Netgear WNAP320

Router Webpage:

WNAP320 — ProSAFE Wireless-N Access Point

Find setup help, user guides, product information, firmware, and troubleshooting for your WNAP320 wireless access point on our official NETGEAR Support site today

https://www.netgear.com/support/product/wnap320#download

Firmware Version: 2.0.3

Firmware Download Link:

https://www.downloads.netgear.com/files/GDC/WNAP320/WNAP320 Firmware Version 2.0.3.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 Netgear -sql 127.0.0.1 -np -nk "../../INSE6120-Fall2023-Project-Group7/Rakshith/Netgear WNAP32
>> Database Image ID: 1

/home/kali/Desktop/INSE6120-Fall2023-Project-Group7/Rakshith/Netgear WNAP320/firmware/WNAP320 Firmware Version 2.0.3.zip
>> MD5: 51eddc7046d77a752ca4b39fbda50aff
>> Tag: 1
>> Temp: /tmp/tmptz48s8uq
>> Status: Kernel: True, Rootfs: False, Do_Kernel: False,                 Do_Rootfs: True
>>>> Zip archive data, at least v2.0 to extract, compressed size: 1197, uncompressed size: 2667, name: ReleaseNotes_WNAP320_fw_2.0.3.HTML
>> Recursing into archive ...

/tmp/tmptz48s8uq/_WNAP320 Firmware Version 2.0.3.zip.extracted/WNAP320_V2.0.3_firmware.tar
        >> MD5: 6b66d0c845ea6f086e0424158d8e5f26
        >> Tag: 1
        >> Temp: /tmp/tmpm7tn0u0r
        >> Status: Kernel: True, Rootfs: False, Do_Kernel: False,                 Do_Rootfs: True
        >>>> POSIX tar archive (GNU), owner user name: "gz.uImage"
        >> Recursing into archive ...

/tmp/tmpm7tn0u0r/_WNAP320_V2.0.3_firmware.tar.extracted/kernel.md5
                >> MD5: 0e15e5398024c854756d3e5f7bc78877
                >> Skipping: text/plain...

/tmp/tmpm7tn0u0r/_WNAP320_V2.0.3_firmware.tar.extracted/root_fs.md5
                >> MD5: b43dc86ce23660652d37d97651ba1c77
                >> Skipping: text/plain...
```

```
/tmp/tmpm7tn0u0r/_WNAP320_V2.0.3_firmware.tar.extracted/rootfs.squashfs
                >> MD5: 7ce95b252346d2486d55866a1a9782be
                >> Tag: 1
                >> Temp: /tmp/tmpm77x_hcf
                >> Status: Kernel: True, Rootfs: False, Do_Kernel: False,                 Do_Rootfs: True
                >>>> XAR archive, version: -6057, header size: 2664, TOC compressed: 18154158142782153979, TOC uncompressed: 10765983841730
                >> Recursing into archive ...
                >>>> Squashfs filesystem, big endian, lzma signature, version 3.1, size: 4433988 bytes, 1247 inodes, blocksize: 65536 bytes
                >>>> Found Linux filesystem in /tmp/tmpm77x_hcf/_rootfs.squashfs.extracted/squashfs-root!
                >> Skipping: completed!
                >> Cleaning up /tmp/tmpm77x_hcf...
        >> Skipping: completed!
        >> Cleaning up /tmp/tmpm7tn0u0r...
>> Skipping: completed!
>> Cleaning up /tmp/tmptz48s8uq...
```

2. Identify the architecture of firmware 1 and store the result in the image table of the database

```
┌──(kali㉿kali)-[~/Desktop/Project/firmadyne]
└─$ ./scripts/getArch.sh ./images/1.tar.gz
./bin/busybox: mipseb
Password for user firmadyne:
```

3. Load the contents of the filesystem for firmware 1 into the database, populating the object and object_to_image tables.

```
┌──(kali㉿kali)-[~/Desktop/Project/firmadyne]
└─$ ./scripts/tar2db.py -i 1 -f ./images/1.tar.gz
```

4. Create the QEMU disk image for firmware 1

```
┌──(kali㉿kali)-[~/Desktop/Project/firmadyne]
└─$ sudo ./scripts/makeImage.sh 1
Querying database for architecture... Password for user firmadyne:
mipseb
----Running----
----Creating working directory /home/kali/Desktop/Project/firmadyne/scratch//1/----
----The size of root filesystem '/home/kali/Desktop/Project/firmadyne/images//1.tar.gz' is 22722560-----
----Creating QEMU Image /home/kali/Desktop/Project/firmadyne/scratch//1//image.raw with size 33554432----
Formatting '/home/kali/Desktop/Project/firmadyne/scratch//1//image.raw', fmt=raw size=33554432
----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 0x628bac0b.

Command (m for help): Created a new DOS (MBR) disklabel with disk identifier 0x9e320577.

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 (2048-65535, default 2048): Last sector, +/-sectors or +/-size{K,M,G,T,
Created a new partition 1 of type 'Linux' and of size 31 MiB.

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

----Mounting QEMU Image----
----Device mapper created at /dev/mapper/loop0p1----
----Creating Filesystem----
mke2fs 1.47.0 (5-Feb-2023)
Discarding device blocks: done
Creating filesystem with 31744 1k blocks and 7936 inodes
Filesystem UUID: 046da6e9-8036-4789-966c-437bd1738a28
Superblock backups stored on blocks:
        8193, 24577

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//1//image/----
----Mounting QEMU Image Partition 1----
----Extracting Filesystem Tarball to Mountpoint----
----Creating FIRMADYNE Directories----
----Patching Filesystem (chroot)----
Backing up /etc/passwd to /etc/passwd.bak
Backing up /etc/shadow to /etc/shadow.bak
Unlocking and blanking default root password. (*May not work since some routers reset the password back to default when booting)
Renaming /etc/securetty to /etc/securetty.bak
----Setting up FIRMADYNE----
----Unmounting QEMU Image----
----Deleting device mapper----
```

5. Infer the network configuration for firmware 1. Kernel messages are logged to ./scratch/1/qemu.initial.serial.log.

```
┌──(kali㉿kali)-[~/Desktop/Project/firmadyne]
└─$ ./scripts/inferNetwork.sh 1
Querying database for architecture... Password for user firmadyne:
mipseb
Running firmware 1: terminating after 60 secs...
qemu-system-mips: terminating on signal 2 from pid 25388 (timeout)
Inferring network...
Interfaces: [('brtrunk', '192.168.0.100')]
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.

