ATTACK DEFENSE

by PentesterAcademy

Name	Bootloader Warmup Lab
URL	https://www.attackdefense.com/challengedetails?cid=1221
Type	IoT : Bootloader

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

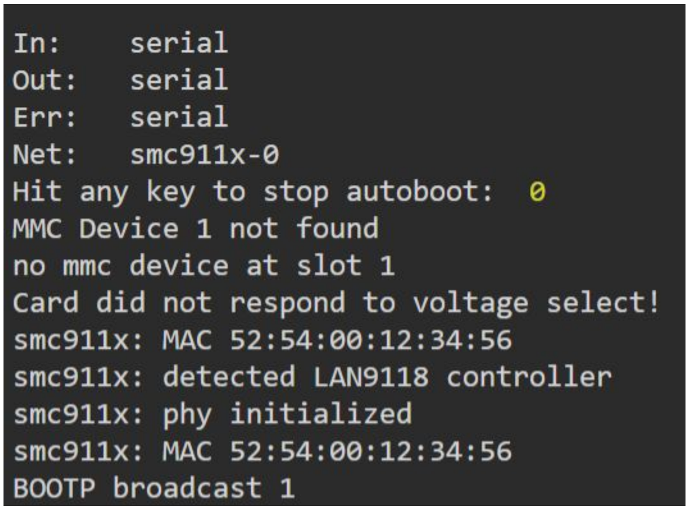
Activity I: Boot the device using provided U-boot and answer the following:

Q1. How much time U-boot waits before starting the next stage (i.e. booting kernel)

Answer: 2

Launch the Vexpress-a9 machine with 256 MB RAM and pass it U-boot

Command: qemu-system-arm -m 256 -M vexpress-a9 -nographic -kernel u-boot



```
In:    serial
Out:   serial
Err:   serial
Net:   smc911x-0
Hit any key to stop autoboot:  0
MMC Device 1 not found
no mmc device at slot 1
Card did not respond to voltage select!
smc911x: MAC 52:54:00:12:34:56
smc911x: detected LAN9118 controller
smc911x: phy initialized
smc911x: MAC 52:54:00:12:34:56
BOOTP broadcast 1
```

Here,

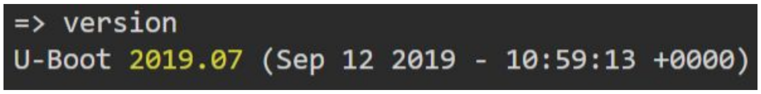
-m 256 : Memory to be allocated to virtual device
-M vexpress-a9: Virtual machine selection
For more on Vexpress: https://crux-arm.nu/SupportedDevices/Vexpress
-nographic : To invoke qemu from CLI
-kernel u-boot **:** Passing u-boot file to start booting from

U-boot will start executing and will show a countdown to stop autoboot. This count starts from 2 seconds in this case. Hence, the answer is 2.

Q2. What is the version of the given U-boot?

Answer: 2019.07

Commands: version

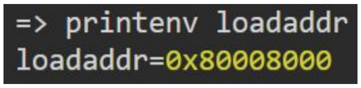


```
=> version
U-Boot 2019.07 (Sep 12 2019 - 10:59:13 +0000)
```

Q3. What is the value stored in U-boot environment variable "loadaddr"?

