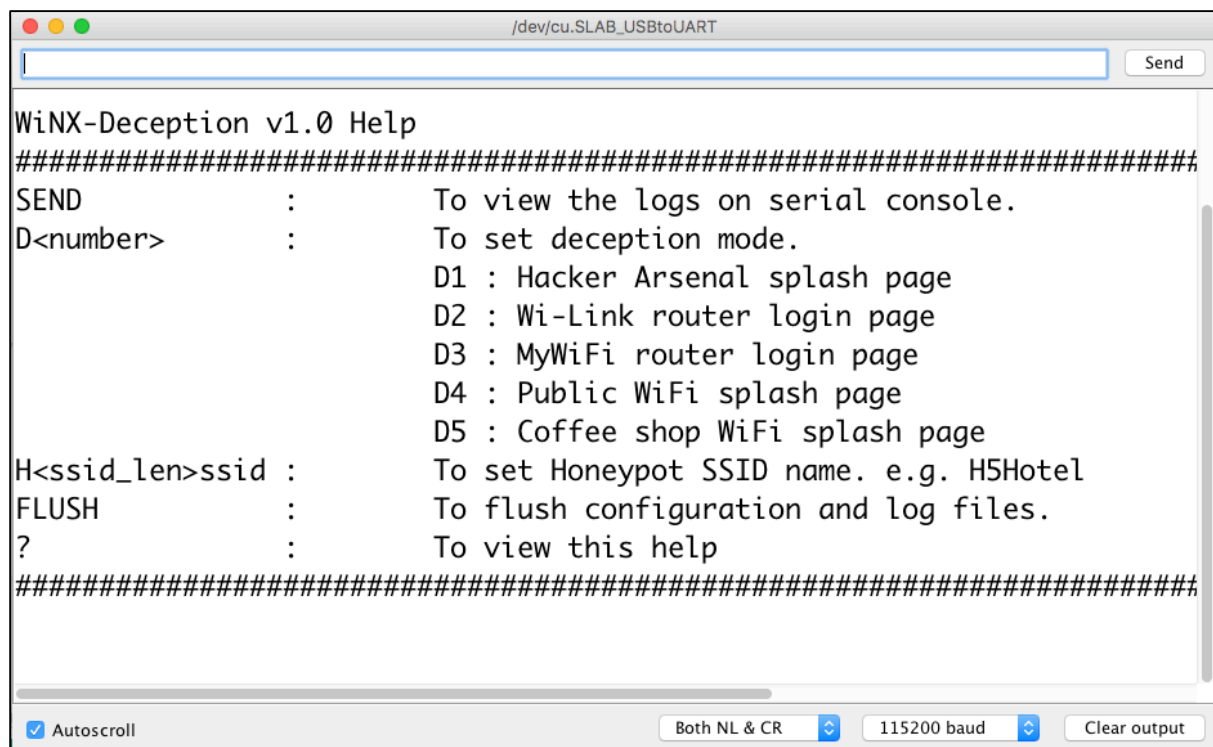
- ☒ Autoscroll
- Both NL & CR (dropdown menu)
- 115200 baud (dropdown menu)
- Clear output (button)

You should be able to view the logs from WiNX Deception firmware. If you are unable to see anything then reset the device using the **EN** button at the bottom. This will restart the device and you should be able to see a logs similar to the above.

Deception Firmware: Configuration

Default Settings:

Once the device boots, it will show you a help screen with the list of supported commands. You can access this anytime by using ? command.



```
WiNX-Deception v1.0 Help
#####
SEND          :      To view the logs on serial console.
D<number>     :      To set deception mode.
                  D1 : Hacker Arsenal splash page
                  D2 : Wi-Link router login page
                  D3 : MyWiFi router login page
                  D4 : Public WiFi splash page
                  D5 : Coffee shop WiFi splash page
H<ssid_len>ssid :      To set Honeypot SSID name. e.g. H5Hotel
FLUSH         :      To flush configuration and log files.
?             :      To view this help
#####
```

The default SSID is **Internet** and the default splash page is **Hacker Arsenal**.

