

50 ton of backdoors

Ulisses Castro - Co0L BSidesSP v10 Novembro/2014



about me

Ulisses Castro

<https://twitter.com/usscastro>

<http://ulissescastro.com>

<https://www.youtube.com/user/usscastro>

- Black magic security specialist
- Subversive thinker as “lifestyle”
- Hardening systems/apps as “jobstyle”
- Problem solver and pentester addictive
- +10 years pro experience
- Bla, bla, bla...

<http://br.linkedin.com/in/ulissescastro/>

A **ton** is a unit of **mass**, **volume**, **energy** or **power**.

[http://en.wikipedia.org/wiki/Ton_\(disambiguation\)](http://en.wikipedia.org/wiki/Ton_(disambiguation))

motivation

Pranks?

Intrusion detection?

Hardening?

(Un)ethical hacking?

Exploitation?

Reputation?

Incident response?

Because we can?



MOTIVATION


Some people need more than others...

PLEASE, don't blame me!

YES, next proof of concepts will be with ROOT user.

BUT, stick to the point and remember motivations!

**Upcoming slides will show you how dangerous “native”
Linux tools are and how we can own someone in a blink of
an eye!**



*“...Like many other Version Control Systems, Git has a way to fire off custom scripts when certain important actions occur. There are two groups of these hooks: client-side and server-side. Client-side hooks are triggered by operations such as committing and merging, while server-side hooks run on network operations such as receiving pushed commits. **You can use these hooks for all sorts of reasons...**”*

DEMO GIT HOOKS

<https://www.youtube.com/watch?v=rCVmWUf8x1E>



“...If set, the value is executed as a command prior to issuing each primary prompt...”

DEMO PROMPT_COMMAND

<https://www.youtube.com/watch?v=IM10kYBoKtg>



*“...It is possible to include other sudoers files from within the sudoers file currently being parsed using the **#include** and **#includedir** directives.....”*

Pound sign (#) as include character? Really?

DEMO SUDOERS

<https://www.youtube.com/watch?v=tkwEn7q0Cc0>



*“...If the first-matched access control rule contains a **shell command**, that command is subjected to %<letter> substitutions (expansions). The **result is executed by a /bin/sh** child process with standard input, output and error connected to /dev/null. Specify an `&` at the end of the command if you do not want to wait until it has completed...”*

DEMO TCP WRAPPERS

<https://www.youtube.com/watch?v=mOOZwodcm40>



*"...File and directory names may be relative or absolute. Absolute names are used directly. **Relative paths are looked for in the scripts of each of the following places***

until found: --datadir

\$NMAPDIR.

***~/nmap** (not searched on Windows).*

***HOME\AppData\Roaming\nmap** (only on Windows).*

the directory containing the nmap executable

the directory containing the nmap executable, followed by ../share/nmap

NMAPDATADIR.

the current directory..."

DEMO NMAP

<https://www.youtube.com/watch?v=bPaCfKc4Ow4>



*ProxyCommand, Specifies the **command** to use to connect to the server...*

DEMO SSH

<https://www.youtube.com/watch?v=byoCWf8SEZc>



*"...The Unicode character set contains many strongly homoglyphic characters. These **present security risks in a variety of situations...**" (Wikipedia)*

DEMO UNICODE HOMOGLYPHS

https://www.youtube.com/watch?v=Os0QKZgvE_I



"...List available WiFi access points. iface and bssid options can be used to get just APs for particular interface or specific AP, respectively...."

DEMO NETWORK-MANAGER

<https://www.youtube.com/watch?v=l6kRJbxzcV4>



deploy alternatives

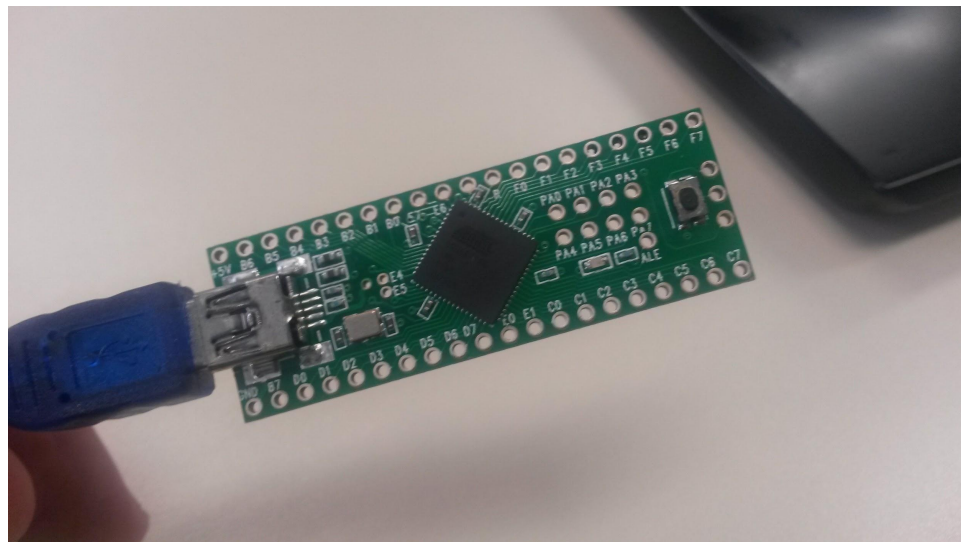
awk curl dig fetch host
iwconfig lynx netcat nmcli
nslookup ntpdate perl php
python ruby scp ssh teensy wget
yum

“teensyduino”

Act like a HID!

“The Teensy is a complete USB-based microcontroller development system, in a very small footprint (...)”

```
int count = 0;
void setup() { } // no setup needed
void loop() {
  Keyboard.print("Hello World ");
  Keyboard.println(count);
  count = count + 1;
  delay(5000);
}
```



<https://www.pjrc.com/teensy/>
https://www.pjrc.com/teensy/td_keyboard.html

DEMO TEENSY



github project

Linux Native Backdoors

<https://github.com/ulissescastro/linux-native-backdoors>

Check out ...

Backdoor demos

Native Linux backdoors cmds

This presentation

Code snippets

Fork it! ;-)



questions?

<http://blog.tendtudo.com.br/wp-content/uploads/2013/12/jpg>

QUESTIONS?



THANKS!

@usscastro // [uss.thebug \[a\] gmail.com](mailto:uss.thebug@gmail.com)

