Hacking d'une Webcam SmartWaves

Get the serial interface

Got it, good

```
screen /dev/ttyUSB0 115200
```

- On boot et on appui sur une touche pour passer dans le mode rescue
- On tape 'printenv'

```
isvp_t21# printenv
baudrate=115200
bootargs=console=ttyS1,115200n8 mem=43M@0x0 rmem=21M@0x2B00000 init=/linuxrc
rootfstype=jffs2 root=/dev/mtdblock2 rw
mtdparts=jz_sfc:256k(boot),2048k(kernel),14080k(root),-(appfs)
bootcmd=sf probe;sf read 0x80600000 0x40000 0x200000; bootm 0x80600000
bootdelay=1
ethact=Jz4775-9161
ethaddr=00:d0:d0:00:95:27
gatewayip=193.169.4.1
ipaddr=193.169.4.81
loads_echo=1
netmask=255.255.255.0
serverip=193.169.4.2
stderr=serial
stdin=serial
stdout=serial

Environment size: 492/16380 bytes
```

- On modifie la ligne qui démarrer en single mode

```
setenv bootargs console=ttyS1,115200n8 mem=43M@0x0 rmem=21M@0x2B00000
init=/linuxrc rootfstype=jffs2 root=/dev/mtdblock2 rw single
mtdparts=jz_sfc:256k(boot),2048k(kernel),14080k(root),-(appfs)
```

- puis on boot la bête

```
boot
passwd # et zou !
reboot
```

[0.000000] Kernel command line: console=ttyS1,57600n8 BootImage=1 root=/dev/mtdblock5 rootfstype=squashfs,jffs2

On est root sur la machine

```
cat /mnt/mtd/wpa.conf < EOF
ctrl_interface=/var/run/wpa_supplicant
network={
ssid="monssid"
key_mgmt=WPA-PSK
proto=RSN WPA WPA2
pairwise=TKIP CCMP
group=TKIP CCMP
psk="mouahahahahaha"
}
EOF
```

```
rm /etc/init.d/motion.sh
rm /etc/init.d/waakhond.sh
rm /etc/init.d/setUnabtoID.sh
rm /etc/init.d/alive.sh
rm /etc/init.d/snapshot.sh
```

Notes diverses

On tue le process 175 pour que ce soit moisn verbeux le temps du setup

Flux RTSP

```
/live/av0?user=&passwd=
root
3wRcEe5rjYfrA
```