Make your own Hacker Gadget

Vivek Ramachandran

Chief Trainer

http://PentesterAcademy.com

Installing Wireless Pentest Tools

FREE Course

- PDF Slides
- Code Snippets
- Automation Scripts
- Updates and Offers

http://PentesterAcademy.com/widy

Wireless-Tools

```
root@OpenWrt:~# iwconfig
-ash: iwconfig: not found
root@OpenWrt:~#
root@OpenWrt:~# opkg install wireless-tools
Installing wireless-tools (29-5) to root...
Downloading http://downloads.openwrt.org/attitude_adjustment/12.09/ar71xx/generic/package
pk.
Configuring wireless-tools.
root@OpenWrt:~#
root@OpenWrt:~# iwconfig
lo        no wireless extensions.

wlan0     IEEE 802.11bgn  ESSID:"TotallySecure"
          Mode:Managed  Frequency:2.462 GHz  Access Point: 3C:DF:BD:26:95:1B
          Bit Rate=57.8 Mb/s   Tx-Power=15 dBm
          RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=70/70  Signal level=-35 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:1  Invalid misc:4   Missed beacon:0

eth0      no wireless extensions.

br-lan    no wireless extensions.

root@OpenWrt:~#
```

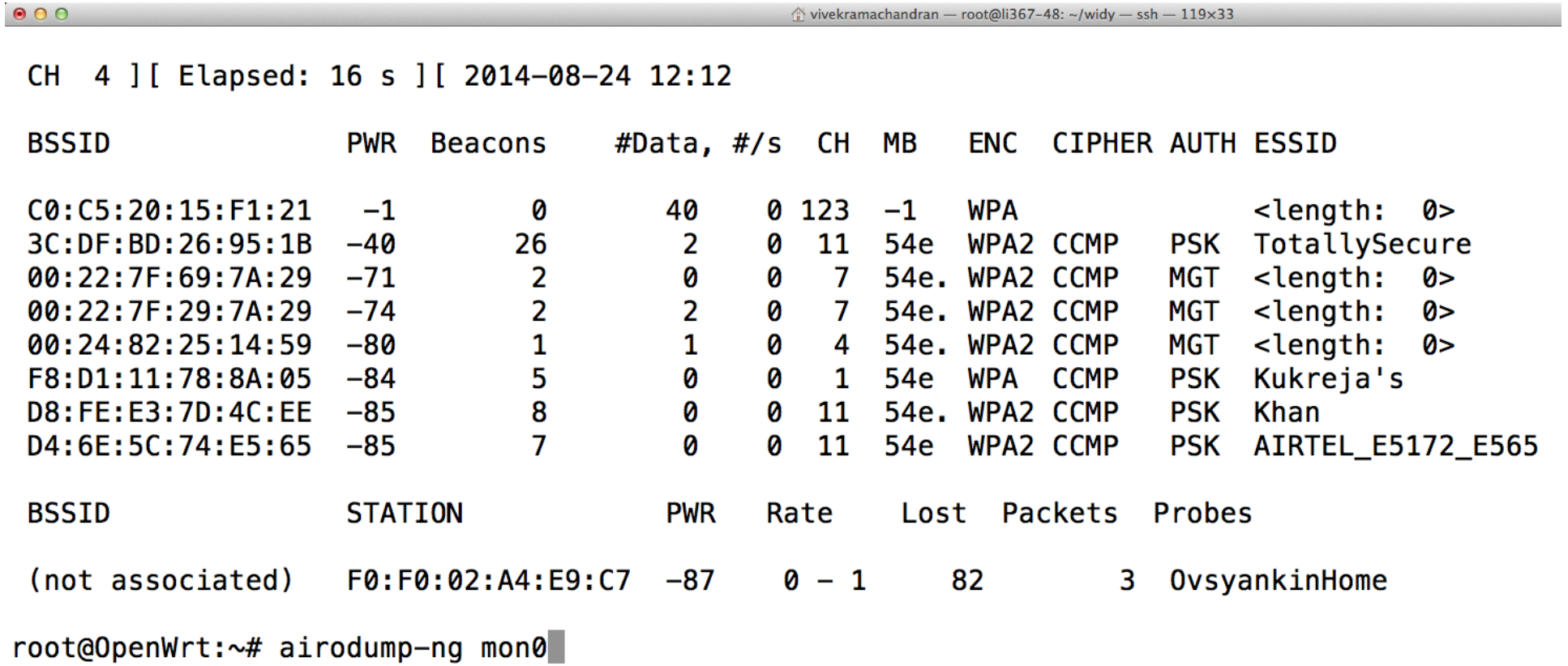
Aircrack-NG

```
root@OpenWrt:~# opkg find *aircrack*
aircrack-ng - 1.1-3 - Aircrack-ng is the next generation of aircrack with new features
aircrack-ptw - 1.0.0-1 - A tool using a new method for breaking WEP Keys
root@OpenWrt:~#
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.i
pk.
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:~# opkg install kmod-tun
Installing kmod-tun (3.3.8-1) to root...
Downloading http://downloads.openwrt.org/attitude_adjustment/12.09/ar71xx/generic/packages/kmod-tun_3.3.8-1_ar71xx.ipk.
Configuring kmod-tun.
root@OpenWrt:~#
```

Test Airacrack

```
root@OpenWrt:~# ifconfig wlan0 down
root@OpenWrt:~# airmon-ng


Interface       Chipset         Driver

wlan0           Atheros         ath9k - [phy0]

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)
                _
```

Test Aircrack (contd..)