Changing the SSID:

To change the SSID of the honeypot, you can use the **H<ssid_len>ssid** command. This means, H followed by length of the SSID and then the SSID. For example the command **H13Free_Internet** will change the honeypot SSID to Free_Internet (13 character long). ***The maximum allowed SSID length is 30 characters.***

```
COM
|
Received command: H13Free_Internet

New Hotspot name: Free_Internet

ets Jun  8 2016 00:22:57

rst:0x10 (RTCWDT_RTC_RESET),boot:0x13 (SPI_FAST_FLASH_BOOT)
configsip: 0, SPIWP:0x00
clk_drv:0x00,q_drv:0x00,d_drv:0x00,cs0_drv:0x00,hd_drv:0x00,wp_drv:0x
mode:DIO, clock div:1
load:0x3fff0008,len:8
load:0x3fff0010,len:160
load:0x40078000,len:10632
load:0x40080000,len:252
entry 0x40080034
Reading configuration
Read from config file. Hotspot name: Free_Internet
Read from config file. Portal : CAPTIVE_PORTAL_PUBLIC
Starting AP with SSID: Free_Internet ...
Free_Internet is now up and broadcasting!
```

Changing the Splash Page:

The firmware comes with five splash/login pages. In order to use a page other than the default one, you will need to use the **D<number>** command. The **<number>** here is the number of the page as shown in the help. For example, D4 is for choosing the Public Wi-Fi splash page.

```
COM3
|
Received command: D4

ets Jun  8 2016 00:22:57

rst:0x10 (RTCWDT_RTC_RESET),boot:0x13 (SPI_FAST_FLASH_BOOT)
configsip: 0, SPIWP:0x00
clk_drv:0x00,q_drv:0x00,d_drv:0x00,cs0_drv:0x00,hd_drv:0x00,wp_drv:0x00
mode:DIO, clock div:1
load:0x3fff0008,len:8
load:0x3fff0010,len:160
load:0x40078000,len:10632
load:0x40080000,len:252
entry 0x40080034
Reading configuration
Hotspot config file not present. Using hotspot name: Internet
Read from config file. Portal : CAPTIVE_PORTAL_PUBLIC
Starting AP with SSID: Internet ...
Internet is now up and broadcasting!
```

Viewing Captured Login Data:

The settings are persistent and retained across reboots. This allows the device to run on a battery for days while collecting data.

To view the collected data logs, connect to the device and issue the **SEND** command. This command will print logs to the serial console and delete the logs from the device.

```
Received command: SEND
Dumping Command received. Dumping file.
Reading file: /log.txt
=====X=====
6186019: Deception SSID Internet is up!
6815037: Started HTTP Server
5926734: Deception SSID Internet is up!
5929559: Deception SSID Internet is up!
=====X=====
```

Reset Device Configuration:

To reset the configuration, we can use **FLUSH** command. This command will delete all configuration files and device will boot with default configuration.

```
COM3

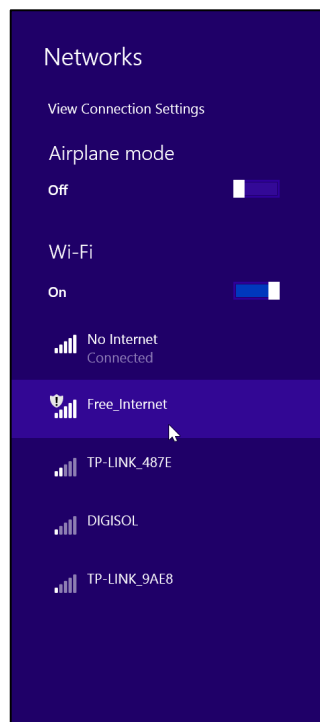
Received command: FLUSH
Deleting all configuration files.
ets Jun  8 2016 00:22:57

rst:0x10 (RTCWDT_RTC_RESET),boot:0x13 (SPI_FAST_FLASH_BOOT)
configsip: 0, SPIWP:0x00
clk_drv:0x00,q_drv:0x00,d_drv:0x00,cs0_drv:0x00,hd_drv:0x00,wp_drv:0x00
mode:DIO, clock div:1
load:0x3fff0008,len:8
load:0x3fff0010,len:160
load:0x40078000,len:10632
load:0x40080000,len:252
entry 0x40080034
Reading configuration
Hotspot config file not present. Using hotspot name: Internet
Portal config file not present. Using portal: CAPTIVE_PORTAL_HACKER_ARSENAL
Starting AP with SSID: Internet ...
Internet is now up and broadcasting!
```

