User Manual: Getting Started

www.HackerArsenal.com

PENTESTER ACADEMY

HACKER ARSENAL
ARTILLERY FOR CYBER WARRIORS

Getting Started: 802.11 b/g/n Wi-Fi Scanner

The Scanner program is the default firmware on your device. This has been pre-flashed and tested to ensure the device is working as expected. When you power up the device, this program runs automatically and scans the air. It then reports the list of SSIDs, BSSIDs, Channel, RSSI, HT20/40 use and Authentication in the vicinity. The rest of this document discusses how to connect to the device and view the output of the Scanner program and also how to re-flash the scanner program on the device if you need to.

Scanner: Connecting on a Mac/Linux/Windows

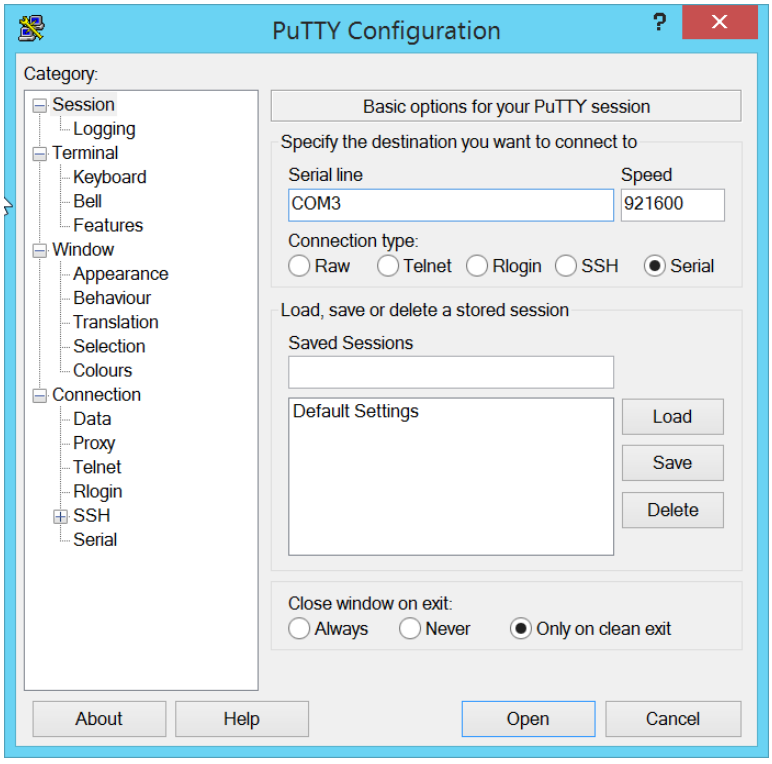
We will be communicating with the device using its serial port which is available through the USB interface. Hence, we will need a serial monitor program to talk to our device.

Windows:

Step 1: Download and install Putty from

https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

Step 2: Start Putty, configure the Serial Line to COMX (find the port name by using the Device Manager) with Speed 921600. Click Open.



Step 3:

You should now be able to see the scan results in tabular format within a few seconds.

	BSSID	SSID	Channel	BW	RSSI	Authentication
1	fc:0a:81:77:01:60	CAESARS	11	HT20	-74	OPEN
2	fc:0a:81:0d:f7:04	CaesarsVillas	1	HT20	-75	OPEN
3	fc:0a:81:0d:f7:00	CAESARS	1	HT20	-75	OPEN
4	fc:0a:81:0d:f7:06	DELTA	1	HT20	-75	WPA2 Enterprise
5	fc:0a:81:0d:f7:02	BETA	1	HT20	-75	WPA2 PSK
6	fc:0a:81:0d:f7:01	ALPHA	1	HT20	-75	WPA2 PSK
7	fc:0a:81:0d:f7:03	GAMMA	1	HT20	-75	WPA2 Enterprise
8	fc:0a:81:77:01:66	DELTA	11	HT20	-75	WPA2 Enterprise
9	fc:0a:81:77:01:61	ALPHA	11	HT20	-76	WPA2 PSK
10	fc:0a:81:77:01:63	GAMMA	11	HT20	-76	WPA2 Enterprise
11	fc:0a:81:77:01:64	CaesarsVillas	11	HT20	-77	OPEN
12	50:a7:33:09:57:98	5916	11	HT20	-83	WEP
13	fc:0a:81:0d:f0:e6	DELTA	11	HT20	-84	WPA2 Enterprise
14	fc:0a:81:78:37:d3	GAMMA	6	HT20	-87	WPA2 PSK
15	02:1a:11:f2:ed:bf	MattAP	6	HT20	-88	WPA2 PSK
16	fc:0a:81:0d:f0:e0	CAESARS	11	HT20	-89	OPEN
17	fc:0a:81:0d:f0:e4	CaesarsVillas	11	HT20	-89	OPEN
18	50:a7:33:09:67:58	6116	6	HT20	-91	WEP
19	fc:0a:81:78:37:d0	CAESARS	6	HT20	-92	OPEN

