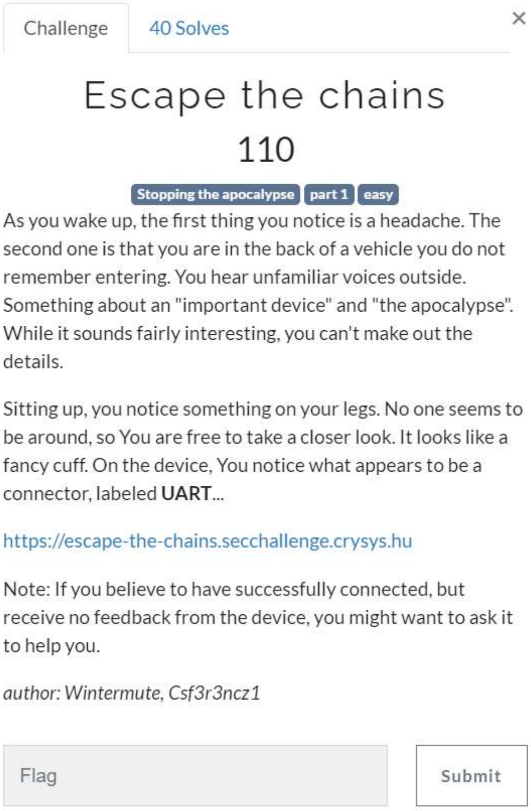
CrySyS Security Challenge 2021 - Escape the chains (hardware) writeup

Challenge description:



Challenge | 40 Solves

Escape the chains

110

Stopping the apocalypse | part 1 | easy

As you wake up, the first thing you notice is a headache. The second one is that you are in the back of a vehicle you do not remember entering. You hear unfamiliar voices outside. Something about an "important device" and "the apocalypse". While it sounds fairly interesting, you can't make out the details.

Sitting up, you notice something on your legs. No one seems to be around, so You are free to take a closer look. It looks like a fancy cuff. On the device, You notice what appears to be a connector, labeled **UART**...

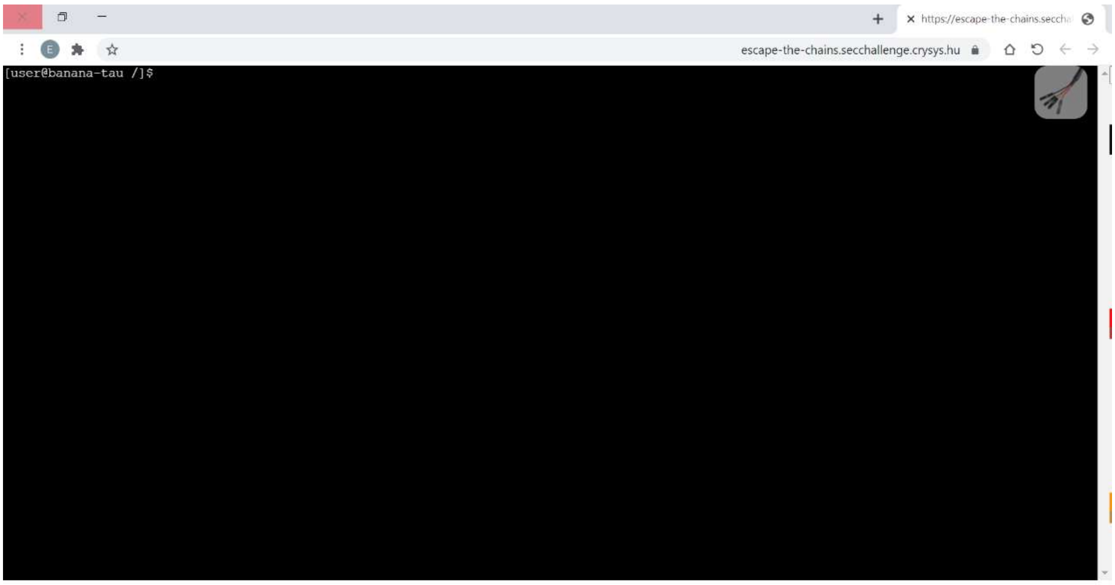
https://escape-the-chains.secchallenge.crysys.hu

