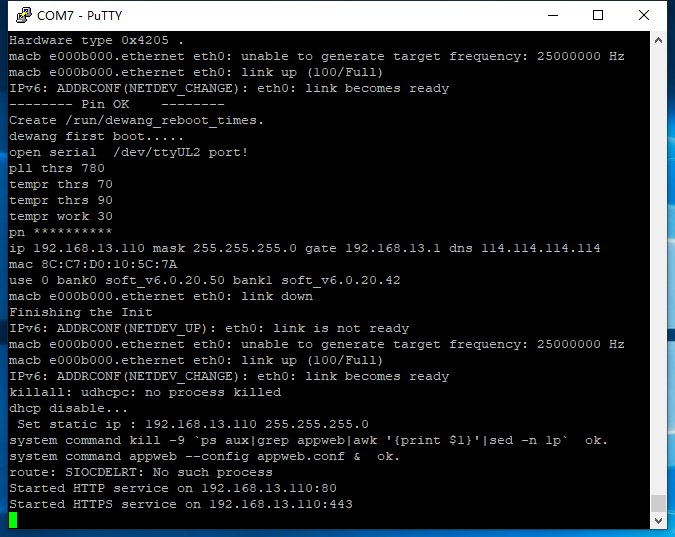
矿渣到手后是原来挖矿的固件，用户名和密码不得而知，不过群里大佬总是有办法

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



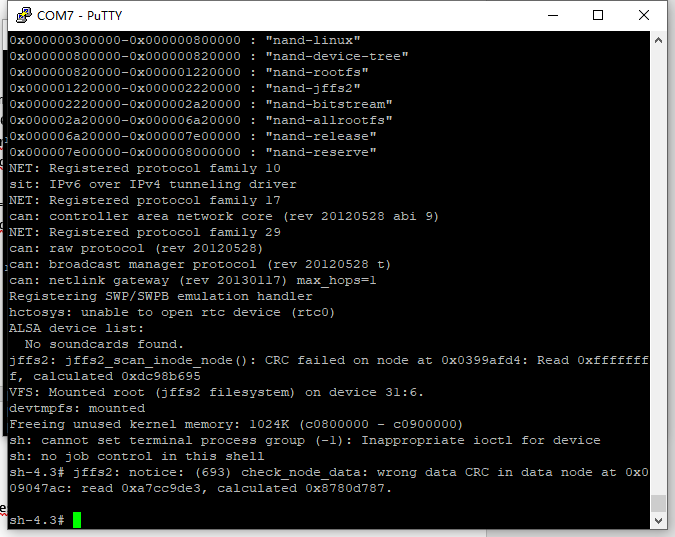
三条命令搞定

**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/>

20190618 @Chin