Answer: 0x80008000

Commands: printenv loadaddr

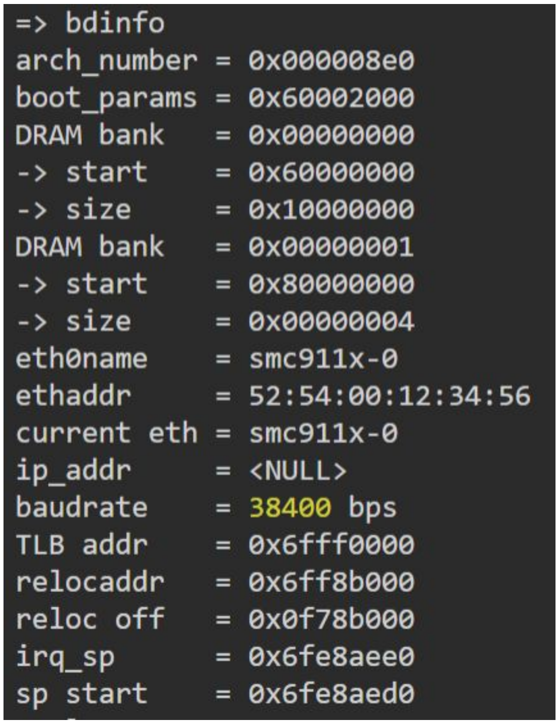


```
=> printenv loadaddr
loadaddr=0x80008000
```

Q4. What is the value of baudrate (in bps)?

Answer: 38400

Command: bdinfo

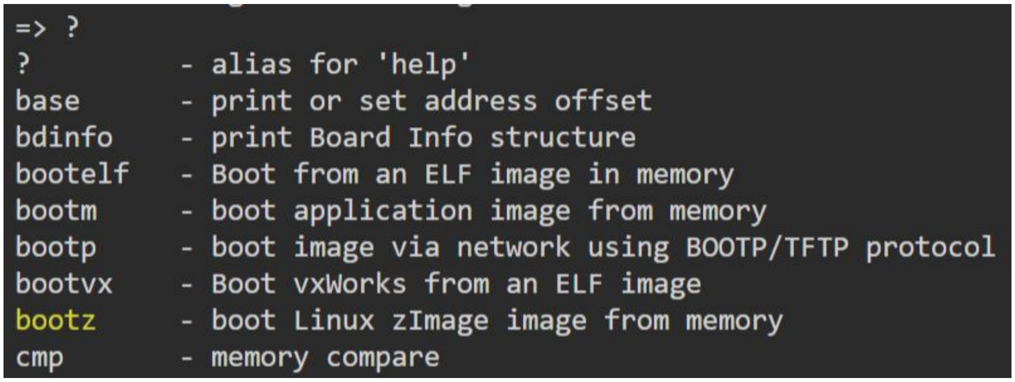


```
=> bdinfo
arch_number = 0x000008e0
boot_params = 0x60002000
DRAM bank   = 0x00000000
-> start    = 0x60000000
-> size     = 0x10000000
DRAM bank   = 0x00000001
-> start    = 0x80000000
-> size     = 0x00000004
eth0name    = smc911x-0
ethaddr     = 52:54:00:12:34:56
current eth = smc911x-0
ip_addr     = <NULL>
baudrate    = 38400 bps
TLB addr    = 0x6fff0000
relocaddr   = 0x6ff8b000
reloc off   = 0x0f78b000
irq_sp      = 0x6fe8aee0
sp start    = 0x6fe8aed0
```

Q5. What command can be used to boot Linux zImage image from memory?

Answer: bootz

Command: ?



```
=> ?
?          - alias for 'help'
base       - print or set address offset
bdinfo     - print Board Info structure
bootelf    - Boot from an ELF image in memory
bootm      - boot application image from memory
bootp      - boot image via network using BOOTP/TFTP protocol
bootvx     - Boot vxWorks from an ELF image
bootz      - boot Linux zImage image from memory
cmp        - memory compare
```

Activity II: Boot the device and retrieve the flag kept in /root directory of the disk image.