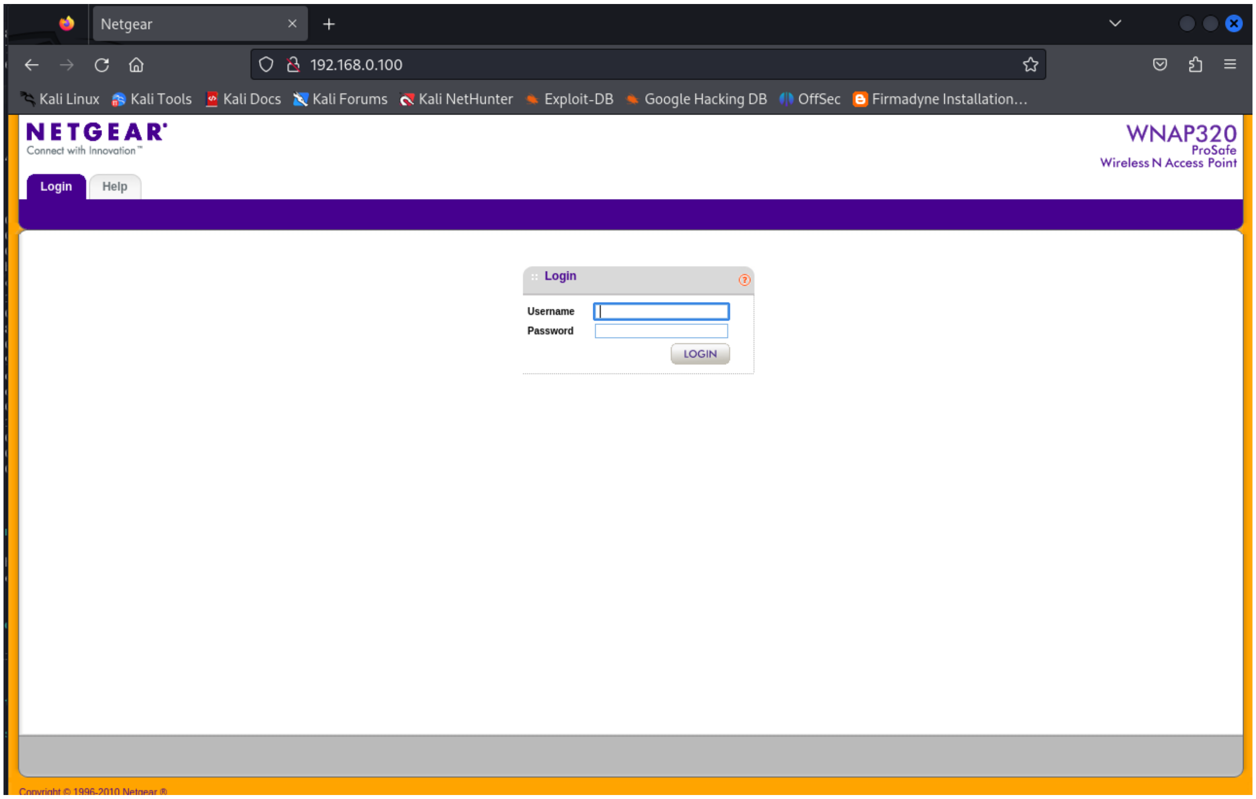
```
┌──(kali㉿kali)-[~/Desktop/Project/firmadyne]
└─$ ./scratch/1/run.sh
Creating TAP device tap1_0...
Set 'tap1_0' persistent and owned by uid 1000
Bringing up TAP device...
Adding route to 192.168.0.100...
Starting firmware emulation... use Ctrl-a + x to exit
[    0.000000] Linux version 2.6.39.4+ (ddcc@ddcc-virtual) (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=64,64,64,64,64,64,64,64,64,64 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 320.00 MHz
[    0.000000] Console: colour dummy device 80x25
[    0.004000] Calibrating delay loop... 1522.68 BogoMIPS (lpj=3045376)
[    0.024000] pid_max: default: 32768 minimum: 301
[    0.028000] Mount-cache hash table entries: 512
[    0.036000] Performance counters: No available PMU.
[    0.040000] NET: Registered protocol family 16
[    0.052000] bio: create slab <bio-0> at 0
[    0.052000] vgaarb: loaded
[    0.056000] SCSI subsystem initialized
[    0.056000] libata version 3.00 loaded.
[    0.056000] usbcore: registered new interface driver usbfs
[    0.056000] usbcore: registered new interface driver hub
[    0.056000] usbcore: registered new device driver usb
[    0.060000] pci 0000:00:00.0: [2046:ab11] type 0 class 0x001000
[    0.060000] pci 0000:00:0a.0: [8086:7110] type 0 class 0x000601
[    0.064000] pci 0000:00:0a.1: [8086:7111] type 0 class 0x000101
[    0.064000] pci 0000:00:0a.1: reg 20: [io  0x0000-0x000f]
[    0.064000] pci 0000:00:0a.2: [8086:7112] type 0 class 0x000c03
[    0.064000] pci 0000:00:0a.2: reg 20: [io  0x0000-0x001f]
[    0.064000] pci 0000:00:0a.3: [8086:7113] type 0 class 0x000680
[    0.064000] pci 0000:00:0a.3: address space collision: [io  0x1100-0x110f] conflicts with GT-64120 PCI I/O [io  0x1000-0x1fffff]
[    0.064000] pci 0000:00:12.0: [1013:00b8] type 0 class 0x000300
[    0.064000] pci 0000:00:12.0: reg 10: [mem 0x00000000-0x01ffffff pref]
[    0.064000] pci 0000:00:12.0: reg 14: [mem 0x00000000-0x00000fff]
[    0.064000] pci 0000:00:12.0: reg 30: [mem 0x00000000-0x0000ffff pref]
[    0.064000] pci 0000:00:13.0: [8086:100e] type 0 class 0x000200
[    0.064000] pci 0000:00:13.0: reg 10: [mem 0x00000000-0x0001ffff]
[    0.064000] pci 0000:00:13.0: reg 14: [io  0x0000-0x003f]
[    0.068000] pci 0000:00:13.0: reg 30: [mem 0x00000000-0x0003ffff pref]
[    0.068000] pci 0000:00:14.0: [8086:100e] type 0 class 0x000200
[    0.068000] pci 0000:00:14.0: reg 10: [mem 0x00000000-0x0001ffff]
[    0.068000] pci 0000:00:14.0: reg 14: [io  0x0000-0x003f]
[    0.068000] pci 0000:00:14.0: reg 30: [mem 0x00000000-0x0003ffff pref]
[    0.068000] pci 0000:00:15.0: [8086:100e] type 0 class 0x000200
[    0.068000] pci 0000:00:15.0: reg 10: [mem 0x00000000-0x0001ffff]
[    0.068000] pci 0000:00:15.0: reg 14: [io  0x0000-0x003f]
[    0.068000] pci 0000:00:15.0: reg 30: [mem 0x00000000-0x0003ffff pref]
[    0.068000] pci 0000:00:16.0: [8086:100e] type 0 class 0x000200
[    0.068000] pci 0000:00:16.0: reg 10: [mem 0x00000000-0x0001ffff]
[    0.068000] pci 0000:00:16.0: reg 14: [io  0x0000-0x003f]
[    0.068000] pci 0000:00:16.0: reg 30: [mem 0x00000000-0x0003ffff pref]
[    0.068000] vgaarb: device added: PCI:0000:00:12.0,decodes=io+mem,owns=none,locks=none
[    0.072000] pci 0000:00:0a.3: BAR 8: [io  0x1100-0x110f] has bogus alignment
[    0.072000] pci 0000:00:12.0: BAR 0: assigned [mem 0x10000000-0x11ffffff pref]
[    0.072000] pci 0000:00:12.0: BAR 0: set to [mem 0x10000000-0x11ffffff pref] (PCI address [0x10000000-0x11ffffff])
[    0.076000] pci 0000:00:13.0: BAR 6: assigned [mem 0x12000000-0x1203ffff pref]
[    0.076000] pci 0000:00:14.0: BAR 6: assigned [mem 0x12040000-0x1207ffff pref]
[    0.076000] pci 0000:00:15.0: BAR 6: assigned [mem 0x12080000-0x120bffff pref]
[    0.076000] pci 0000:00:16.0: BAR 6: assigned [mem 0x120c0000-0x120fffff pref]
[    0.076000] pci 0000:00:13.0: BAR 0: assigned [mem 0x12100000-0x1211ffff]
[    0.076000] pci 0000:00:13.0: BAR 0: set to [mem 0x12100000-0x1211ffff] (PCI address [0x12100000-0x1211ffff])
[    0.076000] pci 0000:00:14.0: BAR 0: assigned [mem 0x12120000-0x1213ffff]
[    0.076000] pci 0000:00:14.0: BAR 0: set to [mem 0x12120000-0x1213ffff] (PCI address [0x12120000-0x1213ffff])
[    0.076000] pci 0000:00:15.0: BAR 0: assigned [mem 0x12140000-0x1215ffff]
[    0.076000] pci 0000:00:15.0: BAR 0: set to [mem 0x12140000-0x1215ffff] (PCI address [0x12140000-0x1215ffff])
[    0.076000] pci 0000:00:16.0: BAR 0: assigned [mem 0x12160000-0x1217ffff]
[    0.076000] pci 0000:00:16.0: BAR 0: set to [mem 0x12160000-0x1217ffff] (PCI address [0x12160000-0x1217ffff])
[    0.076000] pci 0000:00:12.0: BAR 6: assigned [mem 0x12180000-0x1218ffff pref]
[    0.076000] pci 0000:00:12.0: BAR 1: assigned [mem 0x12190000-0x12190fff]
[    0.076000] pci 0000:00:12.0: BAR 1: set to [mem 0x12190000-0x12190fff] (PCI address [0x12190000-0x12190fff])
[    0.076000] pci 0000:00:13.0: BAR 1: assigned [io  0x1000-0x103f]
[    0.076000] pci 0000:00:13.0: BAR 1: set to [io  0x1000-0x103f] (PCI address [0x1000-0x103f])
[    0.076000] pci 0000:00:14.0: BAR 1: assigned [io  0x1040-0x107f]
[    0.076000] pci 0000:00:14.0: BAR 1: set to [io  0x1040-0x107f] (PCI address [0x1040-0x107f])
[    0.076000] pci 0000:00:15.0: BAR 1: assigned [io  0x1080-0x10bf]
[    0.076000] pci 0000:00:15.0: BAR 1: set to [io  0x1080-0x10bf] (PCI address [0x1080-0x10bf])
[    0.080000] pci 0000:00:16.0: BAR 1: assigned [io  0x10c0-0x10ff]
[    0.080000] pci 0000:00:16.0: BAR 1: set to [io  0x10c0-0x10ff] (PCI address [0x10c0-0x10ff])
[    0.080000] pci 0000:00:0a.2: BAR 4: assigned [io  0x1400-0x141f]
[    0.080000] pci 0000:00:0a.2: BAR 4: set to [io  0x1400-0x141f] (PCI address [0x1400-0x141f])
[    0.080000] pci 0000:00:00.0: BAR 2: assigned [mem 0x12191000-0x1219100f 64bit pref]
[    0.080000] pci 0000:00:00.0: BAR 2: error updating (0x1219100c != 0x00001c)
[    0.080000] pci 0000:00:00.0: BAR 2: error updating (high 0x000000 != 0x00001f)
[    0.080000] pci 0000:00:00.0: BAR 2: set to [mem 0x12191000-0x1219100f 64bit pref] (PCI address [0x12191000-0x1219100f])
[    0.080000] pci 0000:00:00.0: BAR 4: assigned [mem 0x12191010-0x1219101f 64bit]
[    0.080000] pci 0000:00:00.0: BAR 4: error updating (0x12191014 != 0x000014)
[    0.080000] pci 0000:00:00.0: BAR 4: error updating (high 0x000000 != 0x1000014)
