KEYBOARD COWBOYS

HERDING SHELLS

$(WHOAMI)

- Eldar Marcussen
- @Wireghoul
- Pentester
- CREST Assessor
- Bug hunter
- Trainer
- http://www.justanotherhacker.com

HackLabs

INTRODUCTION

- TALK ABOUT KEYBOARDS
- TALK ABOUT SOME BUGS
- LOTS OF DEMOS

HackLabs

BACKGROUND

04 DEC 12 ATM Thieves Swap Security Camera for Keyboard

This blog has featured stories about a vast array of impressive, high-tech devices used to steal money from automated teller machines (ATMs). But every so often thieves think up an innovation that makes all of the current ATM skimmers look like child's play. Case in point: Authorities in Brazil have arrested a man who allegedly stole more than USD $41,000 from an ATM after swapping its security camera with a portable keyboard that let him hack the cash machine.

The story comes from O Estado de S. Paulo (*"The State of São Paulo"*), a daily newspaper in Brazil's largest city. According to the paper, late last month a crook approached an ATM at the **Bank of Brazil** and somehow removed the security camera from the machine. Apparently, the camera was a USB-based device, because the thief then was able to insert his own USB stick into the slot previously occupied by the camera. As you can imagine, a scene straight out of Terminator 2 ensued.

Photo: TV Bahia

HackLabs

BACKGROUND

- Suitable targets for these attacks
  - Board room AV control
  - Various kiosks
  - Restricted/Hardened environments
  - ATM
  - Voting machines
- USB ports hidden behind wafer locks

HackLabs

KEYBOARDS

“KEYBOARD”

HackLabs

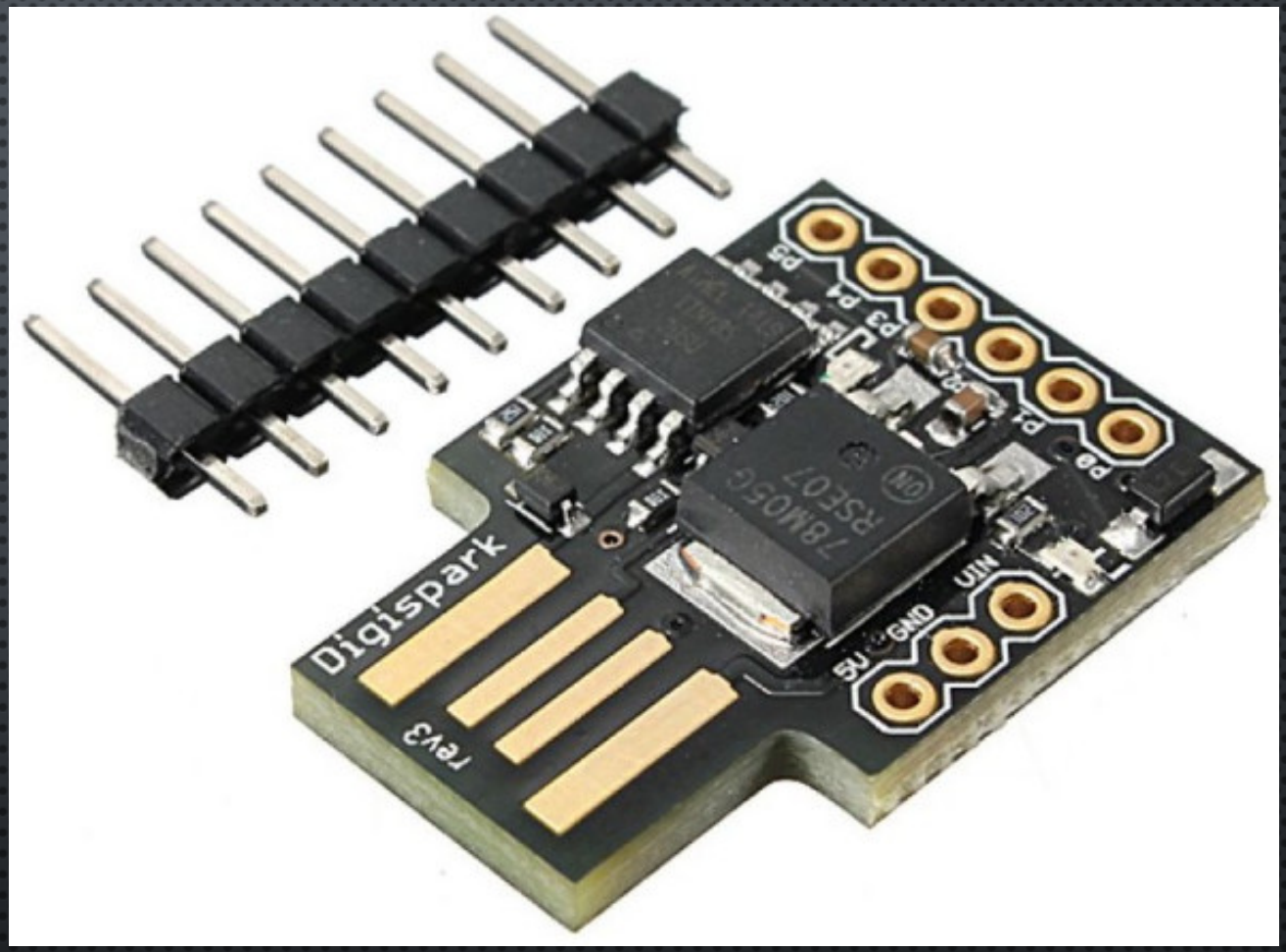
“KEYBOARD”