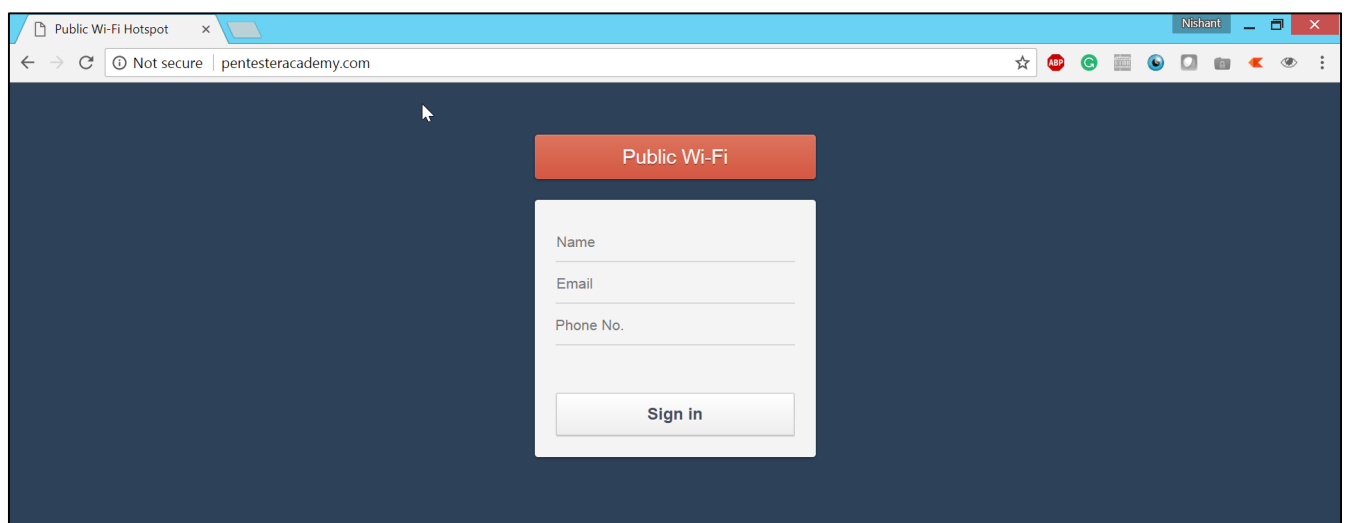
Deception Firmware: In Action

Let us now look at a demo! We are assuming the device is configured with SSID **Free_Internet** and the splash page is **D4 (Public WiFi)**.

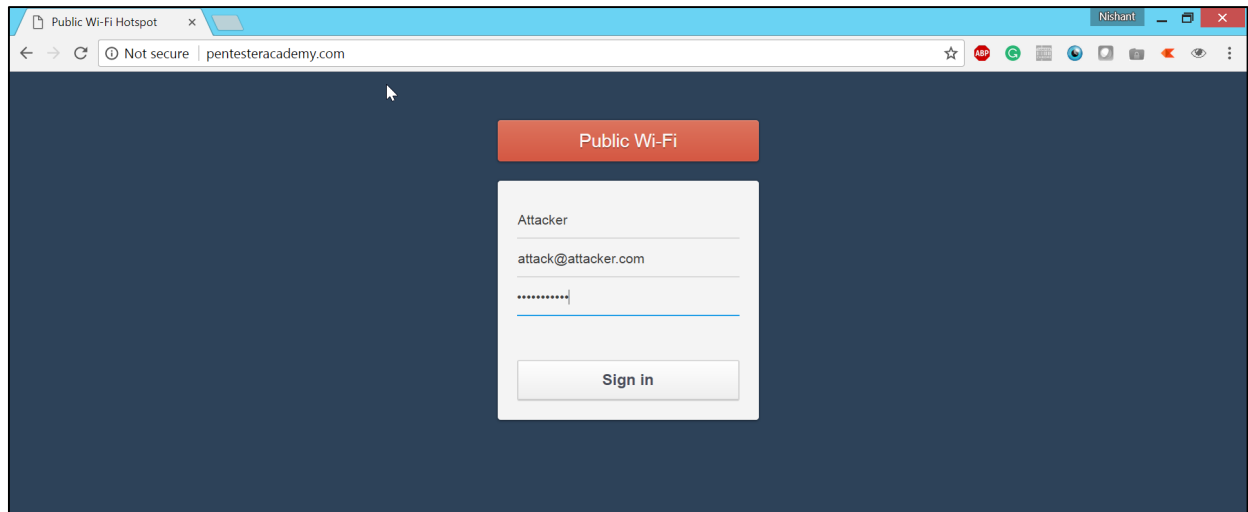
Step 1: The victim device connects to **Free_Internet**, an open WiFi network