[    0.080000] pci 0000:00:00.0: BAR 4: set to [mem 0x12191010-0x1219101f 64bit] (PCI address [0x12191010-0x1219101f])
[    0.080000] pci 0000:00:0a.1: BAR 4: assigned [io  0x1420-0x142f]
[    0.080000] pci 0000:00:0a.1: BAR 4: set to [io  0x1420-0x142f] (PCI address [0x1420-0x142f])
[    0.084000] cfg80211: Calling CRDA to update world regulatory domain
[    0.088000] Switching to clocksource MIPS
[    0.088000] NET: Registered protocol family 2
[    0.092000] Switched to NOHz mode on CPU #0
[    0.092000] IP route cache hash table entries: 2048 (order: 1, 8192 bytes)
[    0.096000] TCP established hash table entries: 8192 (order: 4, 65536 bytes)
[    0.096000] TCP bind hash table entries: 8192 (order: 3, 32768 bytes)
[    0.096000] TCP: Hash tables configured (established 8192 bind 8192)
[    0.096000] TCP reno registered
[    0.096000] UDP hash table entries: 256 (order: 0, 4096 bytes)
[    0.096000] UDP-Lite hash table entries: 256 (order: 0, 4096 bytes)
[    0.100000] NET: Registered protocol family 1
[    0.100000] PCI: CLS 0 bytes, default 64
[    0.164000] squashfs: version 4.0 (2009/01/31) Phillip Lougher
[    0.164000] Registering unionfs 2.6 (for 2.6.39.4)
[    0.164000] JFFS2 version 2.2. (NAND) © 2001-2006 Red Hat, Inc.
[    0.164000] ROMFS MTD (C) 2007 Red Hat, Inc.
[    0.164000] msgmni has been set to 492
[    0.172000] Block layer SCSI generic (bsg) driver version 0.4 loaded (major 253)
[    0.172000] io scheduler noop registered
[    0.172000] io scheduler cfq registered (default)
[    0.172000] firmadyne: devfs: 1, execute: 1, procfs: 1, syscall: 0
[    0.176000] firmadyne: Cannot register character device: watchdog, 0xa, 0x82!
[    0.176000] firmadyne: Cannot register character device: wdt, 0xfd, 0x0!
[    0.208000] PCI: Enabling device 0000:00:12.0 (0000 -> 0002)
[    0.208000] cirrusfb 0000:00:12.0: Cirrus Logic chipset on PCI bus, RAM (4096 kB) at 0x10000000
[    0.468000] Console: switching to colour frame buffer device 80x30
[    0.484000] Serial: 8250/16550 driver, 4 ports, IRQ sharing enabled
[    0.512000] serial8250.0: ttyS0 at I/O 0x3f8 (irq = 4) is a 16550A
[    0.512000] console [ttyS0] enabled, bootconsole disabled
[    0.512000] console [ttyS0] enabled, bootconsole disabled
[    0.536000] serial8250.0: ttyS1 at I/O 0x2f8 (irq = 3) is a 16550A
[    0.536000] brd: module loaded
[    0.536000] loop: module loaded
[    0.536000] ata_piix 0000:00:0a.1: version 2.13
[    0.536000] PCI: Enabling device 0000:00:0a.1 (0000 -> 0001)
[    0.544000] PCI: Setting latency timer of device 0000:00:0a.1 to 64
[    0.552000] scsi0 : ata_piix
[    0.552000] scsi1 : ata_piix
[    0.552000] ata1: PATA max UDMA/33 cmd 0x1f0 ctl 0x3f6 bmdma 0x1420 irq 14
[    0.556000] ata2: PATA max UDMA/33 cmd 0x170 ctl 0x376 bmdma 0x1428 irq 15
[    0.560000] [nandsim] warning: read_byte: unexpected data output cycle, state is STATE_READY return 0x0
[    0.560000] [nandsim] warning: read_byte: unexpected data output cycle, state is STATE_READY return 0x0
[    0.560000] [nandsim] warning: read_byte: unexpected data output cycle, state is STATE_READY return 0x0
[    0.560000] [nandsim] warning: read_byte: unexpected data output cycle, state is STATE_READY return 0x0
[    0.560000] [nandsim] warning: read_byte: unexpected data output cycle, state is STATE_READY return 0x0
[    0.560000] [nandsim] warning: read_byte: unexpected data output cycle, state is STATE_READY return 0x0
[    0.560000] NAND device: Manufacturer ID: 0x98, Chip ID: 0x39 (Toshiba NAND 128MiB 1,8V 8-bit)
[    0.560000] flash size: 128 MiB
[    0.560000] page size: 512 bytes
[    0.560000] OOB area size: 16 bytes
[    0.560000] sector size: 16 KiB
[    0.560000] pages number: 262144
[    0.560000] pages per sector: 32
[    0.560000] bus width: 8
[    0.560000] bits in sector size: 14
[    0.564000] bits in page size: 9
[    0.564000] bits in OOB size: 4
[    0.564000] flash size with OOB: 135168 KiB
[    0.564000] page address bytes: 4
[    0.564000] sector address bytes: 3
[    0.564000] options: 0x62
[    0.568000] Scanning device for bad blocks
[    0.604000] Creating 11 MTD partitions on "NAND 128MiB 1,8V 8-bit":
[    0.604000] 0x000000000000-0x000000100000 : "NAND simulator partition 0"
[    0.616000] 0x000000100000-0x000000200000 : "NAND simulator partition 1"
[    0.616000] 0x000000200000-0x000000300000 : "NAND simulator partition 2"
[    0.616000] 0x000000300000-0x000000400000 : "NAND simulator partition 3"
[    0.616000] 0x000000400000-0x000000500000 : "NAND simulator partition 4"
[    0.620000] 0x000000500000-0x000000600000 : "NAND simulator partition 5"
[    0.620000] 0x000000600000-0x000000700000 : "NAND simulator partition 6"
[    0.620000] 0x000000700000-0x000000800000 : "NAND simulator partition 7"
[    0.620000] 0x000000800000-0x000000900000 : "NAND simulator partition 8"
[    0.620000] 0x000000900000-0x000000a00000 : "NAND simulator partition 9"
[    0.620000] 0x000000a00000-0x000008000000 : "NAND simulator partition 10"
[    0.624000] e1000: Intel(R) PRO/1000 Network Driver - version 7.3.21-k8-NAPI
[    0.624000] e1000: Copyright (c) 1999-2006 Intel Corporation.
[    0.624000] PCI: Enabling device 0000:00:13.0 (0000 -> 0003)
[    0.624000] PCI: Setting latency timer of device 0000:00:13.0 to 64
[    0.904000] ata2.01: NODEV after polling detection
[    0.908000] ata2.00: ATAPI: QEMU DVD-ROM, 2.5+, max UDMA/100
[    0.908000] ata2.00: configured for UDMA/33
[    0.912000] ata1.01: NODEV after polling detection
[    0.912000] ata1.00: ATA-7: QEMU HARDDISK, 2.5+, max UDMA/100
[    0.912000] ata1.00: 65536 sectors, multi 16: LBA48
[    0.912000] ata1.00: configured for UDMA/33
[    0.924000] scsi 0:0:0:0: Direct-Access     ATA      QEMU HARDDISK    2.5+ PQ: 0 ANSI: 5
[    0.928000] scsi 1:0:0:0: CD-ROM            QEMU     QEMU DVD-ROM     2.5+ PQ: 0 ANSI: 5
[    0.932000] sd 0:0:0:0: [sda] 65536 512-byte logical blocks: (33.5 MB/32.0 MiB)
[    0.932000] sd 0:0:0:0: [sda] Write Protect is off
[    0.932000] sd 0:0:0:0: [sda] Mode Sense: 00 3a 00 00
[    0.932000] sd 0:0:0:0: [sda] Write cache: enabled, read cache: enabled, doesn't support DPO or FUA
[    0.956000] e1000 0000:00:13.0: eth0: (PCI:33MHz:32-bit) 52:54:00:12:34:56
[    0.956000] e1000 0000:00:13.0: eth0: Intel(R) PRO/1000 Network Connection
[    0.956000] PCI: Enabling device 0000:00:14.0 (0000 -> 0003)
[    0.956000] PCI: Setting latency timer of device 0000:00:14.0 to 64