Test Aircrack (contd..)

```
root@OpenWrt:~#
root@OpenWrt:~# iwconfig mon0 channel 11
root@OpenWrt:~#
root@OpenWrt:~# aireplay-ng --test mon0
12:13:34  Trying broadcast probe requests...
12:13:34  Injection is working!
12:13:36  Found 3 APs

12:13:36  Trying directed probe requests...
12:13:36  3C:DF:BD:26:95:1B - channel: 11 - 'TotallySecure'
12:13:37  Ping (min/avg/max): 2.172ms/12.331ms/44.048ms Power: -34.57
12:13:37  30/30: 100%
```

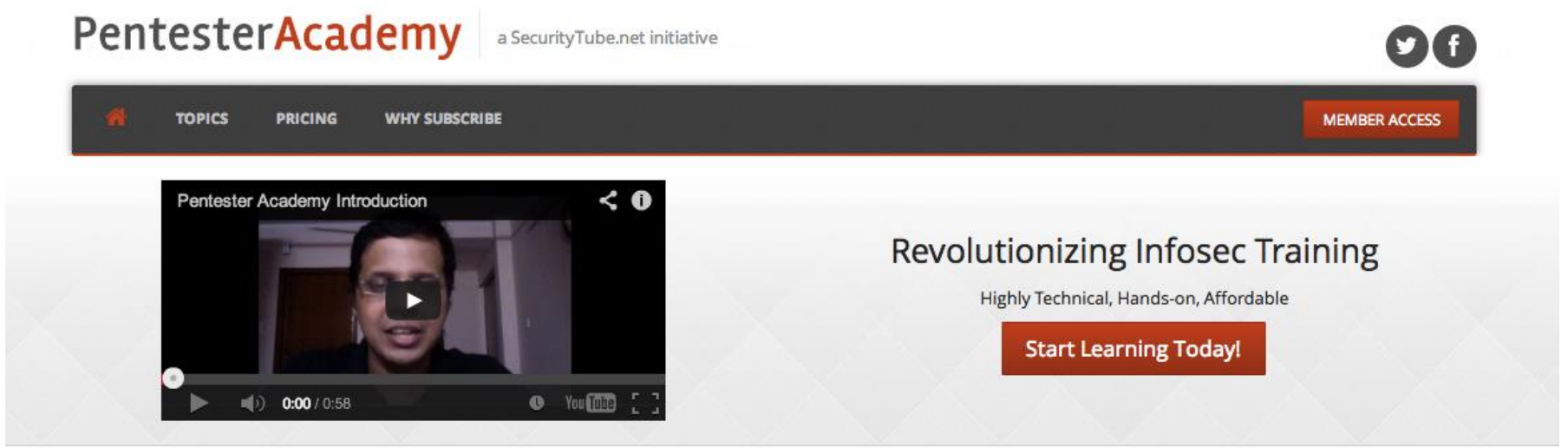
Test Aircrack (contd..)

```
root@OpenWrt:~# airbase-ng --essid Vivek mon0
12:17:12  Created tap interface at0
12:17:12  Trying to set MTU on at0 to 1500
12:17:12  Trying to set MTU on mon0 to 1800
12:17:12  Access Point with BSSID E8:DE:27:69:AA:6C started.

12:17:29  Client C8:BC:C8:EE:12:0B associated (unencrypted) to ESSID: "Vivek"
12:17:29  Client C8:BC:C8:EE:12:0B associated (unencrypted) to ESSID: "Vivek"
```

Mdk3

```
root@OpenWrt:~#
root@OpenWrt:~# opkg install mdk3
Installing mdk3 (v6-1) to root...
Downloading http://downloads.openwrt.org/attitude_adjustment/12.09/ar71xx/generic/pac
Configuring mdk3.
root@OpenWrt:~#
root@OpenWrt:~#
root@OpenWrt:~# mdk3 mon0 b -s 10

Current MAC: CD:BA:AB:F2:FB:E3 on Channel  2 with SSID: a71i0Rk
Current MAC: 48:9A:0A:BC:D5:0E on Channel  3 with SSID: [p.6>kvs35\$oxJh6&s2
Current MAC: 45:39:02:D8:E5:0A on Channel  6 with SSID: !D,55Y{:H7=bi6:r
Current MAC: 1B:01:07:0D:D8:FD on Channel  8 with SSID: jd{=wL5.CHX$- U%
Current MAC: AE:6D:45:46:27:86 on Channel  1 with SSID: U+F`fsP9j4TdtEDi5RRAn9wmdm
Current MAC: D0:55:F1:3C:8D:AF on Channel  9 with SSID: 7Gs>[S47czOww_X,BhqUO2;
Packets sent:     50 - Speed:   10 packets/sec^C
root@OpenWrt:~#
```

Pentester Academy



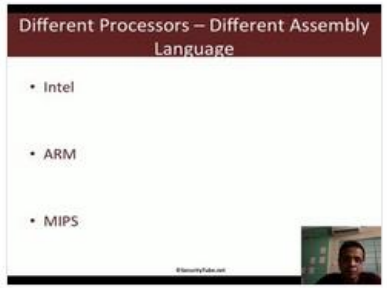
Latest Videos

New content added weekly!

Challenge 7: Cracking Digest Authentication Solution in WAP Challenges

Challenge 7: Cracking Digest Authentication in WAP Challenges

Module 1: GDB Test Solution in x86_64 Assembly Language and Shellcoding on Linux



Module 1: CPU Information in x86_64 Assembly Language and Shellcoding on Linux