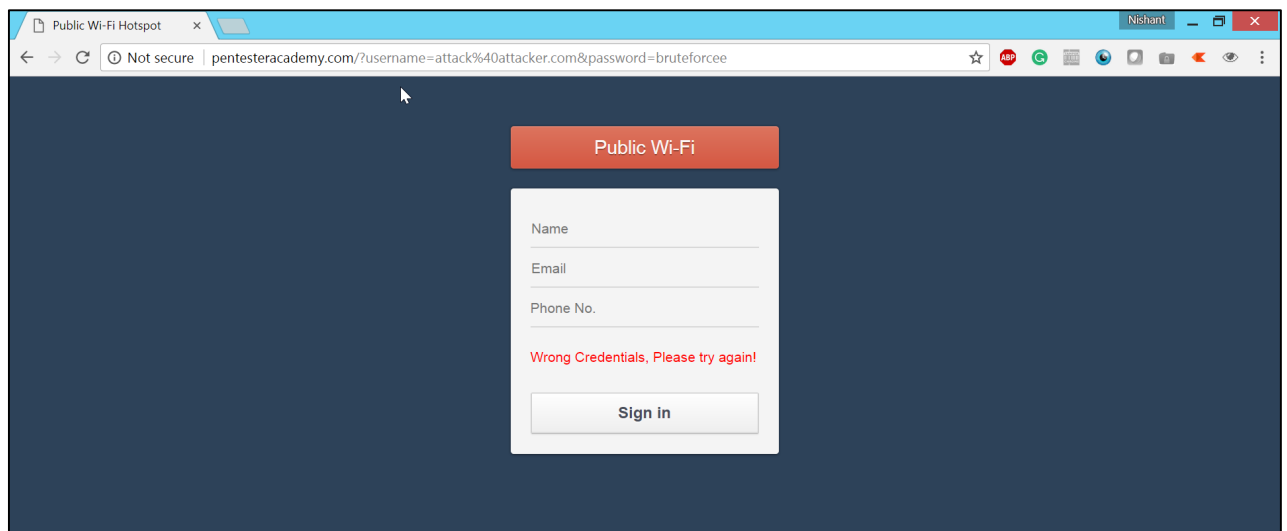
Step 2: When the victim now tries to access any webpage, he should be automatically redirected to our fake splash page.



Step 3: Any information that he enters in to the fields will be logged



Step 4: No matter what credentials are provided, an error page is shown. The victim might end up trying multiple combinations all of which are logged.



Step 5: We will use SEND command to view these stored credentials

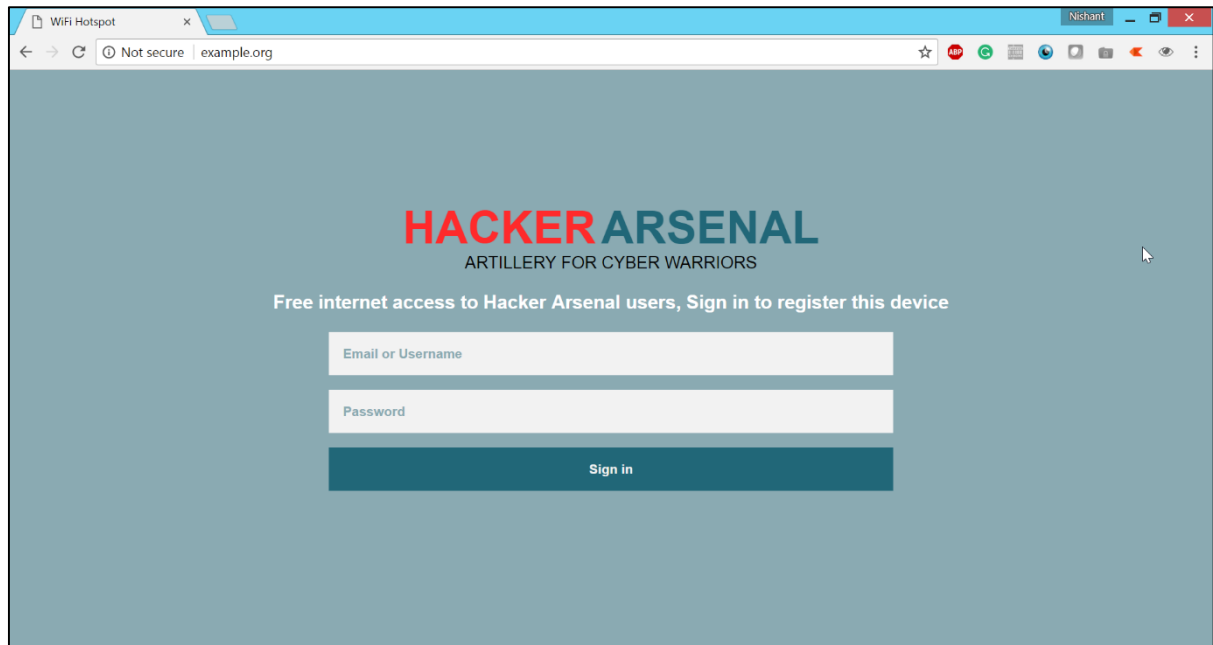
and other logs.

```
Received command: SEND
Dumping Command received. Dumping file.
Reading file: /log.txt
=====X=====
6161939: Deception SSID Free_Internet is up!
19446615: Change in Connected Client list ...: 1 now
19781591: Clients : 34:e6:ad:56:e1:04
39295034: Argument- username: attack@attacker.com
39427816: Argument- password: bruteforce
=====X=====
```