[    0.968000]  sda: sda1
[    0.972000] sd 0:0:0:0: [sda] Attached SCSI disk
[    1.284000] e1000 0000:00:14.0: eth1: (PCI:33MHz:32-bit) 52:54:00:12:34:57
[    1.284000] e1000 0000:00:14.0: eth1: Intel(R) PRO/1000 Network Connection
[    1.288000] PCI: Enabling device 0000:00:15.0 (0000 -> 0003)
[    1.288000] PCI: Setting latency timer of device 0000:00:15.0 to 64
[    1.600000] e1000 0000:00:15.0: eth2: (PCI:33MHz:32-bit) 52:54:00:12:34:58
[    1.600000] e1000 0000:00:15.0: eth2: Intel(R) PRO/1000 Network Connection
[    1.600000] PCI: Enabling device 0000:00:16.0 (0000 -> 0003)
[    1.600000] PCI: Setting latency timer of device 0000:00:16.0 to 64
[    1.924000] e1000 0000:00:16.0: eth3: (PCI:33MHz:32-bit) 52:54:00:12:34:59
[    1.924000] e1000 0000:00:16.0: eth3: Intel(R) PRO/1000 Network Connection
[    1.924000] e1000e: Intel(R) PRO/1000 Network Driver - 1.3.10-k2
[    1.924000] e1000e: Copyright(c) 1999 - 2011 Intel Corporation.
[    1.928000] pcnet32: pcnet32.c:v1.35 21.Apr.2008 tsbogend@alpha.franken.de
[    1.928000] PPP generic driver version 2.4.2
[    1.928000] PPP Deflate Compression module registered
[    1.932000] PPP MPPE Compression module registered
[    1.936000] NET: Registered protocol family 24
[    1.936000] tun: Universal TUN/TAP device driver, 1.6
[    1.936000] tun: (C) 1999-2004 Max Krasnyansky <maxk@qualcomm.com>
[    1.936000] ehci_hcd: USB 2.0 'Enhanced' Host Controller (EHCI) Driver
[    1.936000] ohci_hcd: USB 1.1 'Open' Host Controller (OHCI) Driver
[    1.936000] uhci_hcd: USB Universal Host Controller Interface driver
[    1.936000] PCI: Enabling device 0000:00:0a.2 (0000 -> 0001)
[    1.936000] PCI: Setting latency timer of device 0000:00:0a.2 to 64
[    1.936000] uhci_hcd 0000:00:0a.2: UHCI Host Controller
[    1.940000] uhci_hcd 0000:00:0a.2: new USB bus registered, assigned bus number 1
[    1.940000] uhci_hcd 0000:00:0a.2: irq 11, io base 0x00001400
[    1.948000] hub 1-0:1.0: USB hub found
[    1.948000] hub 1-0:1.0: 2 ports detected
[    1.948000] Initializing USB Mass Storage driver...
[    1.952000] usbcore: registered new interface driver usb-storage
[    1.952000] USB Mass Storage support registered.
[    1.952000] serio: i8042 KBD port at 0x60,0x64 irq 1
[    1.952000] serio: i8042 AUX port at 0x60,0x64 irq 12
[    1.956000] mousedev: PS/2 mouse device common for all mice
[    1.960000] rtc_cmos rtc_cmos: rtc core: registered rtc_cmos as rtc0
[    1.960000] rtc0: alarms up to one day, 242 bytes nvram
[    1.960000] i2c /dev entries driver
[    1.960000] piix4_smbus 0000:00:0a.3: SMBus Host Controller at 0x1100, revision 0
[    1.960000] sdhci: Secure Digital Host Controller Interface driver
[    1.960000] sdhci: Copyright(c) Pierre Ossman
[    1.964000] usbcore: registered new interface driver usbhid
[    1.964000] usbhid: USB HID core driver
[    1.964000] Netfilter messages via NETLINK v0.30.
[    1.964000] nf_conntrack version 0.5.0 (3941 buckets, 15764 max)
[    1.964000] ctnetlink v0.93: registering with nfnetlink.
[    1.964000] IPv4 over IPv4 tunneling driver
[    1.968000] ip_tables: (C) 2000-2006 Netfilter Core Team
[    1.968000] arp_tables: (C) 2002 David S. Miller
[    1.972000] TCP cubic registered
[    1.972000] Initializing XFRM netlink socket
[    1.972000] NET: Registered protocol family 10
[    1.980000] ip6_tables: (C) 2000-2006 Netfilter Core Team
[    1.984000] IPv6 over IPv4 tunneling driver
[    1.988000] NET: Registered protocol family 17
[    1.988000] Bridge firewalling registered
[    1.992000] Ebtables v2.0 registered
[    1.992000] 802.1Q VLAN Support v1.8 Ben Greear <greearb@candelatech.com>
[    1.992000] All bugs added by David S. Miller <davem@redhat.com>
[    1.992000] lib80211: common routines for IEEE802.11 drivers
[    1.992000] lib80211_crypt: registered algorithm 'NULL'
[    2.008000] rtc_cmos rtc_cmos: setting system clock to 2023-11-02 02:49:28 UTC (1698893368)
[    2.060000] input: AT Raw Set 2 keyboard as /devices/platform/i8042/serio0/input/input0
[    2.264000] input: ImExPS/2 Generic Explorer Mouse as /devices/platform/i8042/serio1/input/input1
[    2.280000] EXT2-fs (sda1): warning: mounting unchecked fs, running e2fsck is recommended
[    2.288000] VFS: Mounted root (ext2 filesystem) on device 8:1.
[    2.288000] Freeing prom memory: 956k freed
[    2.328000] Freeing unused kernel memory: 240k freed
[    2.404000] firmadyne: sys_reboot[PID: 53 (init)]: magic1:fee1dead, magic2:28121969, cmd:0
[    2.468000] firmadyne: do_execve: /firmadyne/console
[    2.472000] OFFSETS: offset of pid: 0xc4 offset of comm: 0x1a4

Mounting etc to ramfs.      [DONE]

Mounting var to jffs2.      [FAILED]

Checking SSH keys.          [DONE]

Checking for run file.      [DONE]

Starting System Logger.     [DONE]

Starting Kernel Logger.     [DONE]
[    6.360000] klogd/108: potentially unexpected fatal signal 10.
[    6.360000]
[    6.360000] Cpu 0
[    6.360000] $ 0   : 00000000 1000a400 00000008 ffffffff
[    6.360000] $ 4   : 00000000 00000000 00000000 7fee5e20
[    6.360000] $ 8   : 00000000 00000000 00000000 7fee5c48
[    6.360000] $12   : 2b68d868 2b6a0004 92492493 00000046
[    6.360000] $16   : 7fee5d88 ffffffff 7fee6498 7fee6498
[    6.360000] $20   : 7fee643b 2b6a0c40 7fee5e80 00000000
[    6.360000] $24   : 00000000 2b676bc0
[    6.360000] $28   : 2b6a8440 7fee5c98 ffffffff 2b6735c8
[    6.360000] Hi    : 00000001
[    6.360000] Lo    : 00000000
[    6.372000] epc   : 2b673648 0x2b673648
[    6.372000]     Not tainted
[    6.372000] ra    : 2b6735c8 0x2b6735c8
[    6.372000] Status: 0000a413    USER EXL IE
[    6.376000] Cause : 10800010
[    6.376000] BadVA : ffffffff
[    6.380000] PrId  : 00019300 (MIPS 24Kc)

Starting Panel LED.         [DONE]

Starting watchdog.          Error in opening the device.
: No such device
[DONE]

Starting Reset Detect.      Error in opening the device
: No such device
[DONE]
WN802T_SYS_RESET_DETECT_IOC returned err

Checking Manufac. data      [DEFAULT]
Erase Total 1 Units
Performing Flash Erase of length 16384 at offset 0x0 done
[    8.676000] nand_do_write_ops: Attempt to write not page aligned data
Error Writing device /dev/mtd5.

Checking board file.        [CREATED]

Loading Ethernet module.    [GENMAC]

                            BusyBox v1.11.0 (2011-06-23 15:54:48 IST) multi-call binary

Usage: ifconfig [-a] interface [address]
```

