

ECE 531: INTRODUCTION TO INTERNET OF THINGS

HOMEWORK #1: BINARY FILE ANALYSIS

JOSEPH HILLAND – 101104172 –
JHILLAND@UNM.EDU

SUMMER 2022

Contents

| | | |
|---|-----------------|---|
| 1 | List of Figures | 1 |
| 2 | Abstract | 2 |
| 3 | Binwalk | 2 |
| 4 | Analyzing Tools | 3 |
| 5 | Conclusion | 5 |

List of Figures

| | | |
|---|-------------------------------------|---|
| 1 | Binwalk Command Output | 3 |
| 2 | JFFS2 Filesystem Contents | 3 |
| 3 | Bin Directory Contents | 3 |
| 4 | Strings on passwd | 4 |
| 5 | Qemu Commands | 4 |
| 6 | Radare2 Commands | 5 |
| 7 | Config Directory Contents | 5 |

2 Abstract

The purpose of this assignment is to understand the contents of firmware binary files as well as test the knowledge and setup of tools within the Linux host environment that has been created. These tools include but are not limited to binwalk, binutils, radare and qemu. Three files were utilized during this assignment which included:

- NC220_1.1.12_Build.160321_Rel.27531.bin (Version A)
- NC220_1.1.12_Build.160321_Rel_upgrade.27531.bin (Version B)
- NC220_1.2.0_Build.170516_Rel.B4AC0D_2017-05-16..00.32.bin (Version 2)

3 Binwalk

Binwalk is a tool for searching and identifying files and code embedded within binary files, specifically within firmware images.

To begin, binwalk was used to analyze the Version A, Version B and Version 2 binary files.

```
$ binwalk -e -C 1.1.12a -M NC220_1.1.12_Build.160321_Rel.27531.bin
$ binwalk -e -C 1.1.12a -M NC220_1.1.12_Build.160321_Rel_upgrade.27531.bin
$ binwalk -e -C 1.1.12a -M \
NC220_1.2.0_Build.170516_Rel.B4AC0D_2017-05-16..00.32.bin
```

The figure from the binwalk output below shows that the firmware images were running MIPS architecture. The firmware images also use JFFS2 filesystem. JFFS2 is a filesystem designed for use on flash drives in embedded systems.

There is a U-Boot version and date listed as well as the Linux kernel version. These components could be further investigated as needed to identify any risks or vulnerabilities within the system.

By changing directories into the jffs2-root directory, other directories can be seen that contain different information about the firmware images.

By investigating the bin/ directory, there are several commands that can be seen which are utilized within this firmware image.

There are several other directories including lib, etc and www. These directories appear to contain a web interface, password files, certificates and libraries used. Further investigation can be done on these files and commands to broaden the understanding of their uses in this firmware image.