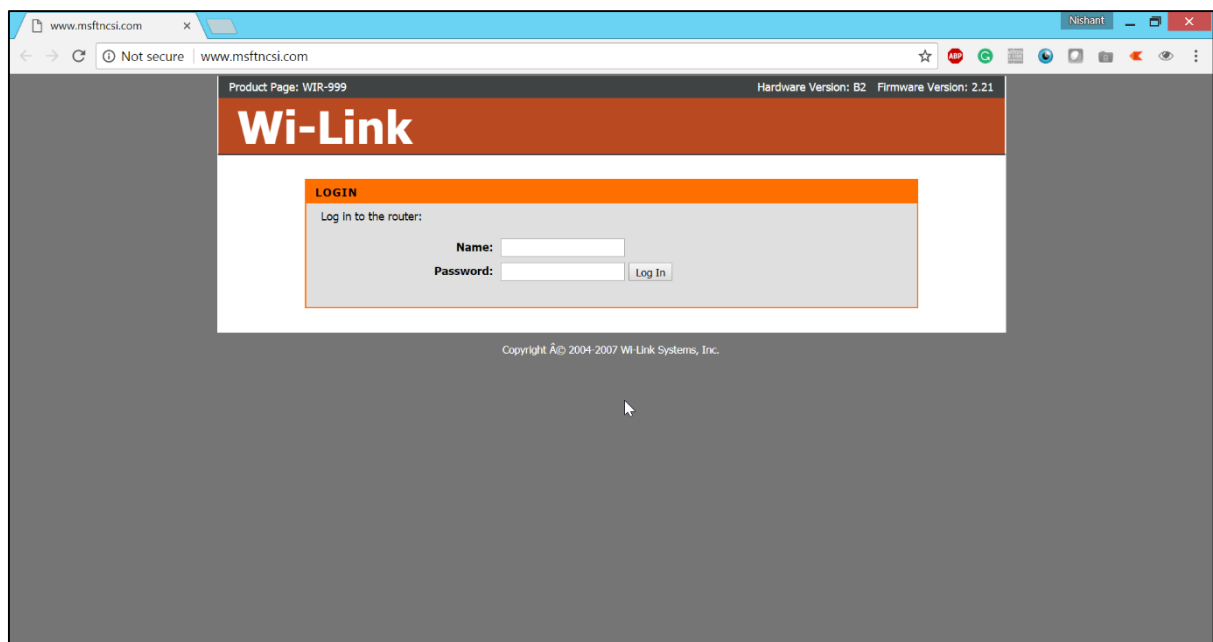
Deception Firmware: Splash Screens

The following screens are available for use on your device:

Screen 1 (default): Hacker Arsenal splash page



Screen 2: Wi-Link router login page



Screen 3: MyWiFi router login page

Login

Not secure | www.msftncsi.com

MyWiFi

Please Log In

Username & Email:

Password:

Log in

System Name : VVHO-MyWiFi

Copyright (c) 2002-2017, MyWiFi Networks, Inc.

Screen 4: Public WiFi splash page

Public Wi-Fi Hotspot

Not secure | www.msftncsi.com

Public Wi-Fi

Name

Email

Phone No.

Sign in

Screen 5: Coffee shop internet splash page screen

Coffee shop Wi-Fi Hotsp... x

Not secure | www.msftncsi.com

Free Coffee Shop Wi-Fi

Name

Email

Phone No.

Sign in

Troubleshooting:

- If you do not see any output then press and release the “**EN**” button on your device. This should reset the device and it should restart the program.
- If you still have problems with viewing the output then it might be a good idea to download the firmware again and flash the device.