```
Configure a network interface

Options:
        [[-]broadcast [ADDRESS]] [[-]pointopoint [ADDRESS]]
        [netmask ADDRESS] [dstaddr ADDRESS]
        [outfill NN] [keepalive NN]
        [hw ether|infiniband ADDRESS] [metric NN] [mtu NN]
        [[-]trailers] [[-]arp] [[-]allmulti]
        [multicast] [[-]promisc] [txqueuelen NN] [[-]dynamic]
        [mem_start NN] [io_addr NN] [irq NN]
        [up|down] ...

[DONE]

Checking database.          [DONE]

Verifing checksum.          [DONE]

Loading Bridge module.      [DONE]
/etc/init.d/rcS: /etc/init.d/S020bridge.sh: line 39: cannot create /proc/sys/net/bridge/bridge-nf-enabled: nonexistent directory

Loading wlan modules.       [DONE]

Creating vap interface.     /usr/local/bin/wlanconfig: ioctl: No such device
ifconfig: SIOCSIFTXQLEN: No such device
/usr/local/bin/wlanconfig: ioctl: No such device
ifconfig: SIOCSIFTXQLEN: No such device
/usr/local/bin/wlanconfig: ioctl: No such device
ifconfig: SIOCSIFTXQLEN: No such device
/usr/local/bin/wlanconfig: ioctl: No such device
ifconfig: SIOCSIFTXQLEN: No such device
/usr/local/bin/wlanconfig: ioctl: No such device
ifconfig: SIOCSIFTXQLEN: No such device
/usr/local/bin/wlanconfig: ioctl: No such device
ifconfig: SIOCSIFTXQLEN: No such device
/usr/local/bin/wlanconfig: ioctl: No such device
ifconfig: SIOCSIFTXQLEN: No such device
/usr/local/bin/wlanconfig: ioctl: No such device
ifconfig: SIOCSIFTXQLEN: No such device
[DONE]

Creating wds interface.     /usr/local/bin/wlanconfig: ioctl: No such device
ifconfig: SIOCSIFMTU: No such device
/usr/local/bin/wlanconfig: ioctl: No such device
ifconfig: SIOCSIFMTU: No such device
/usr/local/bin/wlanconfig: ioctl: No such device
ifconfig: SIOCSIFMTU: No such device
/usr/local/bin/wlanconfig: ioctl: No such device
ifconfig: SIOCSIFMTU: No such device
[DONE]

Starting configd.           [DONE]

Starting web server.        [DONE]

Starting Translator...      start-stop-daemon: cannot start /usr/bin/log_ro: No such file or directory
[syslog]

Starting Translator...      [password]

Starting Translator...      [ssh]

Starting Translator...      [snmp]

Starting Translator...      [telnet]

Starting Translator...      [dns]

Starting Translator...      [   21.908000] ADDRCONF(NETDEV_UP): brtrunk: link is not ready
[   22.072000] device eth0 entered promiscuous mode
[   22.144000] ADDRCONF(NETDEV_UP): eth0: link is not ready
[   22.160000] 8021q: adding VLAN 0 to HW filter on device eth0
[   22.172000] e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: RX
[   22.184000] ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[   22.184000] brtrunk: port 1(eth0) entering forwarding state
[   22.188000] brtrunk: port 1(eth0) entering forwarding state
[   22.192000] ADDRCONF(NETDEV_CHANGE): brtrunk: link becomes ready
set cascaded bridge failed: Operation not supported
```

```
route: SIOCADDRT: Invalid argument
[bridge_and_vlan_translator]

Starting Translator...      [   22.832000] do_page_fault() #2: sending SIGSEGV to hostapd_tr for invalid read access from
[   22.832000] 00000004 (epc == 2b9167d0, ra == 00416804)
[   22.864000] Cpu 0
[   22.864000] $ 0   : 00000000 1000a400 00000004 00000000
[   22.864000] $ 4   : 00000004 00419f18 00000000 00000001
[   22.864000] $ 8   : 2b93f004 006750b8 00000031 fffffff0
[   22.864000] $12   : 8f065eb0 00000234 06ca3695 2b8f3578
[   22.864000] $16   : 7ffcd7c0 7ffcd650 7fe3f354 ffffffff
[   22.864000] $20   : 7ffcd714 00401834 00000001 004019f0
[   22.864000] $24   : 00000002 2b9167d0
[   22.864000] $28   : 00435880 7ffcd0a8 7ffcd0a8 00416804
[   22.864000] Hi    : 00000005
[   22.864000] Lo    : 19999999
[   22.864000] epc   : 2b9167d0 0x2b9167d0
[   22.864000]     Not tainted
[   22.864000] ra    : 00416804 0x416804
[   22.864000] Status: 0000a413    USER EXL IE
[   22.864000] Cause : 10800008
[   22.864000] BadVA : 00000004
[   22.864000] PrId  : 00019300 (MIPS 24Kc)
[   22.864000] Modules linked in:
[   22.864000] Process hostapd_tr (pid: 526, threadinfo=8f064000, task=8f02e078, tls=00000000)
[   22.864000] Stack : 696e6773 3a646863 7073536e 64446e73 00435880 2e302e30 00000000 74656d3a
[   22.864000]         64686370 73536574 7ffcd0d8 00402404 00419f18 0041a030 6e732030 2e302e30
[   22.864000]         00435880 79737465 2f746d70 2f686f73 74617064 2e636f6e 662e7769 6669302e
[   22.864000]         74656d70 00302e30 2e302e30 0a737973 74656d3a 64686370 73536574 74696e67
[   22.864000]         733a6468 6370734c 65617365 54696d65 20383634 30300a0a 73797374 656d3a6c
[   22.864000]         ...
[   22.864000] Call Trace:
[   22.864000]
[   22.864000]
[   22.864000] Code: 00000000  00000000  00000000
[   22.864000]  90a20000  24840001  14600003  24a50001  03e00008
[   22.864000] hostapd_tr/526: potentially unexpected fatal signal 11.
[   22.864000]
[   22.864000] Cpu 0
[   22.864000] $ 0   : 00000000 1000a400 00000004 00000000
[   22.864000] $ 4   : 00000004 00419f18 00000000 00000001
[   22.864000] $ 8   : 2b93f004 006750b8 00000031 fffffff0
[   22.864000] $12   : 8f065eb0 00000234 06ca3695 2b8f3578
[   22.864000] $16   : 7ffcd7c0 7ffcd650 7fe3f354 ffffffff
[   22.864000] $20   : 7ffcd714 00401834 00000001 004019f0
[   22.864000] $24   : 00000002 2b9167d0
[   22.864000] $28   : 00435880 7ffcd0a8 7ffcd0a8 00416804
[   22.864000] Hi    : 00000005
[   22.864000] Lo    : 19999999
[   22.864000] epc   : 2b9167d0 0x2b9167d0
[   22.864000]     Not tainted
[   22.864000] ra    : 00416804 0x416804
[   22.864000] Status: 0000a413    USER EXL IE
[   22.864000] Cause : 10800008
[   22.864000] BadVA : 00000004
[   22.864000] PrId  : 00019300 (MIPS 24Kc)
Segmentation fault
[hostapd_tr]

Starting Translator...      [nmbd_tr]

Starting Translator...      sh: cannot create /proc/sys/net/bridge/bridge-http-redirect-flush-mac: nonexistent directory
sh: cannot create /proc/sys/net/bridge/bridge-http-redirect-enabled: nonexistent directory
[http_redirect_tr]

Starting Translator...      [dhcp]

Starting Translator...      kill: cannot kill pid 601: No such process
[ntp]

Starting Translator...      [timezone]

Starting Translator...      [sc_radio]
kill: cannot kill pid 614: No such process
Error in opening the device.
: No such device

System initilization is ..  [DONE...]
```

```
Welcome to SDK.

Have a lot of fun...

netgear123456 login: [   27.200000] brtrunk: port 1(eth0) entering forwarding state
```

