Make your own Hacker Gadget

Vivek Ramachandran

Chief Trainer

http://PentesterAcademy.com

Vendor Firmware Analysis with Binwalk

What is Firmware?

- Firmware is the combination of persistent memory and program code and data stored in it – http://en.wikipedia.org/wiki/Firmware

- Simply Put
  - The Operating System
  - The Configuration
  - The Filesystem

- Self Contained Package

Multiple Process Architecture

- MIPS
- ARM
- Intel ATOM
- …

Operating Systems

- Linux based
- VxWorks
- Cisco IOS
- …

What does the Firmware contain?

- Bootloader
- OS Kernel
- File System
  - Built-in utilities e.g. Busybox
  - Web Server i.e. external interface
  - Configuration data

Getting the MR-3020 Firmware

- Download Firmware

http://www.tplink.com/en/support/download/?model=TL-MR3020&version=V1

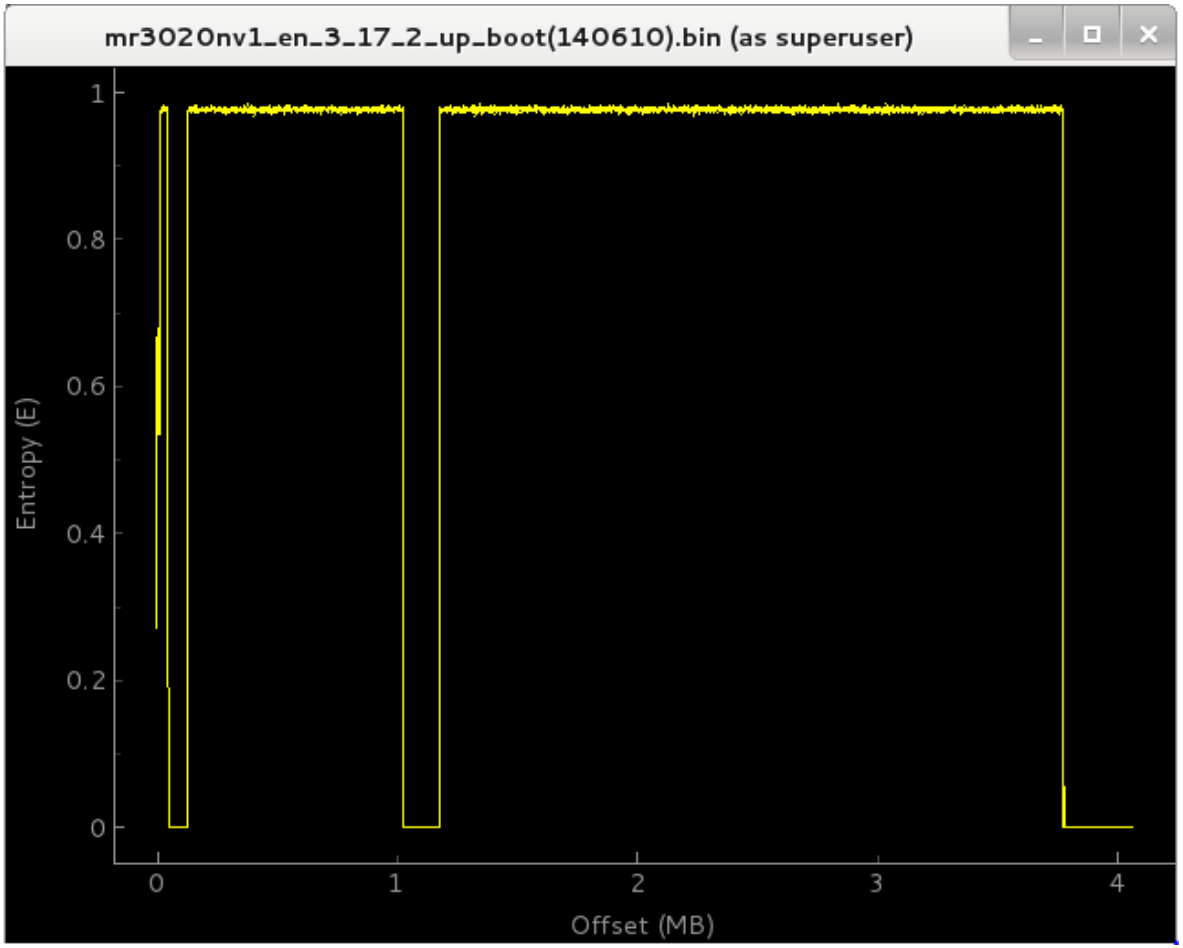
- Version used at this time of writing:

TL-MR3020_V1_140610

Binwalk

- Tool to analyze and extract firmware
- Uses signatures for bootloaders, filesystems etc. to locate them in file
- Can extract some firmware out of the box
- Good tool to analyze firmware which cannot be automatically extracted
- http://binwalk.org/

Binwalk Entropy Analysis



http://www.devttys0.com/2013/06/differentiate-encryption-from-compression-using-math/