When analyzing the version 2 image, there were some extra files and commands found. One of those commands used in the bin directory was logCtrl.

```

jhilland@jhilland:~/git/ECE531/module2/homework1$ binwalk -e -c 1.1.12a -M NC220_1.1.12_Build_160321_Rel.27531.bin
Scan Time:      2022-06-19 10:54:01
Target File:    /home/jhilland/git/ECE531/module2/homework1/NC220_1.1.12_Build_160321_Rel.27531.bin
MD5 Checksum:  ea0d697e7df85bee05e884e9440b0912
Signatures:     411

DECIMAL      HEXADECIMAL    DESCRIPTION
-----
104448      0x19800      U-Boot version string, "U-Boot 1.1.3 (Sep 15 2015 - 07:58:17)"
106096      0x19E70      xz compressed data
127264      0x1F120      UImage header, header size: 64 bytes, header CRC: 0xBE9A003B, created: 2016-03-18 02:51:02, image size: 1867301 bytes
a CRC: 0x10189852, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "Linux Kernel Image"
127328      0x1F160      LZMA compressed data, properties: 0x5D, dictionary size: 33554432 bytes, uncompressed size: 4816188 bytes
1994629     0x1E6F85     JFFS2 filesystem, little endian

Scan Time:      2022-06-19 10:54:03
Target File:    /home/jhilland/git/ECE531/module2/homework1/1.1.12a/NC220_1.1.12_Build_160321_Rel.27531.bin.extracted/1F160
MD5 Checksum:  42e4a8277f6aa022d258d0a1e2b522de
Signatures:     411

DECIMAL      HEXADECIMAL    DESCRIPTION
-----
1573092     0x180BE4      MySQL ISAM index file Version 8
1309644     0x32804C      Linux kernel version 2.6.36
3309760     0x3280C0      CRC32 polynomial table, little endian
3579008     0x369C80      DES SP1, little endian
3579520     0x369E80      DES SP2, little endian
3593488     0x36D510      CRC32 polynomial table, little endian
3924972     0x3BE3EC      xz compressed data
3944560     0x3C3084      Unix path: /var/run/udhcpd.pid
4001272     0x3000FF      Neighborly text, "neighbor %2x%2x.%m lostrouter"
4213721     0x404B09      Intel x86 or x64 microcode, sig 0x0000003f, pf_mask 0x30000000, 1E00-04-04, rev 0x30000000, size 63
4415488     0x436000      LZMA compressed data, properties: 0x5D, dictionary size: 1048576 bytes, uncompressed size: 1475584 bytes

Scan Time:      2022-06-19 10:54:04
Target File:    /home/jhilland/git/ECE531/module2/homework1/1.1.12a/NC220_1.1.12_Build_160321_Rel.27531.bin.extracted/_1F160.extracted/436000
MD5 Checksum:  de34db1e53708f9e05188b18c36b5c3c
Signatures:     411

```

Figure 1: Binwalk Command Output

```

jhilland@jhilland:~/git/ECE531/module2/homework1/.extracted/jffs2-root$ ls
bin  config  etc  lib  sbin  share  www
jhilland@jhilland:~/git/ECE531/module2/homework1/.extracted/jffs2-root$

```

Figure 2: JFFS2 Filesystem Contents

```

jhilland@jhilland:~/git/ECE531/module2/homework1/1.1.12b/NC220_1.1.12_Build_160321_Rel.27531_upgrade.extracted/jffs2-root$ ls bin/
filecut  img_built  pppd  rinetd  ssmtp  tp_mp_server  watch_adalarm.sh  watch_lighttpd.sh  wput
jhilland@jhilland:~/git/ECE531/module2/homework1/1.1.12b/NC220_1.1.12_Build_160321_Rel.27531_upgrade.extracted/jffs2-root$

```

Figure 3: Bin Directory Contents

4 Analyzing Tools

Tools used for further analysis included but were not limited to:

- qemu-mips-static - QEMU emulator static version
- binutils - collection of binary tools

Some of the binutil commands used during analysis are listed below. Many of the commands and files in these images were not able to be analyzed by readelf or objdump tools. However the strings command worked well in searching the files. A lot of the files within the config directory were viewable in plain text. These configuration files may contain important information pertaining to how the system is configured. Radare2 was also installed which comes with other tools for analyzing binary elements.

- `grep -iRn 'SEARCH_TEXT'`
- `strings -n 10 'filename'`
- `mips-linux-gnu-readelf -d COMMAND`
- `sudo chroot . ./qemu-mips-static COMMAND -option`
- `rabin2 -I file`

```
jhilland@jhilland:~/git/ECE531/module2/homework1/1.1.12a/_NC220_1.1.12_Build_160321_Rel.27531.bin.e
ad/jffs2-root/etc$ strings -n 10 passwd
root:$1$gt7/dy0B$6hlpR95uckyG1cQPXJB.H.:0:0:Linux User,,,:/home/root:/bin/sh
jhilland@jhilland:~/git/ECE531/module2/homework1/1.1.12a/_NC220_1.1.12_Build_160321_Rel.27531.bin.e
ad/jffs2-root/etc$
```