Linux:

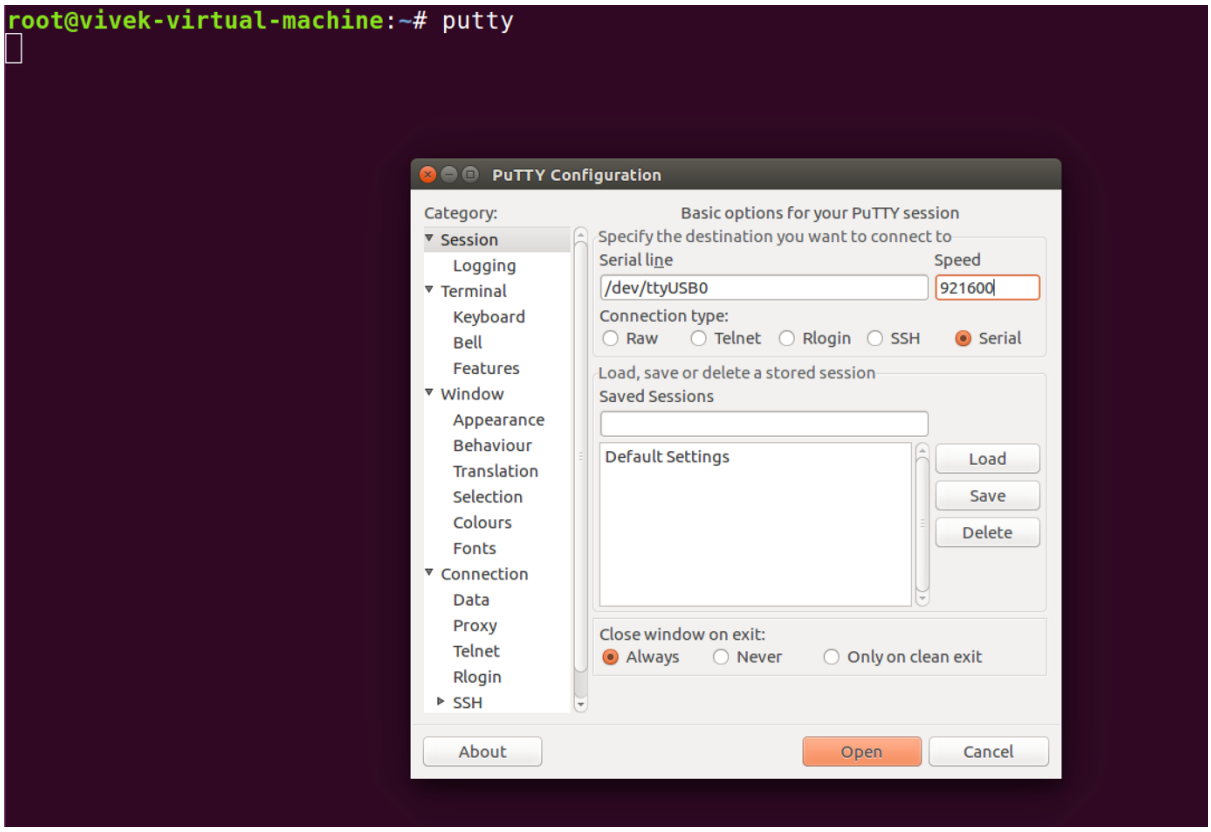
We will be using Ubuntu, but steps would be similar for other Linux distributions.