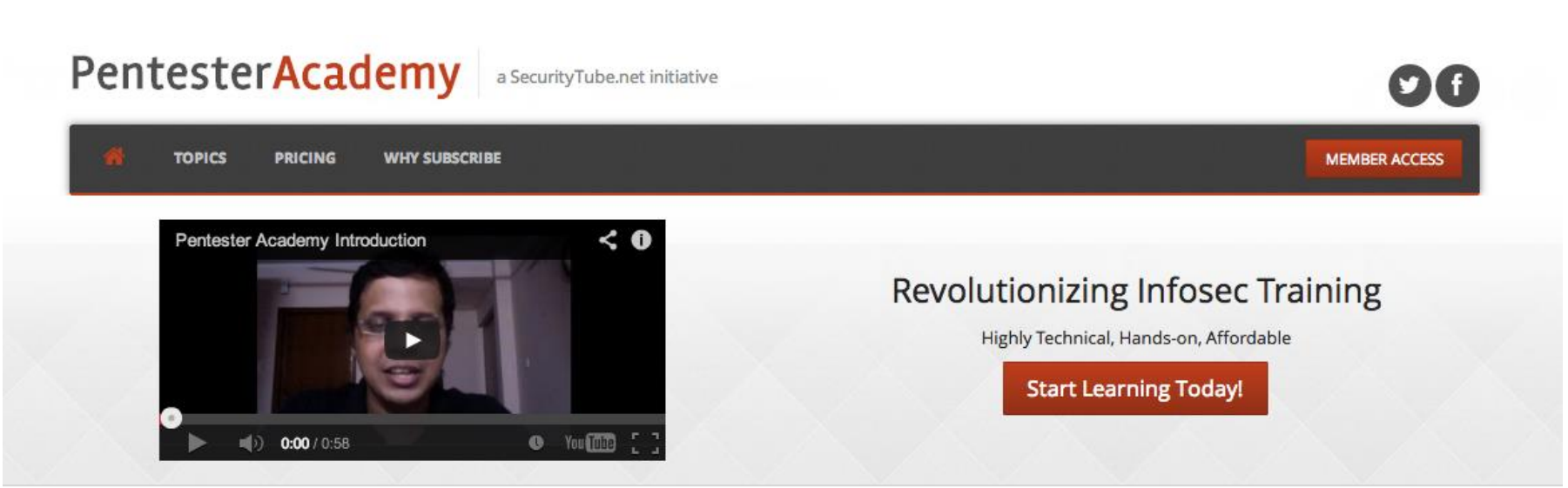
Binwalk Firmware Auto Analysis

```
root@debian:/home/pentester/temp# binwalk -t -vv  mr3020nv1_en_3_17_2_up_boot\(140610\).bin

Scan Time:     2014-11-29 01:57:32
Target File:   mr3020nv1_en_3_17_2_up_boot(140610).bin
MD5 Checksum:  4e44ca7cdabf7286228b8b4324e3d51a
Signatures:    285

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------------------------------------------------------
0             0x0             TP-Link firmware header, firmware version: 3.17.2, image version: "ver. 1.0", product ID: 0x30200001, product
                              version: 1, kernel load address: 0x80002000, kernel entry point: 0x801D58B0, kernel offset: 512, kernel length:
                              892221, rootfs offset: 1048576, rootfs length: 2883584, bootloader offset: 0, bootloader length: 48393
14144         0x3740          U-Boot version string, "U-Boot 1.1.4-ge28c8345 (Jun 10 2014 - 17:57:47)"
15488         0x3C80          uImage header, header size: 64 bytes, header CRC: 0xC21F81, created: Tue Jun 10 05:57:48 2014, image size: 33353
                              bytes, Data Address: 0x80010000, Entry Point: 0x80010000, data CRC: 0x2DF367A0, OS: Linux, CPU: MIPS, image type:
                              Firmware Image, compression type: lzma, image name: "u-boot image"
15552         0x3CC0          LZMA compressed data, properties: 0x5D, dictionary size: 33554432 bytes, uncompressed size: 95584 bytes
131584        0x20200         TP-Link firmware header, firmware version: 3.17.2, image version: "ver. 1.0", product ID: 0x30200001, product
                              version: 1, kernel load address: 0x80002000, kernel entry point: 0x801D58B0, kernel offset: 512, kernel length:
                              892221, rootfs offset: 1048576, rootfs length: 2883584, bootloader offset: 0, bootloader length: 0
132096        0x20400         LZMA compressed data, properties: 0x5D, dictionary size: 33554432 bytes, uncompressed size: 2581428 bytes
1180160       0x120200        Squashfs filesystem, little endian, version 4.0, compression:lzma, size: 2594041 bytes,  624 inodes, blocksize:
                              131072 bytes, created: Tue Jun 10 06:04:31 2014
```

Pentester Academy



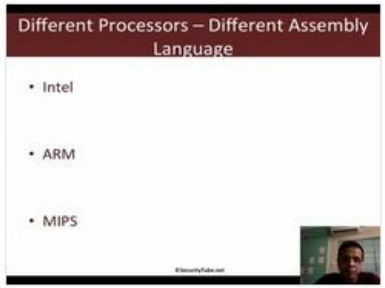
Latest Videos

New content added weekly!

Challenge 7: Cracking Digest Authentication Solution in WAP Challenges

Challenge 7: Cracking Digest Authentication in WAP Challenges

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



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