Note: If you believe to have successfully connected, but receive no feedback from the device, you might want to ask it to help you.

author: Wintermute, Csf3r3ncz1

Flag | Submit

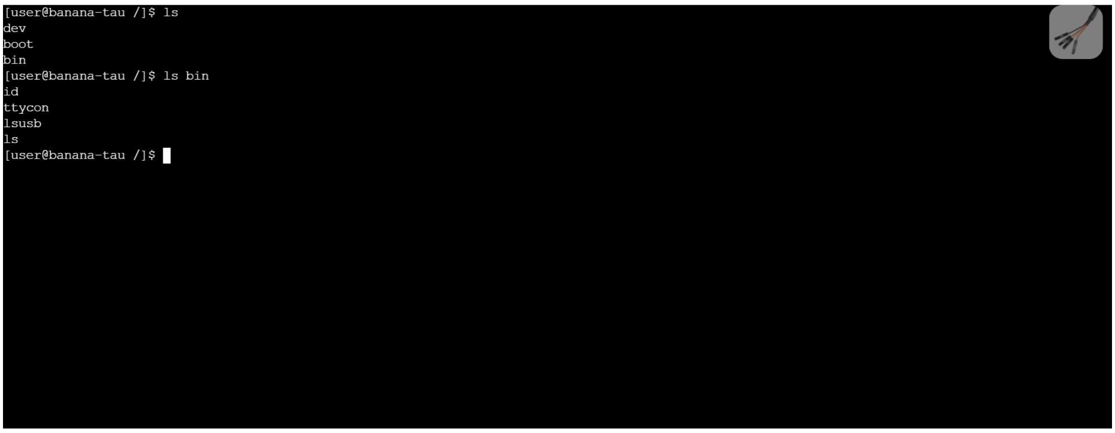
Entering the URL will show:



https://escape-the-chains.secchal
escape-the-chains.secchallenge.crysys.hu

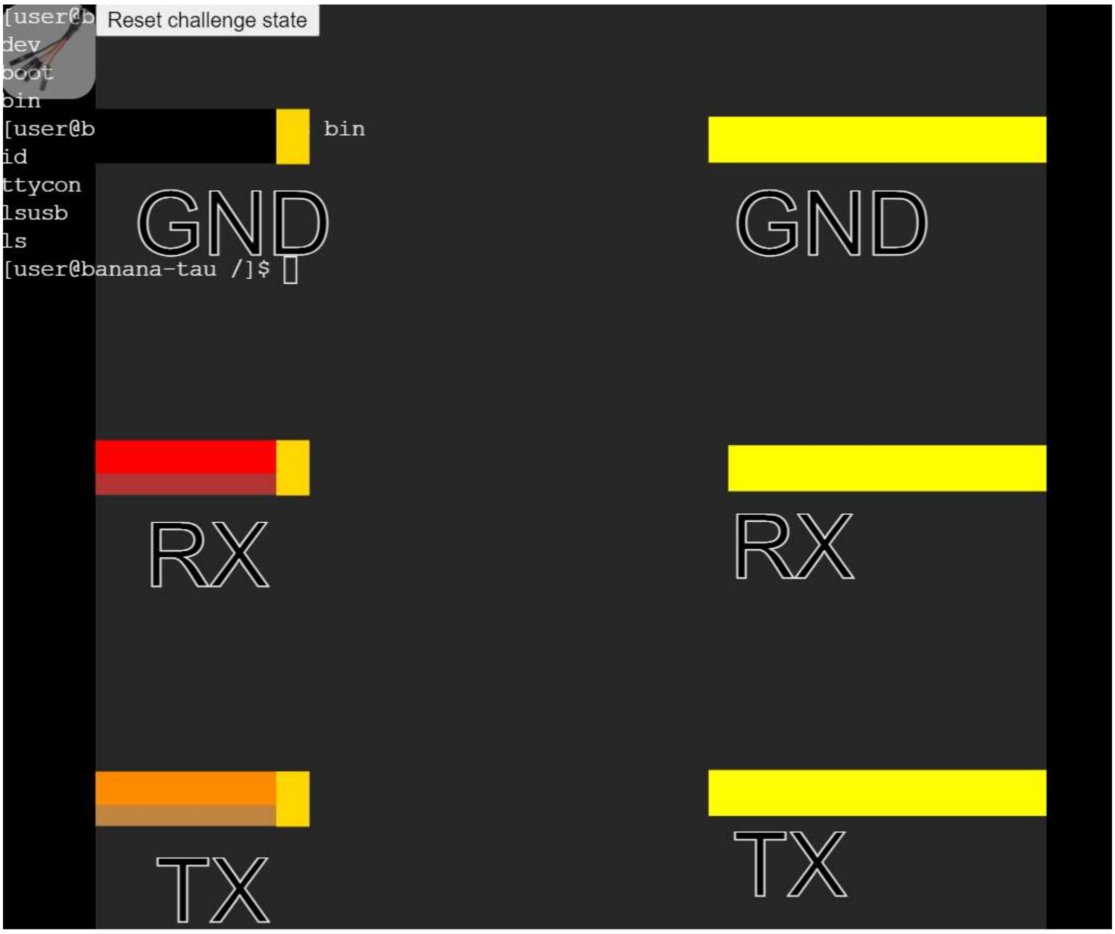
```
[user@banana-tau /]$
```

After a quick Google search, we found out that UART is related to USB.
Using the 'ls' command we'll see the directories that are available and running 'ls bin' will display the commands that this shell supports



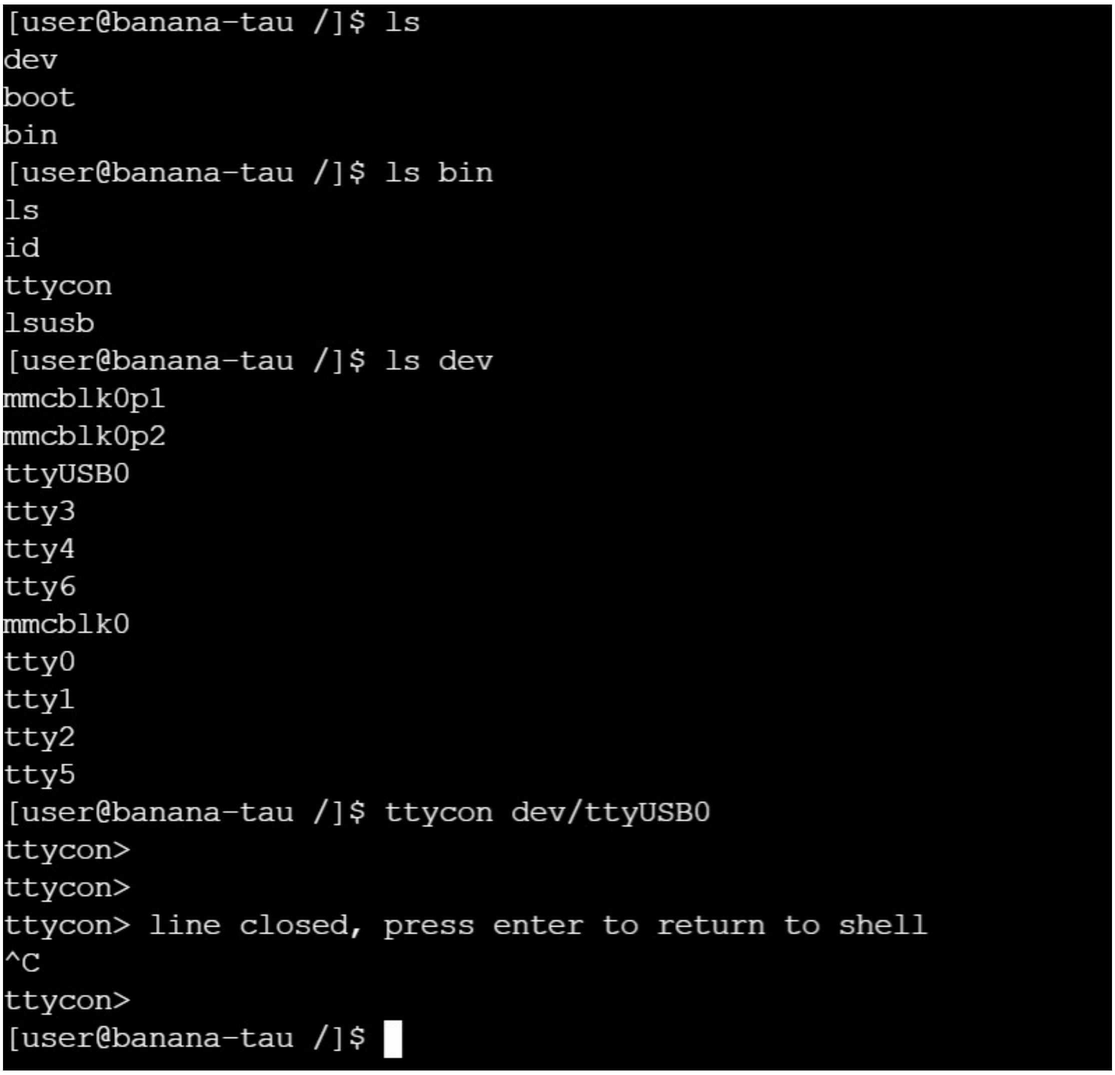
```
[user@banana-tau /]$ ls
dev
boot
bin
[user@banana-tau /]$ ls bin
id
ttycon
lsusb
ls
[user@banana-tau /]$ 
```

