COMP8053 – Embedded Software Security

Lab 1 – Using Binwalk

Binwalk (https://github.com/ReFirmLabs/binwalk) is a firmware analysis tool, which lets us identify unknown firmware images and explore their contents. To initially get firmware, we can either download them from the embedded device manufacturer's website, or they can be extracted through various means. You can read about some of the methods to extract firmware here: https://ianhowson.com/iot/extracting-firmware/

For this lab, you will install binwalk and then explore some of its capabilities.

Step 1) Start the Linux VM on lab computers.

- Login as "studentid@mtu.ie"
- Alternatively, you can use your own laptops as long as you have some version of Linux on it. Free link for a Linux VM is available on Canvas.

Step 2) Download and install binwalk

- We can download binwalk via github using the below commands to download and unpack it:

- `wget https://github.com/devttys0/binwalk/archive/master.zip`
- `unzip master.zip`

- To install binwalk, enter the unpacked directory from the last step 'binwalk-master'

  If any previous version of binwalk was installed, it's best to remove it fully first (not necessary on first install)

- `#remove old install of binwalk if necessary`
- `sudo python3 setup.py uninstall`

- `#install binwalk`
- `sudo python3 setup.py install`

- `#install the squashfs-tools to allow for extracting squashfs file systems`
- `sudo apt-get install squashfs-tools`

Step 3) Get some firmware binaries

- We have now installed binwalk and all its dependencies, so we are ready to start inspecting firmware images! Pick a copy of a device's firmware from this repository of D-Link device firmwares. http://ftp.dlink.ru/pub/Router/
- Search for .bin files in the /firmware/ subdirectories of each device. Not every device has a firmware.
- Download a couple of firmware .bin files and store them in a directory on the VM.

Step 4) Running Binwalk

- `#help options`
- `binwalk  or binwalk -h`

- `#scan for common file signatures`
- `binwalk <filename>  or binwalk -B <filename>`

  This provides us with an automatically filtered list of file type signatures detected by binwalk in the firmware. Binwalk automatically removes what it believes to be false positives from the list of results here. The next two options allow is to disable this automatic filtering and check all the detected signatures.

- `#include invalid signatures`
- `binwalk -I <filename>`
- `#disable smart signature keywords`
- `binwalk -b <filename>`

- Look through the lists of additional signatures that were initially filtered out. Can you guess why some of them were automatically disregarded?

- The next 2 commands allow us to filter out certain results from the list of signatures, and can be combined with each other or other options.

- `#return only signatures containing the regular expression <regexp> (all lower case), only matches on the first field of the signature description`
- `binwalk -y <reg exp> <filename>`
- `#return only signatures excluding the regular expression <regexp> (all lower case), only matches on the first field of the description`
- `binwalk -x <reg exp> <filename>`

- In addition to letting us view the types of files contained within a firmware image, binwalk also allows us to extract those files. While using the more advanced options can allow you to specify specific file signatures to extract, here we will make use of binwalk's automatic extraction command.

- #Extract files automatically
- binwalk –e <filename>

- #Extract files automatically, and recursively scan the extracted data for further extractable files.
- binwalk –Me <filename>

- Explore the extracted file systems from some of the firmwares.

    a. Try to find firmware with full file systems you can extract.
    b. See what kind of hardcoded secret/private information you can find in the extracted file systems.
    c. If the firmware you tried didn't have much that binwalk could extract, try one from a firmware with a very different name. Firmware for devices in the same family will tend to be similar. e.g. DI-2004 and DI-2006 are probably very similar while DI-774 is probably different to them. So try to test firmware in a variety of families.