Figure 4: Strings on passwd

```
0.32.bin.extracted/jffs2-root$ ls sbin/
ad_alarm          ftpnew_alarm      mdnew_alarm       p2pd              ssl-tunnel        upnp
autoupgradenotice gpld              mDNSResponderPosix relayd             streamd           watch_upgrade.sh
autoupgrade.sh    ipcamera          motion            save_last_time.sh syslogd
datetimed          lighttpd          onvif             smtpnew_alarm     upgrader
jhilland@jhilland:~/git/ECE531/module2/homework1/v.2/_NC220_1.2.0_Build_170516_Rel.B4AC0D_2017-05-1
0.32.bin.extracted/jffs2-root$ sudo chroot . ./qemu-mips-static sbin/onvif
Error while loading sbin/onvif: Exec format error
jhilland@jhilland:~/git/ECE531/module2/homework1/v.2/_NC220_1.2.0_Build_170516_Rel.B4AC0D_2017-05-1
0.32.bin.extracted/jffs2-root$ sudo chroot . ./qemu-mips-static sbin/ad_alarm
Error while loading sbin/ad_alarm: Exec format error
jhilland@jhilland:~/git/ECE531/module2/homework1/v.2/_NC220_1.2.0_Build_170516_Rel.B4AC0D_2017-05-1
0.32.bin.extracted/jffs2-root$ sudo chroot . ./qemu-mips-static sbin/datetimed
Error while loading sbin/datetimed: Exec format error
jhilland@jhilland:~/git/ECE531/module2/homework1/v.2/_NC220_1.2.0_Build_170516_Rel.B4AC0D_2017-05-1
0.32.bin.extracted/jffs2-root$ sudo chroot . ./qemu-mips-static sbin/p2pd
Error while loading sbin/p2pd: Exec format error
jhilland@jhilland:~/git/ECE531/module2/homework1/v.2/_NC220_1.2.0_Build_170516_Rel.B4AC0D_2017-05-1
0.32.bin.extracted/jffs2-root$
```

Figure 5: Qemu Commands

Radare2's rabin2 command was used to analyze multiple files. This tool can tell us information about the file, such as the programming language and operating system supported.

```

dateutilmed  lighttpd  dnvcl  smtpnew_alarm  upgrader
jhilland@jhilland:~/git/ECE531/module2/homework1/v.2/_NC220_1.2.0_Build_170516_Rel.B4AC0D_2017-05-
0.32.bin.extracted/jffs2-root/sbin$ rabin2 -I smtpnew_alarm
baddr      0x0
binsz      121548
bits       0
canary     false
crypto     false
endian     little
havecode   false
laddr      0x0
linenum    false
lsyms      false
nx         false
pic        false
relocs     false
sanitize   false
static     true
stripped   false
va         false

```

Figure 6: Radare2 Commands

```

jhilland@jhilland:~/git/ECE531/module2/homework1/v
0.32.bin.extracted/jffs2-root/config$ tree
.
├── conf.d
│   ├── debug.conf
│   ├── dirlisting.conf
│   ├── fastcgi.conf
│   └── mime.conf
├── ipcamera
│   ├── Region
│   ├── Wireless.conf
│   └── workmod.conf
├── lighttpd.conf
├── modules.conf
├── RT2860AP.dat
├── SingleSKU_CE.dat
├── SingleSKU.dat
├── SingleSKU_FCC.dat
├── syslog.conf
└── workmod_define.conf

2 directories, 15 files
jhilland@jhilland:~/git/ECE531/module2/homework1/v
0.32.bin.extracted/jffs2-root/config$ 

```

Figure 7: Config Directory Contents

5 Conclusion

The file structure is fairly similar to that of the HS110 image that was explored during lecture slides. However there is no `usr/bin` directory for analysis. All three NC220 binary files have similar filesystem setups. They are all running off of the JFFS2 filesystem. All three have the same Linux kernel version number. There are a few files extra within the version 2 binary file. Based on commands found in the `bin` and `sbin` directories, further research and analysis could be done. There were attempts at running some commands via `qemu-mips-static`, however results were unsuccessful.