HackLabs

“KEYBOARD”

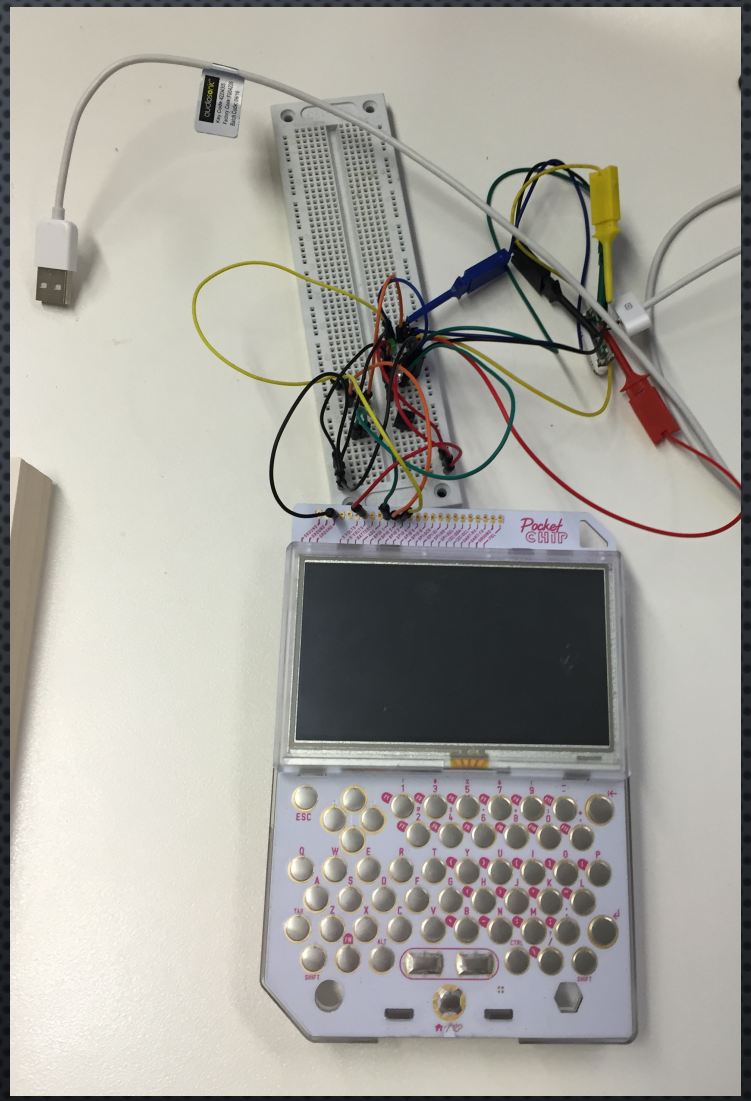
HackLabs

“KEYBOARD”