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 192.168.0.100
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 required authentication.

```
┌──(kali㉿kali)-[~/Desktop/Project/firmadyne]
└─$ ./analyses/webAccess.py 1 192.168.0.100 log.txt
Accessing: http://192.168.0.100/include/libs/internals/core.write_file.php...
Accessing: http://192.168.0.100/help/help_AdvancedWirelessSettings_g.html...
Accessing: http://192.168.0.100/include/libs/plugins/modifier.cat.php...
Accessing: http://192.168.0.100/login_button.html...
Accessing: http://192.168.0.100/getBoardConfig.php...
Accessing: http://192.168.0.100/tmpl/UnknownAPList.tpl.php...
Accessing: http://192.168.0.100/help/help_RebootAP.html...
Skipping: images/back_on.gif...
Accessing: http://192.168.0.100/tmpl/BasicTime.tpl.php...
Accessing: http://192.168.0.100/login.php...
Skipping: images/body_right_next_notch.gif...
Accessing: http://192.168.0.100/tmpl/siteSurvey.tpl.php...
Accessing: http://192.168.0.100/tmpl/DHCPServerSettings.tpl.php...
Skipping: images/tab_l_A.png...
Accessing: http://192.168.0.100/tmpl/Snooping.tpl.php...
Accessing: http://192.168.0.100/boardDataNA.php...
Accessing: http://192.168.0.100/help/help_BridgingandRepeating.html...
Accessing: http://192.168.0.100/include/libs/internals/core.write_compiled_include.php...
Accessing: http://192.168.0.100/tmpl/Login.tpl.php...
-> Redirect
Skipping: images/tip.gif...
Skipping: images/sub_section_side_dots_wide.gif...
Skipping: templates/sample_datablock.tpl...
Skipping: images/cancel_on.gif...
Accessing: http://192.168.0.100/include/libs/plugins/function.fetch.php...
Accessing: http://192.168.0.100/include/libs/plugins/shared.make_timestamp.php...
Accessing: http://192.168.0.100/include/libs/plugins/function.mailto.php...
Skipping: images/save_as_on.gif...
Skipping: images/inline_tab_r.png...
Accessing: http://192.168.0.100/help/help_PacketCapture.html...
Skipping: templates/SNMP.tpl...
Skipping: images/reset_on.gif...
Skipping: templates/RebootAP.tpl...
Accessing: http://192.168.0.100/tmpl/thirdMenu.tpl.php...
Skipping: images/footer_bottom_right.gif...
Skipping: images/backup_off.gif...
Skipping: images/refresh_off.gif...
Accessing: http://192.168.0.100/tmpl/vapSecurityProfile.tpl.php...
Accessing: http://192.168.0.100/include/libs/plugins/modifier.string_format.php...
Skipping: images/left_nav_right_tile.gif...
Accessing: http://192.168.0.100/tmpl/BasicGeneral.tpl.php...
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://192.168.0.100/include/libs/internals/core.run_insert_handler.php...
Accessing: http://192.168.0.100/include/libs/internals/core.get_include_path.php...
Skipping: templates/wdsSecurityProfile.tpl...
Accessing: http://192.168.0.100/help/help_BackupSettings.html...
Skipping: images/footer_bottom_left.gif...
Accessing: http://192.168.0.100/tmpl/AddWPSClient.tpl.php...
Skipping: images/logout_button.gif...
Accessing: http://192.168.0.100/help/help_BasicTime.html...
Skipping: images/left_nav_bottom_middle.gif...
Accessing: http://192.168.0.100/include/libs/plugins/modifier.capitalize.php...
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://192.168.0.100/help/help_WirelessStations.html...
Skipping: images/sub_section_bottom_dots.gif...
Accessing: http://192.168.0.100/include/libs/plugins/modifier.strip.php...
Accessing: http://192.168.0.100/include/libs/plugins/modifier.lower.php...
Skipping: templates/help.tpl...
Skipping: images/tab_r.png...
Accessing: http://192.168.0.100/tmpl/IPSettings.tpl.php...
Accessing: http://192.168.0.100/include/libs/plugins/modifier.strip_tags.php...
```

```
Accessing: http://192.168.0.100/include/libs/Smarty.class.php...
Skipping: templates/Logs.tpl...
Skipping: templates/AdvancedWirelessSettings.tpl...
Accessing: http://192.168.0.100/include/libs/internals/core.process_cached_inserts.php...
Skipping: include/scripts/menu.js...
Skipping: templates/AdvancedHotspot.tpl...
Accessing: http://192.168.0.100/boardDataWW.php...
Skipping: images/details_on.gif...
Accessing: http://192.168.0.100/include/libs/internals/core.is_trusted.php...
Skipping: images/datahead_right.png...
Accessing: http://192.168.0.100/tmpl/BasicQoSSettings.tpl.php...
Accessing: http://192.168.0.100/getJsonData.php...
Skipping: templates/Bridging.tpl...
Accessing: http://192.168.0.100/saveTable.php...
Skipping: images/pushButton_Off.gif...
Accessing: http://192.168.0.100/include/libs/plugins/outputfilter.trimwhitespace.php...
Accessing: http://192.168.0.100/tmpl/BasicWirelessSettings.tpl.php...
Skipping: images/back_off.gif...
Accessing: http://192.168.0.100/help/help_SNMP.html...
Skipping: templates/404.tpl...
Accessing: http://192.168.0.100/common.php...
Skipping: templates/BasicWirelessSettings.tpl...
Skipping: include/css/style.css...
Accessing: http://192.168.0.100/tmpl/WPSSettings.tpl.php...
Skipping: templates/bandStrip.tpl...
Accessing: http://192.168.0.100/tmpl/WirelessStations.tpl.php...
Skipping: templates/Login.tpl...
Accessing: http://192.168.0.100/help/help_BasicGeneral.html...
Accessing: http://192.168.0.100/tmpl/AdvancedHotspot.tpl.php...
Skipping: images/alert.gif...
Skipping: templates/UnknownAPList.tpl...
Accessing: http://192.168.0.100/include/libs/internals/core.get_php_resource.php...
Accessing: http://192.168.0.100/include/libs/plugins/function.html_select_date.php...
Accessing: http://192.168.0.100/tmpl/ProfileSettings.tpl.php...
Accessing: http://192.168.0.100/help/help_BasicWirelessSettings_g.html...
Accessing: http://192.168.0.100/help/help_RestoreSettings.html...
Skipping: templates/main.tpl...
Skipping: images/tab_l.png...
Skipping: images/reset_disabled.gif...
Accessing: http://192.168.0.100/include/libs/Smarty_Compiler.class.php...
Skipping: images/left_nav_top_middle.gif...
Accessing: http://192.168.0.100/include/libs/plugins/function.input_row.php...
Accessing: http://192.168.0.100/tmpl/master.tpl.php...
Skipping: images/sub_section_grey_tab_top_le.gif...
Accessing: http://192.168.0.100/tmpl/button.tpl.php...
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://192.168.0.100/help/help_UnknownAPList.html...
Skipping: images/pushButton_On.gif...
Accessing: http://192.168.0.100/include/libs/plugins/function.html_radios.php...
Accessing: http://192.168.0.100/tmpl/KnownAPList.tpl.php...
Accessing: http://192.168.0.100/include/libs/internals/core.get_microtime.php...
Accessing: http://192.168.0.100/include/libs/plugins/modifier.regex_replace.php...
Skipping: images/close_help.gif...
Accessing: http://192.168.0.100/tmpl/AdvancedMACAuthentication.tpl.php...
Accessing: http://192.168.0.100/help/help_DHCPServerSettings.html...
Skipping: images/refresh_on.gif...
Accessing: http://192.168.0.100/include/libs/internals/core.load_plugins.php...
Skipping: images/add_new_stat_off.gif...
Accessing: http://192.168.0.100/tmpl/wdsSecurityProfile.tpl.php...
Accessing: http://192.168.0.100/include/libs/internals/core.assemble_plugin_filepath.php...
Accessing: http://192.168.0.100/login_header.php...
Accessing: http://192.168.0.100/help/help_AdvancedGeneral.html...
Skipping: templates/Statistics.tpl...
Skipping: templates/FirmwareUpgradeTFTP.tpl...
Accessing: http://192.168.0.100/tmpl/AdvancedEthernet.tpl.php...
Skipping: images/edit_on.gif...
Accessing: http://192.168.0.100/tmpl/data.tpl.php...
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://192.168.0.100/include/libs/internals/core.write_compiled_resource.php...
Skipping: images/details_off.gif...
```

```
Accessing: http://192.168.0.100/tmpl/System.tpl.php...
Skipping: templates/header.tpl...
Accessing: http://192.168.0.100/tmpl/PacketCapture.tpl.php...
Accessing: http://192.168.0.100/help/help_AdvancedHotspot.html...
Accessing: http://192.168.0.100/logout.html...
Accessing: http://192.168.0.100/logout.php...
Accessing: http://192.168.0.100/body.php...
Skipping: templates/System.tpl...
Accessing: http://192.168.0.100/recreate.php...
Skipping: images/footer_copyright_new.gif...
Accessing: http://192.168.0.100/include/libs/plugins/function.eval.php...
Accessing: http://192.168.0.100/tmpl/FirmwareUpgrade.tpl.php...
Skipping: templates/ChangePassword.tpl...
Accessing: http://192.168.0.100/include/libs/plugins/modifier.wordwrap.php...
Accessing: http://192.168.0.100/help/help_AdvancedWirelessSettings_a.html...
Skipping: include/scripts/browser-ext.js...
Skipping: templates/siteSurvey.tpl...
Skipping: images/body_right_notch.gif...
Accessing: http://192.168.0.100/redirect.html...
Skipping: images/product_logo.gif...
Accessing: http://192.168.0.100/help/help_AdvancedWirelessSettings.html...
Accessing: http://192.168.0.100/include/libs/internals/core.smarty_include_php.php...
Skipping: images/body_middile_notch.gif...
Accessing: http://192.168.0.100/tmpl/AdvancedWirelessSettings.tpl.php...
Skipping: images/footer_right_copyright.gif...
Skipping: templates/background.tpl...
Skipping: images/button.png...
Accessing: http://192.168.0.100/tmpl/ChangePassword.tpl.php...
Accessing: http://192.168.0.100/include/libs/plugins/function.data_header.php...
Skipping: templates/TR069.tpl...
Accessing: http://192.168.0.100/config.php...
Accessing: http://192.168.0.100/help/help_ChangePassword.html...
Accessing: http://192.168.0.100/include/libs/Config_File.class.php...
Accessing: http://192.168.0.100/help/help.html...
Accessing: http://192.168.0.100/include/libs/plugins/modifier.truncate.php...
Accessing: http://192.168.0.100/killall.php...
-> Socket Timeout: timed out
Accessing: http://192.168.0.100/include/libs/plugins/shared.escape_special_chars.php...
Skipping: templates/BasicQoSSettings.tpl...
Accessing: http://192.168.0.100/include/libs/plugins/function.sortable_header_row.php...
Skipping: images/Thumbs.db...
Skipping: templates/BasicScheduledWirelessON-OFF.tpl...
Skipping: templates/master.tpl...
Accessing: http://192.168.0.100/button.html...
Accessing: http://192.168.0.100/tmpl/RestoreDefaults.tpl.php...
Accessing: http://192.168.0.100/help/help_AdvancedMACAuthentication.html...
Accessing: http://192.168.0.100/tmpl/Bridging.tpl.php...
Accessing: http://192.168.0.100/tmpl/SNMP.tpl.php...
Accessing: http://192.168.0.100/help/help_BasicProfileSettings.html...
Accessing: http://192.168.0.100/include/libs/plugins/modifier.indent.php...
Skipping: include/scripts/TableSort.js...
Accessing: http://192.168.0.100/include/libs/plugins/function.popup_init.php...
Accessing: http://192.168.0.100/include/libs/plugins/modifier.debug_print_var.php...
