The bootloader or boot program or bootstrap loader is a special software program that is responsible for locating and loading all the required files i.e. kernel, filesystem, and starting the operating system. Universal Boot Loader (U-Boot) is one of the most popular open-source bootloaders that is used in a lot of different architectures/platforms/devices.

In this section, we will learn about U-Boot, creating emulated IoT devices using Qemu, booting the IoT devices, and bypassing device login to access the files and resources of an IoT device.

What will you learn?

- Basics of U-boot bootloader
- How to emulate an embedded/IoT device using Qemu
- Booting an embedded device using TFTP server and local files
- Bypassing login authentication to steal files from the device filesystem

References:

1. Qemu (https://www.qemu.org/)
2. ARM Device emulation with qemu (https://www.qemu.org/docs/master/system/target-arm.html)
3. U-boot (https://github.com/u-boot/u-boot)
4. Embedded IoT Linux for Red-Blue Teams (https://www.pentesteracademy.com/course?id=37)

Labs:

- Bootloader Warmup Lab
  Learn the basics of a U-Boot bootloader by interacting with the bootloader of a simulated IoT device.

- Build Lab: ARM vexpress Board
  Build u-boot, kernel, filesystem archives from source and create an emulated IoT device using Qemu.

- Local Boot using U-Boot
  Locate the kernel and filesystem archives on the filesystem of the device using u-boot. Then, load these archives into the memory and boot the device.

- TFTP Boot using U-Boot
  Boot an IoT device by fetching the required files (kernel, DTB and filesystem archives) from a TFTP server present on the same network.

- U-Boot: Insert Backdoor Shell into FS
  Bypass the login authentication of an emulated IoT device by writing a rogue service file to the filesystem of this device.

- U-Boot: Backdoor FS with Kernel Module
  Bypass the login authentication of an emulated IoT device by inserting a rogue kernel module into the kernel of this device.

- U-Boot: Stealing Files from FS
  Steal the files present on the filesystem of an emulated IoT device by using the u-boot console.

Bootloader Warmup Lab

Start