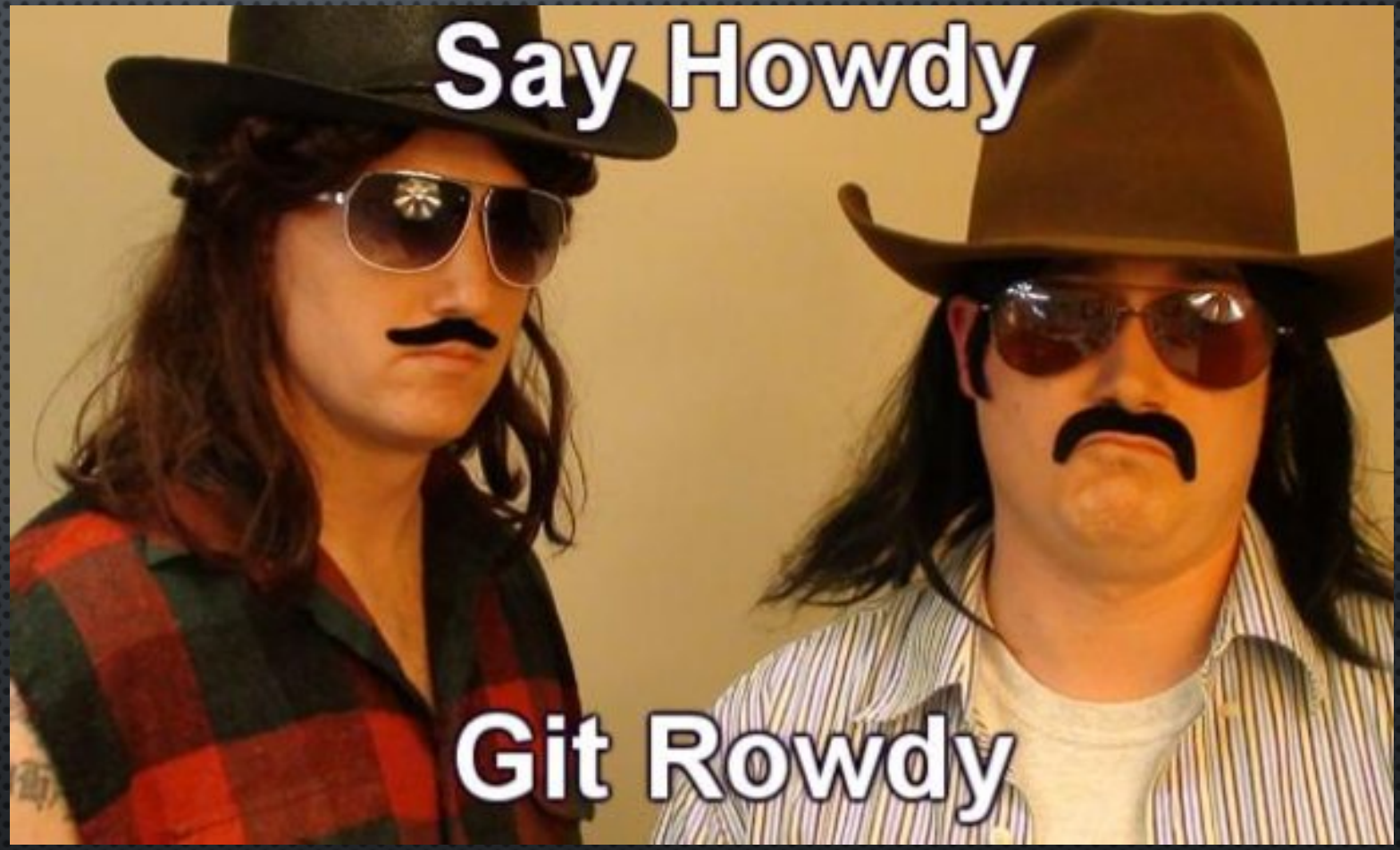
HackLabs

“KEYBOARD”