Accessing: http://192.168.0.100/UserGuide.html...
Skipping: images/backup_on.gif...
Skipping: images/main_logo.gif...
Accessing: http://192.168.0.100/include/libs/plugins/modifier.count_paragraphs.php...
Accessing: http://192.168.0.100/include/libs/plugins/modifier.default.php...
Skipping: images/loading.gif...
Skipping: images/clear_on.gif...
Accessing: http://192.168.0.100/tmpl/RebootAP.tpl.php...
Accessing: http://192.168.0.100/include/libs/plugins/function.html_select_time.php...
Accessing: http://192.168.0.100/help/help_Logs.html...
Skipping: images/sub_section_grey_tab_top_right.gif...
Accessing: http://192.168.0.100/help/help_BasicIPSettings.html...
Accessing: http://192.168.0.100/include/libs/internals/core.process_compiled_include.php...
Accessing: http://192.168.0.100/include/libs/plugins/function.cycle.php...
Skipping: include/scripts/validation.js...
Skipping: templates/titleLogo.tpl...
Accessing: http://192.168.0.100/checkSession.php...
Accessing: http://192.168.0.100/include/libs/internals/core.load_resource_plugin.php...
Skipping: templates/BackupSettings.tpl...
Skipping: images/tab_l_A.gif...
Skipping: templates/AdvancedRogueAP.tpl...
Accessing: http://192.168.0.100/tmpl/BackupSettings.tpl.php...
Accessing: http://192.168.0.100/include/libs/plugins/function.debug.php...
Skipping: images/login_off.gif...
Skipping: templates/progress.tpl...
```

```
Accessing: http://192.168.0.100/background.html...
Skipping: templates/AdvancedRadiusServerSettings.tpl...
Skipping: images/left_nav_bottom_left.gif...
Accessing: http://192.168.0.100/tmpl/BasicClientSettings.tpl.php...
Accessing: http://192.168.0.100/downloadFile.php...
Accessing: http://192.168.0.100/help/help_System.html...
Skipping: include/scripts/common.js...
Accessing: http://192.168.0.100/tmpl/404.tpl.php...
Skipping: images/move_on.gif...
Accessing: http://192.168.0.100/tmpl/FirmwareUpgradeTFTP.tpl.php...
Skipping: images/footer_left_bottom.gif...
Skipping: templates/BasicTime.tpl...
Skipping: templates/WirelessStations.tpl...
Skipping: images/inactive.png...
Accessing: http://192.168.0.100/clearLog.php...
Accessing: http://192.168.0.100/include/libs/internals/core.assign_smarty_interface.php...
Accessing: http://192.168.0.100/help/help_BasicQoSSettings.html...
Skipping: templates/Snooping.tpl...
Skipping: images/body_left_notch.gif...
Accessing: http://192.168.0.100/include/libs/plugins/function.generate_input_fields.php...
Accessing: http://192.168.0.100/include/libs/plugins/function.math.php...
Skipping: images/arrow_right.gif...
Skipping: images/add_new_stat_on.gif...
Skipping: images/down_arrow.gif...
Accessing: http://192.168.0.100/include/libs/plugins/function.ip_field.php...
Accessing: http://192.168.0.100/include/libs/plugins/function.html_checkboxes.php...
Skipping: images/reset_off.pdn...
Skipping: templates/AdvancedGeneral.tpl...
Skipping: images/background_right.gif...
Skipping: templates/AddWPSClient.tpl...
Accessing: http://192.168.0.100/help/help_BasicWirelessSettings_a.html...
Skipping: images/datahead_left.png...
Skipping: templates/AdvancedQoSSettings.tpl...
Skipping: templates/FirmwareUpgrade.tpl...
Accessing: http://192.168.0.100/include/libs/internals/core.write_cache_file.php...
Accessing: http://192.168.0.100/include/libs/plugins/modifier.upper.php...
Accessing: http://192.168.0.100/help/help_ProfileSettings.html...
Skipping: include/scripts/control-modal.js...
Skipping: include/scripts/livevalidation.js...
Accessing: http://192.168.0.100/help/help_IPSettings.html...
Skipping: templates/footer.tpl...
Accessing: http://192.168.0.100/help/help_AdvancedRogueAP.html...
Skipping: templates/AdvancedMACAuthentication.tpl...
Accessing: http://192.168.0.100/include/libs/plugins/function.html_options.php...
Skipping: include/css/csshover.htc...
Skipping: images/background_left.gif...
Skipping: images/datahead_left.gif...
Accessing: http://192.168.0.100/tmpl/AdvancedSyslog.tpl.php...
Accessing: http://192.168.0.100/help/help_vapSecurityProfile.html...
Accessing: http://192.168.0.100/include/libs/plugins/modifier.nl2br.php...
Accessing: http://192.168.0.100/help/help_FirmwareUpgradeTFTP.html...
Accessing: http://192.168.0.100/help/help_RestoreDefaults.html...
Accessing: http://192.168.0.100/include/libs/internals/core.read_cache_file.php...
Skipping: templates/BasicGeneral.tpl...
Accessing: http://192.168.0.100/packetCapture.php...
Skipping: templates/RestoreDefaults.tpl...
Accessing: http://192.168.0.100/tmpl/Documentation.tpl.php...
Accessing: http://192.168.0.100/include/libs/internals/core.is_secure.php...
Accessing: http://192.168.0.100/include/libs/internals/core.rmdir.php...
Accessing: http://192.168.0.100/include/libs/plugins/modifier.date_format.php...
Accessing: http://192.168.0.100/tmpl/TR069.tpl.php...
Accessing: http://192.168.0.100/tmpl/bandStrip.tpl.php...
Accessing: http://192.168.0.100/help/help_RogueAPList.html...
Accessing: http://192.168.0.100/include/libs/plugins/compiler.assign.php...
Accessing: http://192.168.0.100/include/libs/internals/core.create_dir_structure.php...
Accessing: http://192.168.0.100/help/help_Bridging.html...
Accessing: http://192.168.0.100/tmpl/main.tpl.php...
Skipping: images/left_nav_top_left.gif...
Skipping: images/buttons.png...
Skipping: images/body_notch.gif...
Accessing: http://192.168.0.100/index.php...
Accessing: http://192.168.0.100/include/libs/plugins/function.html_table.php...
Accessing: http://192.168.0.100/include/libs/plugins/function.popup.php...
Skipping: images/left_nav_bottom_right.gif...
Skipping: images/apply_disabled.gif...
Skipping: images/tab_separator.gif...
Accessing: http://192.168.0.100/help/help_wdsSecurityProfile.html...
Skipping: images/footer_middle_top_divider.gif...
```

```
Skipping: templates/vapSecurityProfile.tpl...
Skipping: templates/DHCPServerSettings.tpl...
Accessing: http://192.168.0.100/header.php...
Skipping: images/go_on.gif...
Skipping: include/scripts/prototype.js...
Skipping: templates/RestoreSettings.tpl...
Accessing: http://192.168.0.100/tmpl/BasicScheduledWirelessON-OFF.tpl.php...
Skipping: include/css/layout.css...
Accessing: http://192.168.0.100/include/libs/plugins/function.config_load.php...
Skipping: images/background_inside_left.gif...
Skipping: templates/WPSSettings.tpl...
Accessing: http://192.168.0.100/BackupConfig.php...
Accessing: http://192.168.0.100/tmpl/AdvancedRogueAP.tpl.php...
Accessing: http://192.168.0.100/help/help_AdvancedSyslog.html...
Skipping: templates/KnownAPList.tpl...
Accessing: http://192.168.0.100/tmpl/Statistics.tpl.php...
Accessing: http://192.168.0.100/tmpl/RestoreSettings.tpl.php...
Skipping: images/tab.png...
Skipping: templates/PacketCapture.tpl...
Skipping: images/apply_on.gif...
Accessing: http://192.168.0.100/thirdMenu.php...
Accessing: http://192.168.0.100/tmpl/help.tpl.php...
Accessing: http://192.168.0.100/include/libs/plugins/function.assign_debug_info.php...
Skipping: templates/body.tpl...
Skipping: include/css/fonts.css...
Skipping: images/inline_tab_l.png...
Accessing: http://192.168.0.100/siteSurvey.php...
-> Redirect
Skipping: monitorFile.cfg...
Accessing: http://192.168.0.100/help/help_BasicScheduledWirelessON-OFF.html...
Skipping: images/delete_on.gif...
Skipping: images/sub_section_grey_tab_top_ri.gif...
Accessing: http://192.168.0.100/include/libs/plugins/modifier.replace.php...
Skipping: include/css/default.css...
Accessing: http://192.168.0.100/data.php...
Skipping: images/add_off.gif...
Accessing: http://192.168.0.100/help/help_KnownAPList.html...
Accessing: http://192.168.0.100/thirdMenu.html...
Accessing: http://192.168.0.100/include/libs/plugins/modifier.count_characters.php...
Skipping: images/cancel_off.gif...
Skipping: templates/RemoteConsole.tpl...
Accessing: http://192.168.0.100/include/libs/plugins/modifier.spacify.php...
Skipping: images/clear.gif...
Accessing: http://192.168.0.100/tmpl/AdvancedRadiusServerSettings.tpl.php...
Skipping: images/apply_off.gif...
Skipping: images/tab_r_A.png...
Accessing: http://192.168.0.100/tmpl/progress.tpl.php...
Accessing: http://192.168.0.100/help/help_RemoteConsole.html...
Accessing: http://192.168.0.100/include/libs/plugins/function.html_image.php...
Accessing: http://192.168.0.100/include/libs/plugins/modifier.count_sentences.php...
Skipping: templates/button.tpl...
Skipping: templates/IPSettings.tpl...
Accessing: http://192.168.0.100/redirect.php...
-> Redirect
Accessing: http://192.168.0.100/tmpl/AdvancedGeneral.tpl.php...
Skipping: images/left_nav_left_tile.gif...
Skipping: include/scripts/effects.js...
Accessing: http://192.168.0.100/help/help_FirmwareUpgrade.html...
Accessing: http://192.168.0.100/tmpl/AdvancedQoSSettings.tpl.php...
Skipping: include/libs/debug.tpl...
Skipping: images/footer_left_copyright.gif...
Accessing: http://192.168.0.100/tmpl/header.tpl.php...
Accessing: http://192.168.0.100/help/help_ConfigManagement.html...
Accessing: http://192.168.0.100/include/libs/plugins/block.textformat.php...
Accessing: http://192.168.0.100/test.php...
Accessing: http://192.168.0.100/checkConfig.php...
-> Redirect
Accessing: http://192.168.0.100/help/help_Login.html...
Skipping: images/sidebox.gif...
Accessing: http://192.168.0.100/tmpl/Logs.tpl.php...
Accessing: http://192.168.0.100/tmpl/RemoteConsole.tpl.php...
Skipping: templates/Documentation.tpl...
Accessing: http://192.168.0.100/help/help_Statistics.html...
Accessing: http://192.168.0.100/include/libs/plugins/function.counter.php...
Skipping: images/datahead_right.gif...
Accessing: http://192.168.0.100/include/libs/internals/core.display_debug_console.php...
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://192.168.0.100/help/help_AdvancedRadiusServerSettings.html...
Skipping: images/save_on.gif...
Skipping: include/scripts/prototype-ext.js...
Accessing: http://192.168.0.100/include/libs/plugins/modifier.escape.php...
Skipping: images/move_off.gif...
Skipping: images/reset_off.gif...
Skipping: images/sub_section_grey_tab_shadow.gif...
Accessing: http://192.168.0.100/titleLogo.php...
Accessing: http://192.168.0.100/include/libs/plugins/modifier.count_words.php...
Skipping: images/up_arrow.gif...
Accessing: http://192.168.0.100/help/help_AdvancedQoSSettings.html...
Accessing: http://192.168.0.100/include/libs/internals/core.rm_auto.php...
Skipping: images/sub_section_grey_tab_top_left.gif...
Skipping: include/scripts/wirelessnew.js...

┌──(kali㉿kali)-[~/Desktop/Project/firmadyne]
└─$ less log.txt
```