We noticed the icon on the right top corner, and it opened a connectors simulation



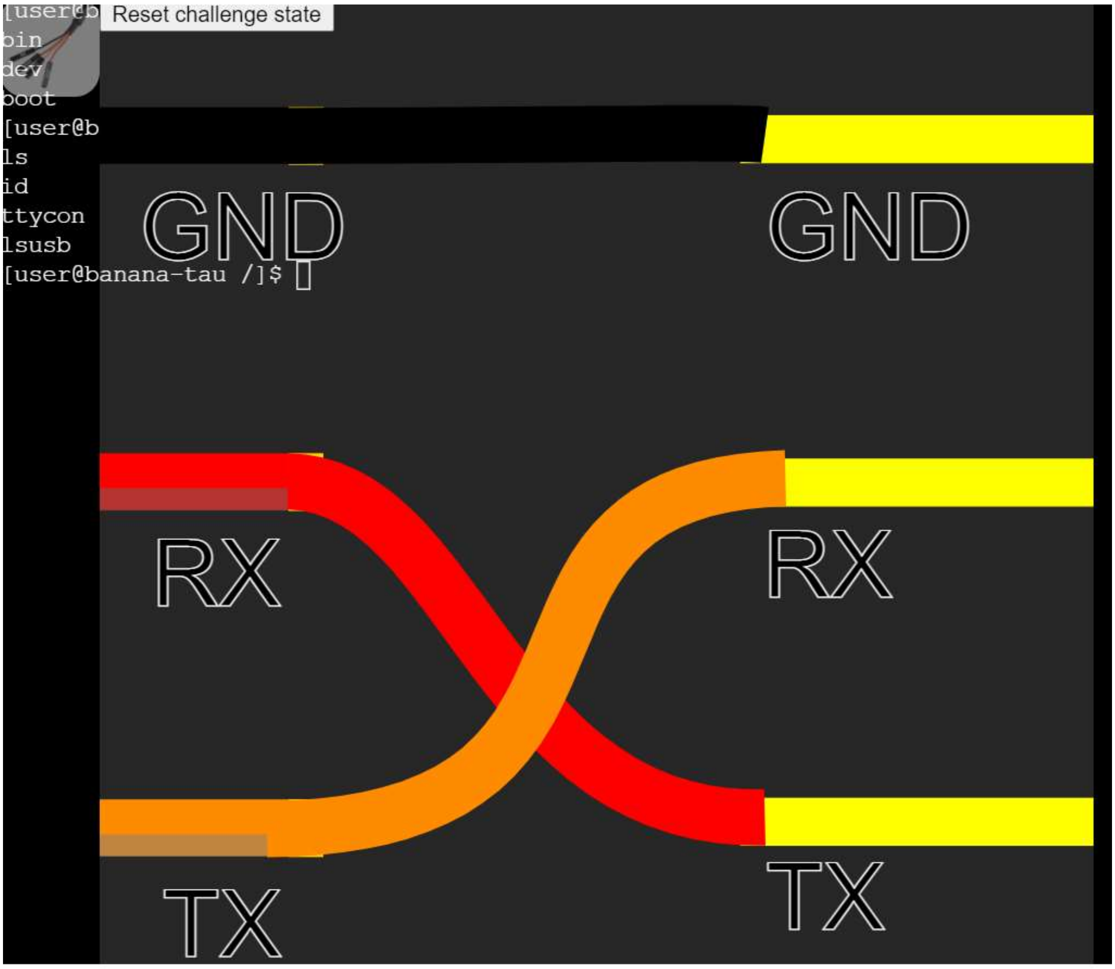
```
[user@b
dev
boot
bin
[user@b          bin
id
ttycon
lsusb
ls
[user@banana-tau /]$ 
```

