WHID

Injector

Ressa F.

Sono Francesco Ressa mi occupo di informatica dal 1990.

- Presidente di bit01
- Certificato Linux Essentials
- Teacher abilitato da LPI
- Moderatore di Ethical Hacker Italiani la più grande community italiana di hacking
- Sono un libero professionista e collaboro con aziende di cyber security

- Non inserire nei vostri dispositivi chiavette usb “trovate casualmente”.
- Diffidare da chi vi “regala” qualche oggetto usb senza un plausibile motivo.
- Non fare accedere fisicamente, se non in vostra presenza, al vostro dispositivo.
- Inserire una password di accesso al vostro PC.

Gli attacchi informatici

ESPERIMENTO SOCIALE

Linux Day 2022

2016

300

135

45%

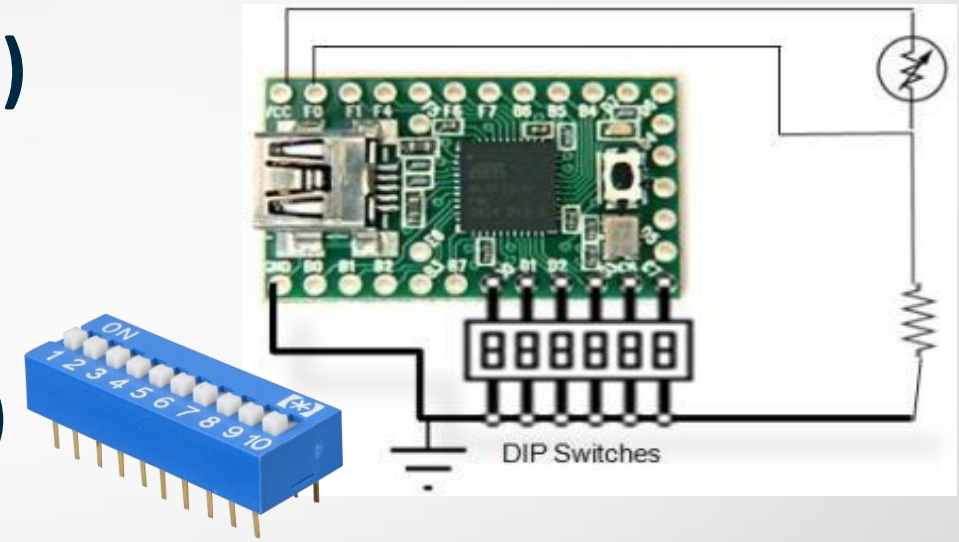
=

PAYLOAD

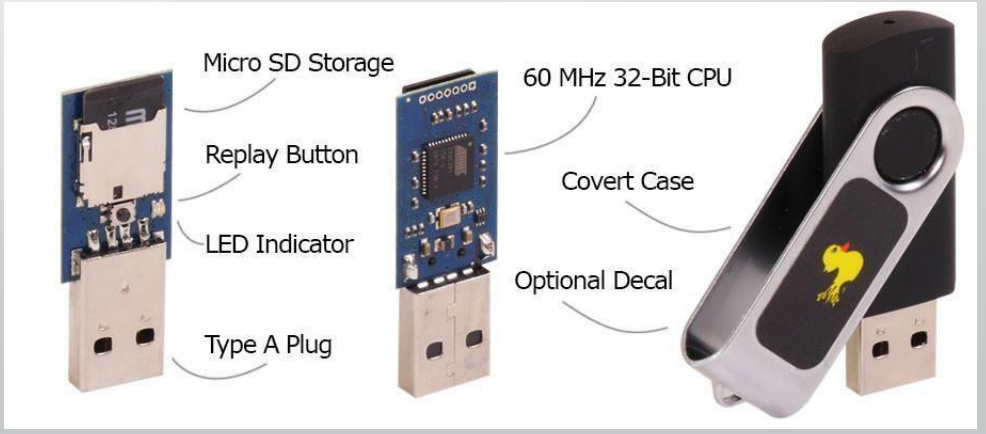
Quell'insieme di azioni che vengono eseguite dopo aver infettato o essere penetrati in un sistema.

