

P4wnP1



Come trasformare un Pi Zero in una piattaforma di attacco

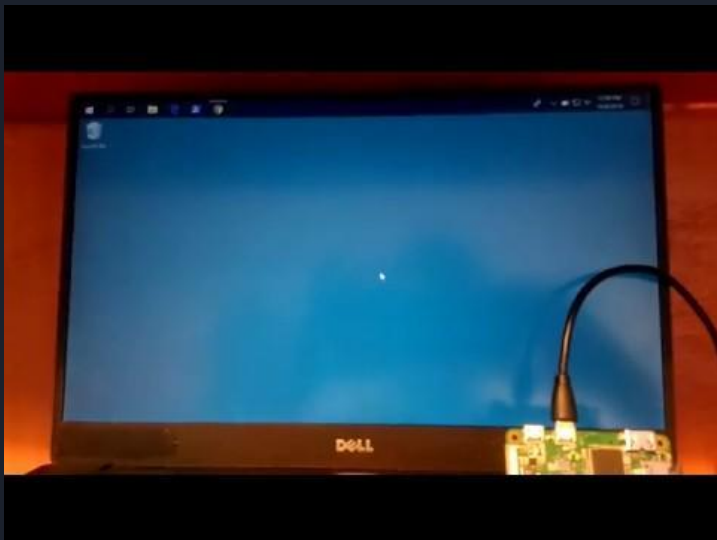


Requisiti

- **RPi Zero** (meglio il modello W) [NB: Tutti gli altri RPi *non* sono supportati]
- **MicroSD** con la pre-built image oppure Raspbian Stretch lite
- **Cavo micro USB** (evitare quelli charge-only) oppure saldate un connettore usb sul RPi

Totale ~= 15 euro

Features: il classico Keyboard HID



- ❑ Supporta **DuckyScripts**
- ❑ Scelta **layout tastiera** (it, en, us...)
- ❑ Payload attivato al KeyboardUp()
- ❑ Payload scritti in **BASH**
- ❑ Possibilità di attivare attacco tramite i led di CAPSLOCK, etc...

BUT

→ È lento (~23s di boot)



Features: oltre il classico Keyboard HID

Ma allora perché usare il P4wnP1?

- Possibilità di attivare i Payloads tramite **callbacks** (e.g. quando la vittima si collega ad internet)
- Payload HID remoti
- Simulare altri device (Mouse, USB Mass storage, CDC ECM, RNDIS)
- Customizzare Vendor ID e Product ID
- Batterie incluse: payload completi e template disponibili sin da subito
- Attacchi karma con nexmon
- Lockpicking di password deboli su Win10
- ...more



Piccolo Tour

Una volta fatto il git clone della repo il P4wnP1 crea tre canali per l'accesso:

1. Ethernet Over USB
2. Wifi
3. Bluetooth Pan

Una volta collegati troveremo il file `P4wnP1/setup.cfg` che è il file di configurazione principale.



Piccolo Tour: Setup.cfg

Il file contiene configurazioni globali che possono essere sovrascritte dai singoli payload.

Il file è diviso per sezioni, di cui le più interessanti sono:

USB setup: permette di scegliere il tipo di device da emulare

Wifi options: permette di attivare il driver Nexmon per attacchi KARMA (MITM) con supporto AP mentre si tiene una interfaccia di monitoring attiva

AutoSSH: permette di fare tunneling del server ssh del RPi ad uno remoto

...etc



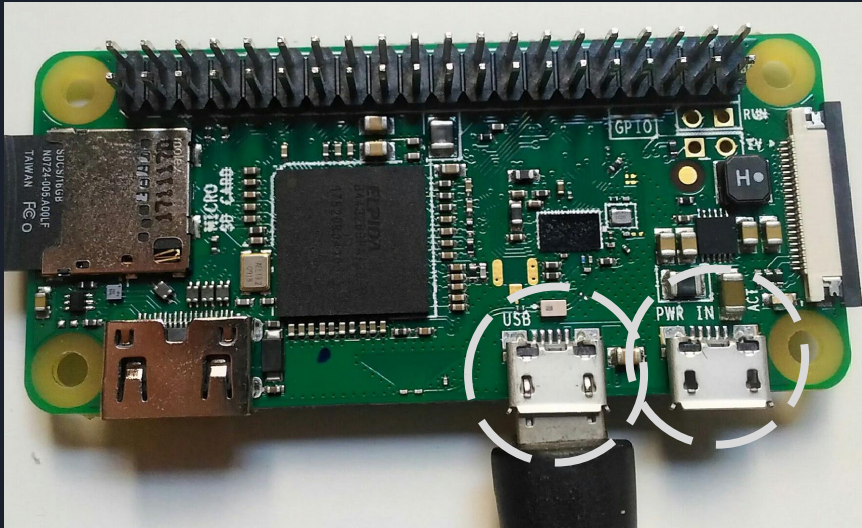
Piccolo Tour: i payloads

```
Win10_LockPicker.txt  
ciaomister.txt  
hakin9_tutorial  
hid_backdoor.txt  
hid_backdoor_remote.txt  
hid_frontdoor.txt  
hid_keyboard.txt  
hid_keyboard2.txt  
hid_keyboard_test.txt  
hid_mouse.txt  
network_only.txt  
nexmon  
stickykey  
template.txt  
wifi_connect.txt  
wifi_covert_channel
```

In fondo al file setup.cfg viene settata la variabile PAYLOAD con il path del file da eseguire.