HackLabs

“COWBOYS”



HackLabs

WINDOWS

HackLabs

USEFUL KEYS

- F1 – Help
- CTRL+ESC – Start menu
- CTRL+SHIFT+ESC – Task manager
- TAB/SHIFT+TAB – Next/Previous item
- CTRL+TAB/CTRL+SHIFT+TAB Next/Previous window/tab
- F6 – Change panel (sometimes)
- SHIFT+F10 – Right click

USEFUL KEYS

- **BIG** LIST OF SHORTCUT KEYS:
- HTTPS://SUPPORT.MICROSOFT.COM/EN-GB/HELP/126449/KEYBOARD-SHORTCUTS-FOR-WINDOWS

WINDOWS "KIOSKAMI CODE" (WIN XP/7)

- CTRL+ESC
- ESC
- SHIFT+TAB
- DOWN
- ENTER

DEMO

I'M REALLY OBSESSED WITH THE F1 KEY ON MY KEYBOARD. I'M TRYING TO GET HELP

HackLabs

FROM $APP TO SHELL

- Ctrl+o to open file dialog
- Type 'c:\windows\system32\' => Enter
- Type '*.*' => Enter
- Shift+tab x2
- Press c,m,d
- Shift+F10
- Down arrow x2 => Enter

HackLabs

DEMO

I LOVE PRESSING THE F5 KEY. IT'S REFRESHING.

HackLabs

Considerations

- Can be automated
- Works even if the start menu/taskbar is hidden or suppressed

HP THIN CLIENT

HackLabs

HackLabs

PLAY ALONG AT HOME

- WGET FTP://FTP.HP.COM/PUB/TCDEBIAN/IMAGES/T6X44017.DD.GZ
- QEMU-IMG CONVERT -F RAW -O VMDK T6X43101.DD THINPRO.VMDK
- CREATE A VM WHICH USES THINPRO.VMDK

THANKS TO ROBERTO SUGGI (@MALERISH)

HTTP://BLOG.MALERISCH.NET/2015/04/PWNING-HP-THIN-CLIENT.HTML

HackLabs

LETS POP SOME ROOT SHELLS

STEALING THE ROOT KEYS

- RUN DIAGNOSTICS
- SAVE TO USB DRIVE
- EXTRACT ON ANOTHER COMPUTER
- CRACK ROOT PASSWORD FROM /ETC/SHADOW IN THE TAR.GZ

DEMO

Just can't get away from my broken keyboard. There's no escape

Escaping from Firefox

- In firefox:
- Press ctrl+p
- Tab down to the print command
- Change 'lpr' to 'xterm'
- Click print

DEMO

Did you hear about the keyboard collector with anxiety issues?

He was ANSI all the time

HackLabs

RESET ROOT PASSWORD PRIVESC

- In xterm run 'hptc-security --unlock-root'
- Enter the new root password x2 in the popup box
- …
- Use 'su' with the new password to become root

DEMO

I DECIDED TO TAKE THE REALLY BIG KEY OFF MY KEYBOARD AND THROW IT AWAY

IT'S A WASTE OF SPACE

HackLabs

ROOT VIA VPN PRIVESC

- In xterm run 'hptc-network-mgr'
- Click the VPN tab
- Tick auto start
- Set type to PPTP
- For gateway enter ';xterm;echo'
- Enter anything for NT domain, user name and user password
- Press ok
- Wait for it ....
- Receive root shell

HackLabs

DEMO

Just put it on my 'Tab'

HackLabs

CONCLUSION

- PHYSICAL ACCESS FTW!
- CAN LOOK LEGITIMATE, WHICH IS HANDY FOR RED TEAM
- INJECTION FLAWS ARE EVERYWHERE
- SO ARE LOGIC BUGS
- THERE ARE MANY MORE WAYS THAN SHOWN HERE
- GO FIND SOME BUGS?

QUESTIONS?

- THANKS FOR LISTENING
- YOU'RE AWESOME

HackLabs