**Quiz #4**

**Name:** CENSORED

**Due Date:** 11/15/19

**Class:** COMP-5970

**Firmware Extension Definitions:**

IMG: These are bitmap files that contain image data; the image that is contained in the IMG file can be a graphic bitmap or an image of a disc. These are usually used to execute the image of a disc so that the disc media can be played without owning the physical copy of the disc, like how an ISO file would be used.

BIN: These are compressed binary files that are used by many different computer applications for a variety of reasons. The BIN files contain binary code that could be used by different applications on the computer, although it is usually used by CD and DVD backup image files and certain anti-virus programs.

TRX: These are firmware image files that are typically used in embedded systems such as routers. They include a header with a file checksum, a file length, and the node offsets within the file; it can be used for the update or recovery of the firmware that is stored in ROM on the device.

**Firmware Extension Differences:** BIN and TRX files are almost identical to each other, although BIN files have some extra data at the beginning of the file. The extra header bytes contain data used to validate whether the firmware is appropriate for the target system or not. The difference between IMG and BIN files are that IMG files sometimes consist of more than one BIN file, although it’s mostly just a naming convention; functionally these file types behave the same. The real difference lies in where these firmware files are used; IMG files are typically seen on CD’s, BIN files are binary files that can be used in a variety of settings (Microsoft system files, embedded in IMG files, etc.) and are therefore the most common type of firmware file to see, and TRX files are firmware image files that are typically used in embedded systems.

**Model Numbers:**

IMG: The AC2100-V1.2.0.42\_1.0.1.img file correlates to the NETGEAR AC2100 router, so the model number is AC2100.

BIN: The dir300-firmware.bin file correlates to the D-Link DIR-300 router, so the model number is DIR-300.

TRX: The RT-AC51U\_3.0.0.4\_380\_8497-g179ec32.trx file correlates to the ASUS RT-AC51U router, so the model number is RT-AC51U.

**File Systems:**

IMG: The AC2100-V1.2.0.42\_1.0.1.img file uses a Zip archive as it’s filesystem (located at offset 512).

BIN: The dir300-firmware.bin file uses the Squashfs filesystem (located at offset 851996).

TRX: The RT-AC51U\_3.0.0.4\_380\_8497-g179ec32.trx file uses the Squashfs filesystem (located at offset 1174784).

**Compression Schemes:**

IMG: The AC2100-V1.2.0.42\_1.0.1.img file compresses its’ contents as a ZIP file.

BIN: The dir300-firmware.bin file compresses its’ contents with a LZMA compression scheme; this is located at byte offset 28.

TRX: The RT-AC51U\_3.0.0.4\_380\_8497-g179ec32.trx file compresses its’ contents with a LZMA compression scheme; this is located at byte offset 64.

**Useful File System Information:** Some information contained in the file systems that could be useful during a penetration test includes device configurations, default login credentials, public/private key pairs and security configurations. If a file system contains any of this information, it can be used to gain access to the file system itself (using the default login credentials, manipulating the security configs, etc.) on the target machine once it has been installed correctly. This means that an attacker could dive into the file system, pull something like a private key or default credentials from it, and then use them to gain access to the file system once it has been installed on a machine.