Port Scan

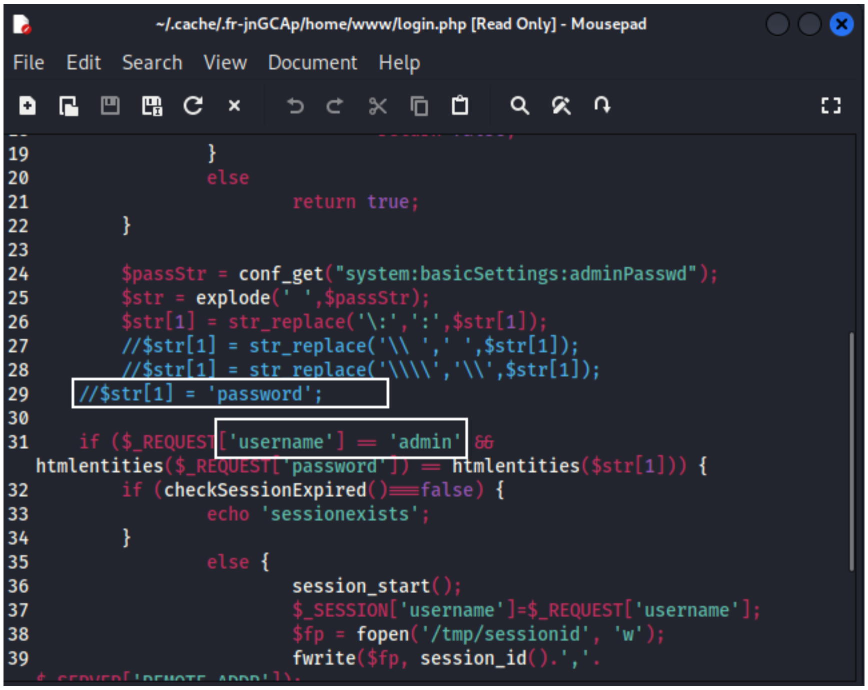
```
┌──(kali㉿kali)-[~/Desktop/Project/firmadyne]
└─$ sudo nmap -O -sV 192.168.0.100
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-01 23:11 EDT
Nmap scan report for 192.168.0.100
Host is up (0.00090s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      Dropbear sshd 0.51 (protocol 2.0)
80/tcp  open  http     lighttpd 1.4.18
443/tcp open  ssl/http lighttpd 1.4.18
MAC Address: 52:54:00:12:34:56 (QEMU virtual NIC)
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: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 18.55 seconds
```

Exploit

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

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

┌──(kali㉿kali)-[~/Desktop/Project/firmadyne]
└─$ less exploits/exploit.metasploit.log
exploits/exploit.metasploit.log: No such file or directory

┌──(kali㉿kali)-[~/Desktop/Project/firmadyne]
└─$ python ./analyses/runExploits.py -t 192.168.0.100 -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...
```

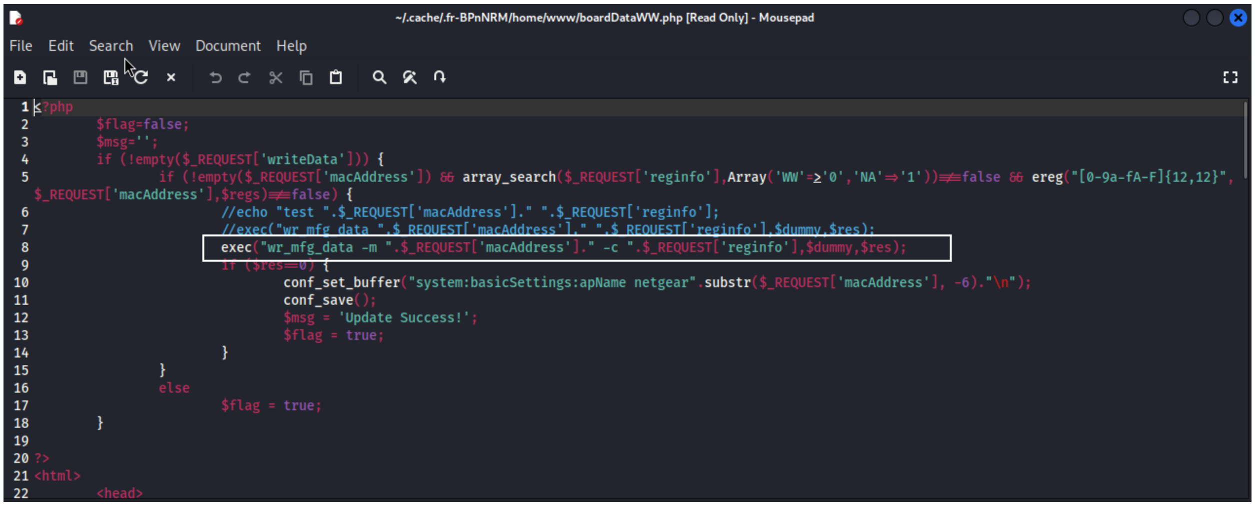
- The file login.php reveals the username and password



~/.cache/.fr-jnGCAp/home/www/login.php [Read Only] - Mousepad
File Edit Search View Document Help

```
                }
                else
                        return true;
        }

        $passStr = conf_get("system:basicSettings:adminPasswd");
        $str = explode(' ',$passStr);
        $str[1] = str_replace('\:',':',$str[1]);
        //$str[1] = str_replace('\\ ',' ',$str[1]);
        //$str[1] = str_replace('\\\\','\\',$str[1]);
    //$str[1] = 'password';

    if ($_REQUEST['username'] == 'admin' &&
htmlentities($_REQUEST['password']) == htmlentities($str[1])) {
        if (checkSessionExpired()===false) {
                echo 'sessionexists';
        }
                else {
                        session_start();
                        $_SESSION['username']=$_REQUEST['username'];
                        $fp = fopen('/tmp/sessionid', 'w');
                        fwrite($fp, session_id().','.
$_SERVER['REMOTE_ADDR']);
```

- The file boardDataWW.php reveals use of `exec()` to execute system commands based on values from request parameters 'macAddress' and 'reginfo'. Attackers can exploit this by injecting a payload like `'<macaddress>; <system command> #'` into the 'macAddress' parameter. This would allow them to execute arbitrary system commands.



~/.cache/.fr-BPnNRM/home/www/boardDataWW.php [Read Only] - Mousepad
File Edit Search View Document Help

```
<?php
        $flag=false;
        $msg='';
        if (!empty($_REQUEST['writeData'])) {
                if (!empty($_REQUEST['macAddress']) && array_search($_REQUEST['reginfo'],Array('WW'=>'0','NA'=>'1'))!==false && ereg("[0-9a-fA-F]{12,12}",
$_REQUEST['macAddress'],$regs)!==false) {
                        //echo "test ".$_REQUEST['macAddress']." ".$_REQUEST['reginfo'];
                        //exec("wr_mfg_data ".$_REQUEST['macAddress']." ".$_REQUEST['reginfo'],$dummy,$res);
                        exec("wr_mfg_data -m ".$_REQUEST['macAddress']." -c ".$_REQUEST['reginfo'],$dummy,$res);
                        if ($res==0) {
                                conf_set_buffer("system:basicSettings:apName netgear".substr($_REQUEST['macAddress'], -6)."\n");
                                conf_save();
                                $msg = 'Update Success!';
                                $flag = true;
                        }
                }
                else
                        $flag = true;
        }

?>
<html>
        <head>
```