Step 1: Install Putty

```
root@vivek-virtual-machine:~# apt install putty
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  gyp libjs-inherits libjs-jquery libjs-node-uuid libjs-underscore libssl-dev libssl-doc libuv1
  libuv1-dev linux-headers-4.4.0-31 linux-headers-4.4.0-31-generic linux-headers-4.4.0-79
  linux-headers-4.4.0-79-generic linux-headers-4.4.0-81 linux-headers-4.4.0-81-generic
  linux-image-4.4.0-31-generic linux-image-4.4.0-79-generic linux-image-4.4.0-81-generic
  linux-image-extra-4.4.0-31-generic linux-image-extra-4.4.0-79-generic
  linux-image-extra-4.4.0-81-generic zlib1g-dev
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  putty-tools
Suggested packages:
  putty-doc
The following NEW packages will be installed:
  putty putty-tools
0 upgraded, 2 newly installed, 0 to remove and 261 not upgraded.
Need to get 662 kB of archives.
After this operation, 2,713 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Step 2: Launch Putty, select ***Connection Type*** as *Serial*, ***Speed*** as 921600 and ***Serial Line*** as */dev/ttyUSB0* or the correct port path.

Click ***Open*** to have Putty connect to the device.



Step 3: You should now be able to see the scan results table. The device automatically initiates a new scan every few seconds.

	BSSID	SSID	Channel	BW	RSSI	Authentication
1	fc:0a:81:77:01:60	CAESARS	11	HT20	-74	OPEN
2	fc:0a:81:0d:f7:04	CaesarsVillas	1	HT20	-75	OPEN
3	fc:0a:81:0d:f7:00	CAESARS	1	HT20	-75	OPEN
4	fc:0a:81:0d:f7:06	DELTA	1	HT20	-75	WPA2 Enterprise
5	fc:0a:81:0d:f7:02	BETA	1	HT20	-75	WPA2 PSK
6	fc:0a:81:0d:f7:01	ALPHA	1	HT20	-75	WPA2 PSK
7	fc:0a:81:0d:f7:03	GAMMA	1	HT20	-75	WPA2 Enterprise
8	fc:0a:81:77:01:66	DELTA	11	HT20	-75	WPA2 Enterprise
9	fc:0a:81:77:01:61	ALPHA	11	HT20	-76	WPA2 PSK
10	fc:0a:81:77:01:63	GAMMA	11	HT20	-76	WPA2 Enterprise
11	fc:0a:81:77:01:64	CaesarsVillas	11	HT20	-77	OPEN
12	50:a7:33:09:57:98	5916	11	HT20	-83	WEP
13	fc:0a:81:0d:f0:e6	DELTA	11	HT20	-84	WPA2 Enterprise
14	fc:0a:81:78:37:d3	GAMMA	6	HT20	-87	WPA2 PSK
15	02:1a:11:f2:ed:bf	MattAP	6	HT20	-88	WPA2 PSK
16	fc:0a:81:0d:f0:e0	CAESARS	11	HT20	-89	OPEN
17	fc:0a:81:0d:f0:e4	CaesarsVillas	11	HT20	-89	OPEN
18	50:a7:33:09:67:58	6116	6	HT20	-91	WEP
19	fc:0a:81:78:37:d0	CAESARS	6	HT20	-92	OPEN

Mac:

You will have to install the CP2102 drivers to use the device on a MAC. You can download and install the drivers from here:

https://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers

Once you have successfully installed the driver, please use the steps below:

Step 1:

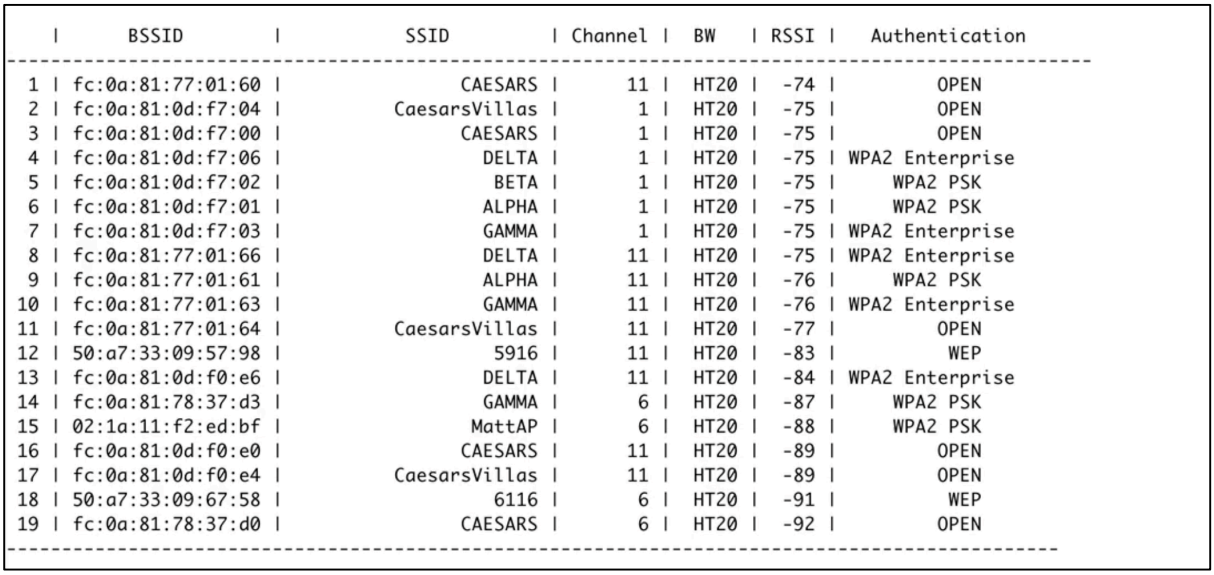
```
Viveks-MBP:~ vivek$ miniterm.py - 921600

