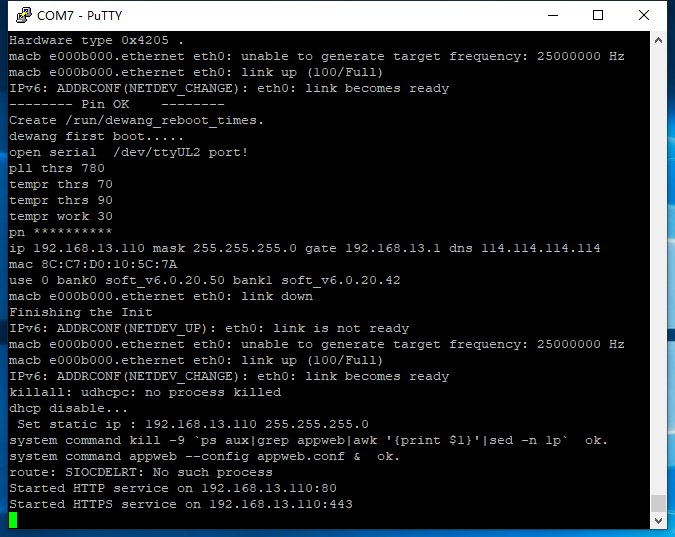
矿渣到手后是原来挖矿的固件，用户名和密码不得而知，不过群里大佬总是有办法

感谢大佬 @帝都流浪着 @橘子

基本思想就是通过进入linux的单用户模式绕过原来的password验证

如果你收到的矿渣uboot版本为U-Boot 2015.07 (May 18 2017 - 22:22:09 +0800)，那么请直接看文章的后面部分，这里只针对uboot版本为U-Boot 2015.07 (Jun 28 2017 - 21:05:18 +0800)的矿渣



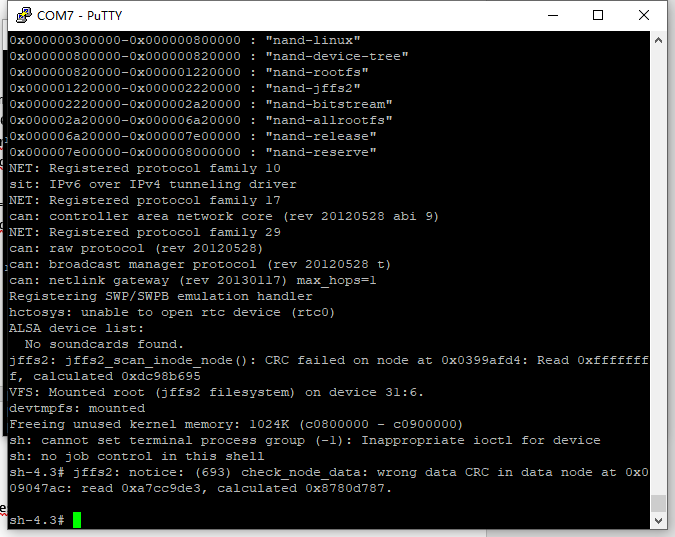
三条命令搞定

**nandboot=echo Copying Linux from NAND flash to RAM... && nand info && run nandroot;nand read 0x100000 0x2220000 0x300000 && fpga loadb 0 0x100000 0x300000 && nand read ${kernel\_load\_address} 0x300000 ${kernel\_size} && nand read ${devicetree\_load\_address} 0x800000 ${devicetree\_size}**

**setenv bootargs 'console=ttyPS0,115200 root=/dev/mtdblock6 rootfstype=jffs2 noinitrd rw rootwait reboot=cold,hard emergency init=/bin/sh'**

**bootm ${kernel\_load\_address} - ${devicetree\_load\_address} init=/bin/sh**

启动后promot为sh-4.3#,即成功，用passwd修改密码即可



参考链接

<https://wrgms.com/entering-single-user-mode-on-a-synology/>

**[非常规uboot破解]**

如果uboot版本为U-Boot 2015.07 (May 18 2017 - 22:22:09 +0800)，用上面的办法没法直接破解密码，根据的办法就是要更新uboot，dtb,rootfs

不更新uboot进入系统

1. 需要更新dtb,allrootfs

setenv ipaddr 192.168.1.200

setenv serverip 192.168.1.100

#### DTB ####

tftpboot 0x100000 devicetree.dtb

nand erase 0x800000 0x20000

nand write 0x100000 0x800000 0x20000

****

#### ROOTFS ####

**tftpboot 0x100000 allrootfs.new**

**zynq-uboot> nand erase 0x2a20000 0x4000000**

**zynq-uboot> nand write 0x100000 0x2a20000 0x4000**000



1. 更新完成后便可以之前的方式破解
2. 由于没有更新uboot，所以进入的方式需要更改为如下命令

**nandboot=echo Copying Linux from NAND flash to RAM... && nand info && run nandroot;nand read 0x100000 0x2220000 0x300000 && fpga loadb 0 0x100000 0x300000 && nand read ${kernel\_load\_address} 0x300000 ${kernel\_size} && nand read ${devicetree\_load\_address} 0x800000 ${devicetree\_size}**

**setenv bootargs 'console=ttyPS0,115200 root=/dev/mtdblock6 rootfstype=jffs2 noinitrd rw rootwait reboot=cold,hard'**

**bootm ${kernel\_load\_address} - ${devicetree\_load\_address}**

20190626 @Chin