

Make your own Hacker Gadget

Vivek Ramachandran

Chief Trainer

<http://PentesterAcademy.com>

Connecting to the Network

FREE Course

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

<http://PentesterAcademy.com/widy>

SSH into box

- Telnet gets disabled once you set the password
- SSH into the box with the same password and username root

Network Connectivity

```
root@OpenWrt:~# ifconfig -a
br-lan    Link encap:Ethernet  HWaddr E8:DE:27:69:AA:6C
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:899 errors:0 dropped:33 overruns:0 frame:0
          TX packets:748 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:109392 (106.8 KiB)  TX bytes:249768 (243.9 KiB)

eth0     Link encap:Ethernet  HWaddr E8:DE:27:69:AA:6C
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:900 errors:0 dropped:0 overruns:0 frame:0
          TX packets:751 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:122038 (119.1 KiB)  TX bytes:249906 (244.0 KiB)
          Interrupt:4

lo       Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1648 (1.6 KiB)  TX bytes:1648 (1.6 KiB)

wlan0    Link encap:Ethernet  HWaddr E8:DE:27:69:AA:6C
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:227 errors:0 dropped:0 overruns:0 frame:0
          TX packets:64 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:32
          RX bytes:56115 (54.7 KiB)  TX bytes:7496 (7.3 KiB)
```

GUI

The screenshot displays the OpenWrt web interface (LuCI) in a browser. The address bar shows the URL `192.168.1.1/cgi-bin/luci/;stok=b946101ecb461b9cbcd86b36edd1975d/admin/network/r`. The browser's address bar also includes a search bar and navigation icons. The page header shows the system status: `OpenWrt | OpenWrt Attitude Adjustment 12.09 | Load: 0.03 0.07 0.04 | Auto Refresh: on` and `Changes: 0`. The main navigation menu includes `Status`, `System`, `Network` (selected), and `Logout`. The `Network` section is further divided into `Interfaces`, `Wifi`, `DHCP and DNS`, `Hostnames`, `Static Routes`, `Firewall`, and `Diagnostics`. The `Interfaces` sub-section is active, showing an `Interface Overview` table. The table lists the `LAN` interface (br-lan) with its status and actions. The `LAN` interface is highlighted in green, indicating it is active. The status information for the `LAN` interface is: `Uptime: 0h 18m 25s`, `MAC-Address: E8:DE:27:69:AA:6C`, `RX: 465.12 KB (4063 Pkts.)`, `TX: 1.16 MB (3608 Pkts.)`, and `IPv4: 192.168.1.1/24`. The actions for the `LAN` interface are `Connect`, `Stop`, `Edit`, and `Delete`. There is also a button to `Add new interface...`

Network	Status	Actions
LAN br-lan	Uptime: 0h 18m 25s MAC-Address: E8:DE:27:69:AA:6C RX: 465.12 KB (4063 Pkts.) TX: 1.16 MB (3608 Pkts.) IPv4: 192.168.1.1/24	Connect Stop Edit Delete

[Add new interface...](#)

Connecting to your Wi-Fi

OpenWrt | OpenWrt Attitude Adjustment 12.09 | Load: 0.00 0.01 0.04 Changes: 0

Status System **Network** Logout

Interfaces Wifi DHCP and DNS Hostnames Static Routes Firewall Diagnostics

Join Network: Wireless Scan

TotallySecure Channel: 11 | Mode: Master | BSSID: 3C:DF:BD:26:95:1B | Encryption: mixed WPA/WPA2 - PSK Join Network

OpenWrt | OpenWrt Attitude Adjustment 12.09 | Load: 0.00 0.01 0.04 Changes: 0

Status System **Network** Logout

Interfaces Wifi DHCP and DNS Hostnames Static Routes Firewall Diagnostics

Join Network: Settings

Replace wireless configuration An additional network will be created if you leave this unchecked.

WPA passphrase Specify the secret encryption key here.

Name of the new network The allowed characters are: A-Z, a-z, 0-9 and _

Create / Assign firewall-zone

lan: lan:

wan: (empty)

unspecified -or- create:

Choose the firewall zone you want to assign to this interface. Select *unspecified* to remove the interface from the associated zone or fill out the *create* field to define a new zone and attach the interface to it.