Ci sono circa 15 payload/demo pronti per essere usati.

Come far partire i payloads



Modalità **“attack + remote access”** se il cavo è collegato alla porta **“USB”**

Modalità **“remote access only”** se il cavo è collegato alla porta **“PWR”**




Demo: Keyboard hid con triggers

Come già spiegato il tempo di boot non permette di essere efficaci per attacchi 'mordi e fuggi'.

Possiamo però agire in due fasi:

1. Colleghiamo di nascosto il P4wnP1 ad una porta usb.
2. In un secondo momento attiviamo il payload premendo velocemente il tasto CapsLock

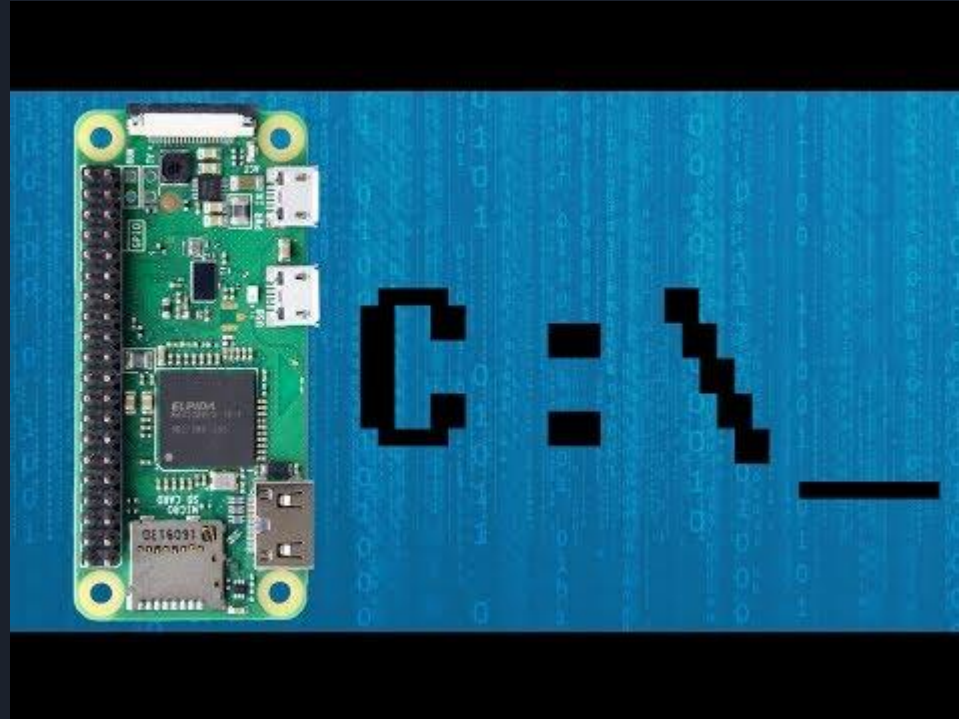


BRACE YOURSELVES



LIVE DEMO IS COMING

Demo: Hid Backdoor

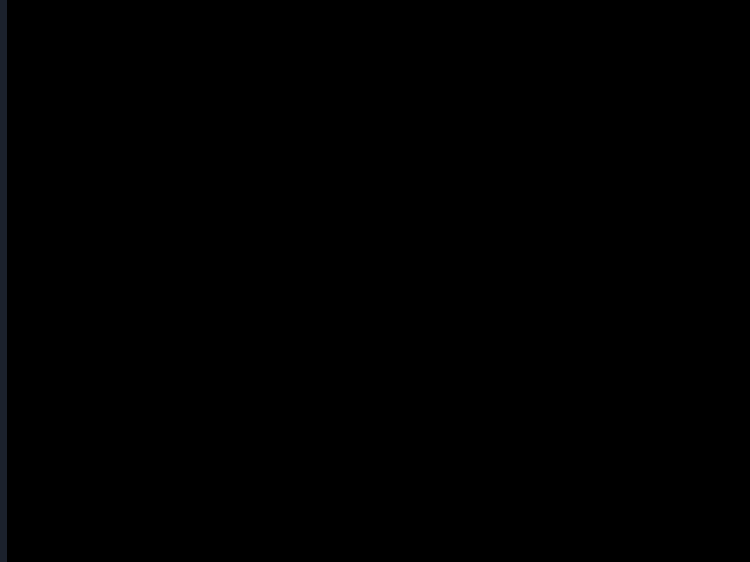


Demo: Wifi Covert Channel





Demo: Windows password hashes





Demo: Windows password hashes

```
pi@MAME82-P4WNP1:~/P4wnP1 $ cd collected/  
pi@MAME82-P4WNP1:~/P4wnP1/collected $ 1  
-bash: 1: command not found  
pi@MAME82-P4WNP1:~/P4wnP1/collected $ ls  
DESKTOP-BNMGU8O_172.16.0.2_0.hashes  DESKTOP-BNMGU8O_172.16.0.2_2.hashes  
DESKTOP-BNMGU8O_172.16.0.2_1.hashes  DESKTOP-BNMGU8O_172.16.0.2_3.hashes
```

Adesso “basta” fare reverse delle hash, per esempio con hashcat



Altre features

Le possibilità sono tante, per esempio:

- ❑ Payload per ottenere credenziali salvate nei browsers
- ❑ Fake Wifi hotspot
- ❑ Simulare device usb
- ❑ Attacchi Bluetooth
- ❑ ...etc