Displayed the devices and tried to connect the 'ttyUSB0' device, following our understanding that this is a USB related challenge, but after pressing 'Enter' nothing happened.



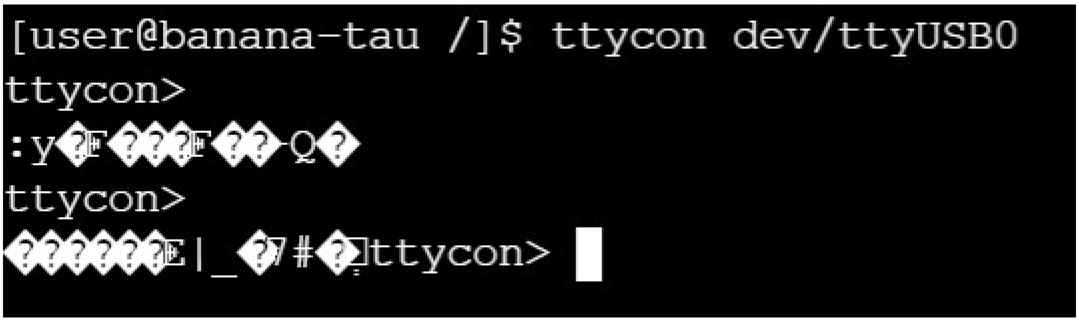
```
[user@banana-tau /]$ ls
dev
boot
bin
[user@banana-tau /]$ ls bin
ls
id
ttycon
lsusb
[user@banana-tau /]$ ls dev
mmcblk0p1
mmcblk0p2
ttyUSB0
tty3
tty4
tty6
mmcblk0
tty0
tty1
tty2
tty5
[user@banana-tau /]$ ttycon dev/ttyUSB0
ttycon>
ttycon>
ttycon> line closed, press enter to return to shell
^C
ttycon>
[user@banana-tau /]$ 
```

So according to the commands that we are allowed to use (lsusb and ttycon) and the image above we looked for UART architecture and found out that the right way to connect it is this:



```
[user@b
bin
dev
boot
[user@b
ls
id
ttycon
lsusb
[user@banana-tau /]$ 
```

After the connection is in its right manner, pressing 'Enter' and we will get:

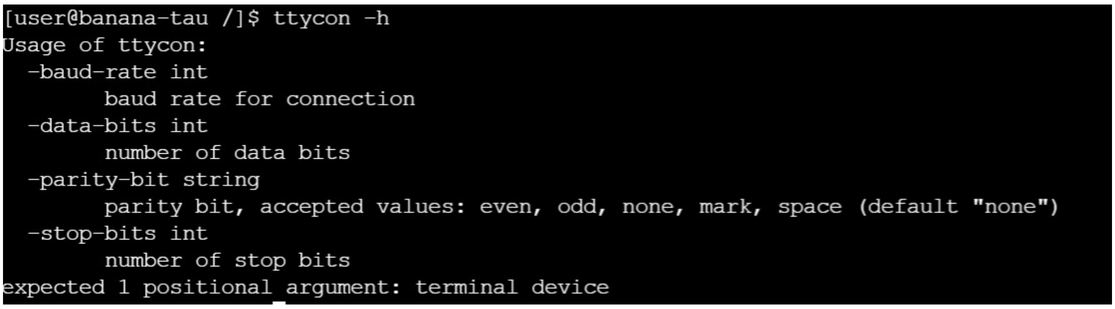


```
[user@banana-tau /]$ ttycon dev/ttyUSB0
ttycon>
:y�F���F��Q�
ttycon>
������E|_�7#��ttycon>
```

Note: as seen above, any other combination of connections will not work.

We realized that something is right because we got some kind of response but it should be better than that.

'ttycon -h' gave the possible flags that can be attached to this command.



```
[user@banana-tau /]$ ttycon -h
Usage of ttycon:
  -baud-rate int
        baud rate for connection
  -data-bits int
        number of data bits
  -parity-bit string
        parity bit, accepted values: even, odd, none, mark, space (default "none")
  -stop-bits int
        number of stop bits
expected 1 positional argument: terminal device
```

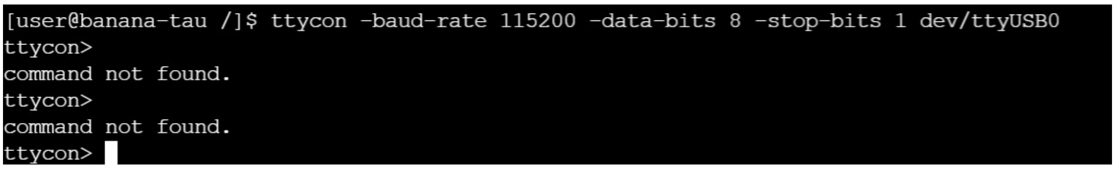
We had to figure out the right way of using the flags, so we turned to another Google search.

In that search we understood that 'ttycon' is a made-up command but the flags are genuine.

Found this:

```
tio --baudrate 115200 --databits 8 --flow none --stopbits 1 --parity none /dev/ttyS0
```

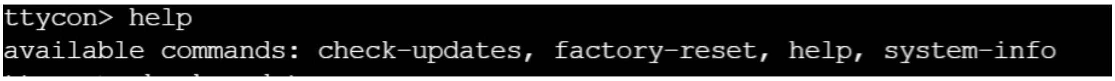
And wanted to see the output after pressing 'Enter' along with the right values of the flags.



```
[user@banana-tau /]$ ttycon -baud-rate 115200 -data-bits 8 -stop-bits 1 dev/ttyUSB0
ttycon>
command not found.
ttycon>
command not found.
ttycon>
```