Getting an IP and Internet Connection

```
root@OpenWrt:~# ifconfig wlan0
wlan0      Link encap:Ethernet  HWaddr E8:DE:27:69:AA:6C
           UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
           RX packets:27 errors:0 dropped:0 overruns:0 frame:0
           TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:32
           RX bytes:6518 (6.3 KiB)  TX bytes:288 (288.0 B)

root@OpenWrt:~# udhcpc -i wlan0
udhcpc (v1.19.4) started
Sending discover...
Sending select for 192.168.10.2...
Lease of 192.168.10.2 obtained, lease time 86400
udhcpc: ifconfig wlan0 192.168.10.2 netmask 255.255.255.0 broadcast +
udhcpc: setting default routers: 192.168.10.1
root@OpenWrt:~#
root@OpenWrt:~# ifconfig wlan0
wlan0      Link encap:Ethernet  HWaddr E8:DE:27:69:AA:6C
           inet addr:192.168.10.2  Bcast:192.168.10.255  Mask:255.255.255.0
           UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
           RX packets:54 errors:0 dropped:0 overruns:0 frame:0
           TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:32
           RX bytes:13532 (13.2 KiB)  TX bytes:1708 (1.6 KiB)

root@OpenWrt:~# ping google.com
ping: bad address 'google.com'
root@OpenWrt:~# echo nameserver 208.67.222.222 > /etc/resolv.conf
root@OpenWrt:~# ping google.com
PING google.com (173.194.36.40): 56 data bytes
64 bytes from 173.194.36.40: seq=0 ttl=55 time=49.304 ms
64 bytes from 173.194.36.40: seq=1 ttl=55 time=58.115 ms
```

Low Disk Space

The screenshot shows the OpenWrt web interface. The 'System' tab is active, and the 'Software' sub-tab is selected. A message indicates 'No package lists available' with an 'Update lists' button. Below this, a disk space warning shows 'Free space: 80% (872.00 KB)' with a progress bar. At the bottom, there are input fields for 'Download and install package:' and 'Filter:', each with an 'OK' or 'Find package' button.

```
root@OpenWrt:~# df -h
Filesystem      Size      Used Available Use% Mounted on
rootfs          1.1M      216.0K   872.0K   20% /
/dev/root       2.0M      2.0M      0    100% /rom
tmpfs           14.3M     568.0K   13.7M    4% /tmp
tmpfs           512.0K      0    512.0K   0% /dev
/dev/mtdblock3  1.1M      216.0K   872.0K   20% /overlay
overlayfs:/overlay 1.1M      216.0K   872.0K   20% /
root@OpenWrt:~# █
```

Connect our USB

dmesg

```
[ 1996.140000] usb 1-1: new high-speed USB device number 2 using ehci-platform
```

```
root@OpenWrt:~# df -h
```

Filesystem	Size	Used	Available	Use%	Mounted on
rootfs	1.1M	216.0K	872.0K	20%	/
/dev/root	2.0M	2.0M	0	100%	/rom
tmpfs	14.3M	604.0K	13.7M	4%	/tmp
tmpfs	512.0K	0	512.0K	0%	/dev
/dev/mtdblock3	1.1M	216.0K	872.0K	20%	/overlay
overlayfs:/overlay	1.1M	216.0K	872.0K	20%	/

```
root@OpenWrt:~# ls /dev/
```

bus	mem	mtd2	mtd4ro	mtdblock2	port	shm	ttyS10	ttyS15	ttyS6	watchdog
console	mtd0	mtd2ro	mtd5	mtdblock3	ppp	tty	ttyS11	ttyS2	ttyS7	zero
full	mtd0ro	mtd3	mtd5ro	mtdblock4	ptmx	ttyATH0	ttyS12	ttyS3	ttyS8	
kmsg	mtd1	mtd3ro	mtdblock0	mtdblock5	pts	ttyS0	ttyS13	ttyS4	ttyS9	
log	mtd1ro	mtd4	mtdblock1	null	random	ttyS1	ttyS14	ttyS5	urandom	

```
root@OpenWrt:~# █
```

We don't have the drivers 😊

FREE Course

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

<http://PentesterAcademy.com/widy>

Pentester Academy

PentesterAcademy

a SecurityTube.net initiative



TOPICS

PRICING

WHY SUBSCRIBE

MEMBER ACCESS



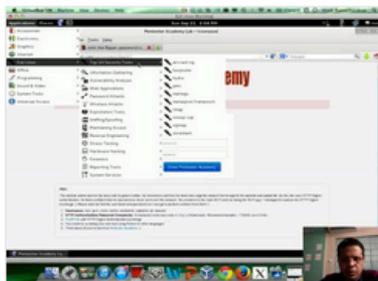
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

Start Learning Today!

Latest Videos

New content added weekly!



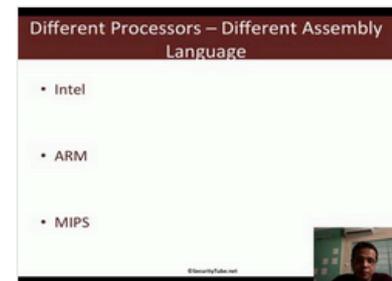
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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