--- Available ports:
---  1: /dev/cu.Bluetooth-Incoming-Port n/a
---  2: /dev/cu.SLAB_USBtoUART CP2102 USB to UART Bridge Controller -
ller
--- Enter port index or full name:
```

Step 2:

```
--- Enter port index or full name: 2
--- Miniterm on /dev/cu.SLAB_USBtoUART  921600,8,N,1 ---
--- Quit: Ctrl+] | Menu: Ctrl+T | Help: Ctrl+T followed by Ctrl+H ---
```

Step 3: You should now be able to see the scan results table. The device automatically initiates a new scan every few seconds.



	BSSID	SSID	Channel	BW	RSSI	Authentication
1	fc:0a:81:77:01:60	CAESARS	11	HT20	-74	OPEN
2	fc:0a:81:0d:f7:04	CaesarsVillas	1	HT20	-75	OPEN
3	fc:0a:81:0d:f7:00	CAESARS	1	HT20	-75	OPEN
4	fc:0a:81:0d:f7:06	DELTA	1	HT20	-75	WPA2 Enterprise
5	fc:0a:81:0d:f7:02	BETA	1	HT20	-75	WPA2 PSK
6	fc:0a:81:0d:f7:01	ALPHA	1	HT20	-75	WPA2 PSK
7	fc:0a:81:0d:f7:03	GAMMA	1	HT20	-75	WPA2 Enterprise
8	fc:0a:81:77:01:66	DELTA	11	HT20	-75	WPA2 Enterprise
9	fc:0a:81:77:01:61	ALPHA	11	HT20	-76	WPA2 PSK
10	fc:0a:81:77:01:63	GAMMA	11	HT20	-76	WPA2 Enterprise
11	fc:0a:81:77:01:64	CaesarsVillas	11	HT20	-77	OPEN
12	50:a7:33:09:57:98	5916	11	HT20	-83	WEP
13	fc:0a:81:0d:f0:e6	DELTA	11	HT20	-84	WPA2 Enterprise
14	fc:0a:81:78:37:d3	GAMMA	6	HT20	-87	WPA2 PSK
15	02:1a:11:f2:ed:bf	MattAP	6	HT20	-88	WPA2 PSK
16	fc:0a:81:0d:f0:e0	CAESARS	11	HT20	-89	OPEN
17	fc:0a:81:0d:f0:e4	CaesarsVillas	11	HT20	-89	OPEN
18	50:a7:33:09:67:58	6116	6	HT20	-91	WEP
19	fc:0a:81:78:37:d0	CAESARS	6	HT20	-92	OPEN

Troubleshooting:

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