Run the emulated machine with given components and 256 MB RAM

Command: qemu-system-arm -m 256 -M vexpress-a9 -nographic -kernel vmlinuz-3.2.0-4-vexpress -initrd initrd.img-3.2.0-4-vexpress -drive if=sd,file=debian_wheezy_armhf_standard.qcow2 -append "root=/dev/mmcblk0p2 rw console=ttyAMA0"

Here,

-m 256 : Memory to be allocated to virtual device

-M vexpress-a9: Virtual machine selection

For more on Vexpress: https://crux-arm.nu/SupportedDevices/Vexpress

-nographic : To invoke qemu from CLI

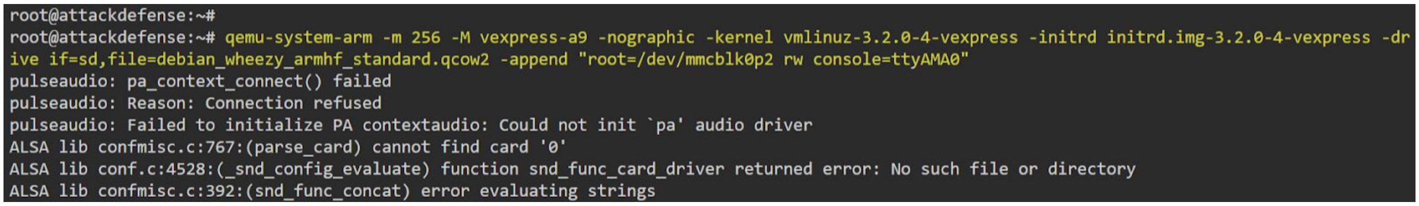
-kernel vmlinuz-3.2.0-4-vexpress: Linux kernel image to use

-initrd initrd.img-3.2.0-4-vexpress: Initial RAM image to use

-drive if=sd,file=debian_wheezy_armhf_standard.qcow2 : disk image to be mounted as SD card

-append : to define Boot parameters

- root=/dev/mmcblk0p2 : Filesystem location i.e. 2nd partition (p2) of mounted SD card
- rw : Mounting SD card in read/write mode
- console=ttyAMA0 : Direct console output to current shell session



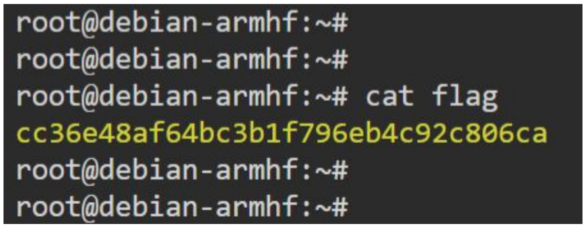
```
root@attackdefense:~#
root@attackdefense:~# qemu-system-arm -m 256 -M vexpress-a9 -nographic -kernel vmlinuz-3.2.0-4-vexpress -initrd initrd.img-3.2.0-4-vexpress -dr
ive if=sd,file=debian_wheezy_armhf_standard.qcow2 -append "root=/dev/mmcblk0p2 rw console=ttyAMA0"
pulseaudio: pa_context_connect() failed
pulseaudio: Reason: Connection refused
pulseaudio: Failed to initialize PA contextaudio: Could not init `pa' audio driver
ALSA lib confmisc.c:767:(parse_card) cannot find card '0'
ALSA lib conf.c:4528:(_snd_config_evaluate) function snd_func_card_driver returned error: No such file or directory
ALSA lib confmisc.c:392:(snd_func_concat) error evaluating strings
```

The machine will start and after going through boot sequence, eventually present console login to the user. The user has to use the following credentials:

Username: root
Password: root

After logging into the machine, the flag cat be retrieved from the /root directory.

Command: cat flag



```
root@debian-armhf:~#
root@debian-armhf:~#
root@debian-armhf:~# cat flag
cc36e48af64bc3b1f796eb4c92c806ca
root@debian-armhf:~#
root@debian-armhf:~#
```

The flag is **cc36e48af64bc3b1f796eb4c92c806ca**

References:

- U-boot source: https://www.denx.de/wiki/U-Boot/SourceCode
- All Kernel, Initrd image and disk image are taken from here: https://people.debian.org/~aurel32/qemu/armhf/