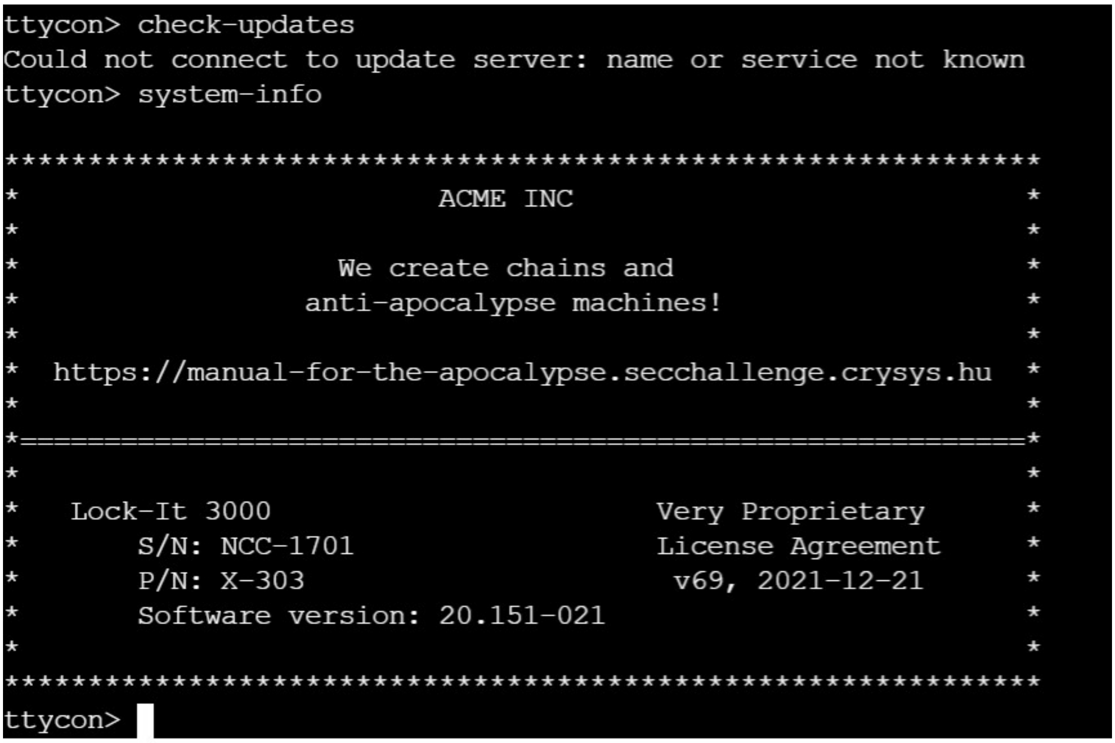
The behavior now is different then before and we had to learn more about our options.

Typed in 'help' and got:



```
ttycon> help
available commands: check-updates, factory-reset, help, system-info
```

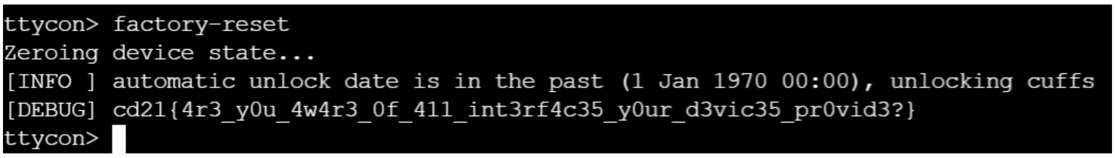
Tried all the options:



```
ttycon> check-updates
Could not connect to update server: name or service not known
ttycon> system-info

**************************************************************
*                         ACME INC                           *
*                                                            *
*                   We create chains and                     *
*                 anti-apocalypse machines!                  *
*                                                            *
*  https://manual-for-the-apocalypse.secchallenge.crysys.hu  *
*                                                            *
*============================================================*
*                                                            *
*   Lock-It 3000                       Very Proprietary      *
*       S/N: NCC-1701                  License Agreement     *
*       P/N: X-303                      v69, 2021-12-21      *
*       Software version: 20.151-021                         *
*                                                            *
**************************************************************
ttycon>
```

And the only option that left (and the "scariest") gave us our reward!



```
ttycon> factory-reset
Zeroing device state...
[INFO ] automatic unlock date is in the past (1 Jan 1970 00:00), unlocking cuffs
[DEBUG] cd21{4r3_y0u_4w4r3_0f_411_int3rf4c35_y0ur_d3vic35_pr0vid3?}
ttycon>
```