Offensive Devices – 1st Generation

- **Teensy – (PHUKD 2009 & Kautilya 2011)**
  - DIY Solution
  - Multiplatform (Win, *nix, OSX)
  - Multipayload (through DIP-Switches)



- **Rubberducky (2010)**
  - Dedicated Hardware
  - Multiplatform (Win, *nix, OSX)
  - Can emulate Keyboard & USB Disk
  - Changeable VID/PID
  - Multipayload (CAPS-INS-NUM)



Piccolo approfondimento sulla Rubberducky

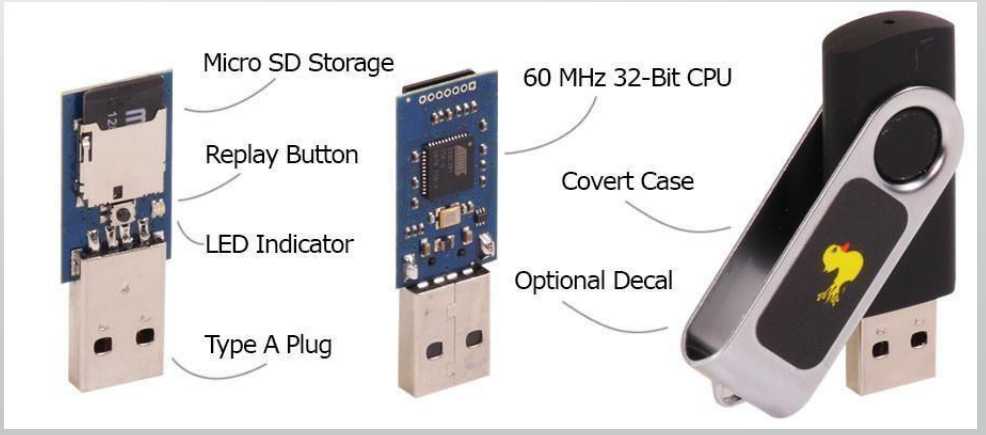
Rubberducky (2010)

inject.bin - payload predefinito (verrà sempre eseguito per primo)

inject2.bin - NUM_LOCK

inject3.bin - CAPS_LOCK

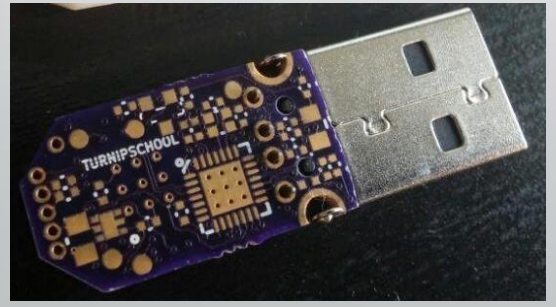
inject4.bin – INS



Offensive Devices – 2nd Generation

- **BadUSB (2014)**
  - It exploits the controllers within commercial USB devices and turns them into a covert keystrokes injecting device.

- **TURNIPSCHOOL (2015)**
  - Is a hardware implant concealed in a USB cable. It provides short range RF communication capability to software running on the host computer. Alternatively it could serve as a custom USB device under radio control.

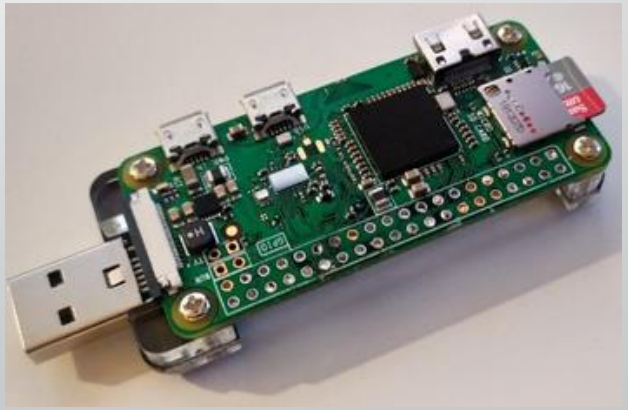


Offensive Devices – 3rd Generation

Linux Day 2022

- **WHID Injector (2017) – A Rubberducky evolution**
  - Dedicated Hardware
  - Open source
  - Multiplatform (Win, *nix, OSX)
  - Changeable VID/PID
  - Has WiFi and USB

- **P4wnP1 (2017)– A Bash Bunny on Steroids**
  - Based on RPi Zero W (~15 €)
  - Has WiFi and USB
  - It can emulate USB Key FileSystem
  - Changeable VID/PID
  - NexMon WiFi Drivers
  - Next Gen AirGap bypass



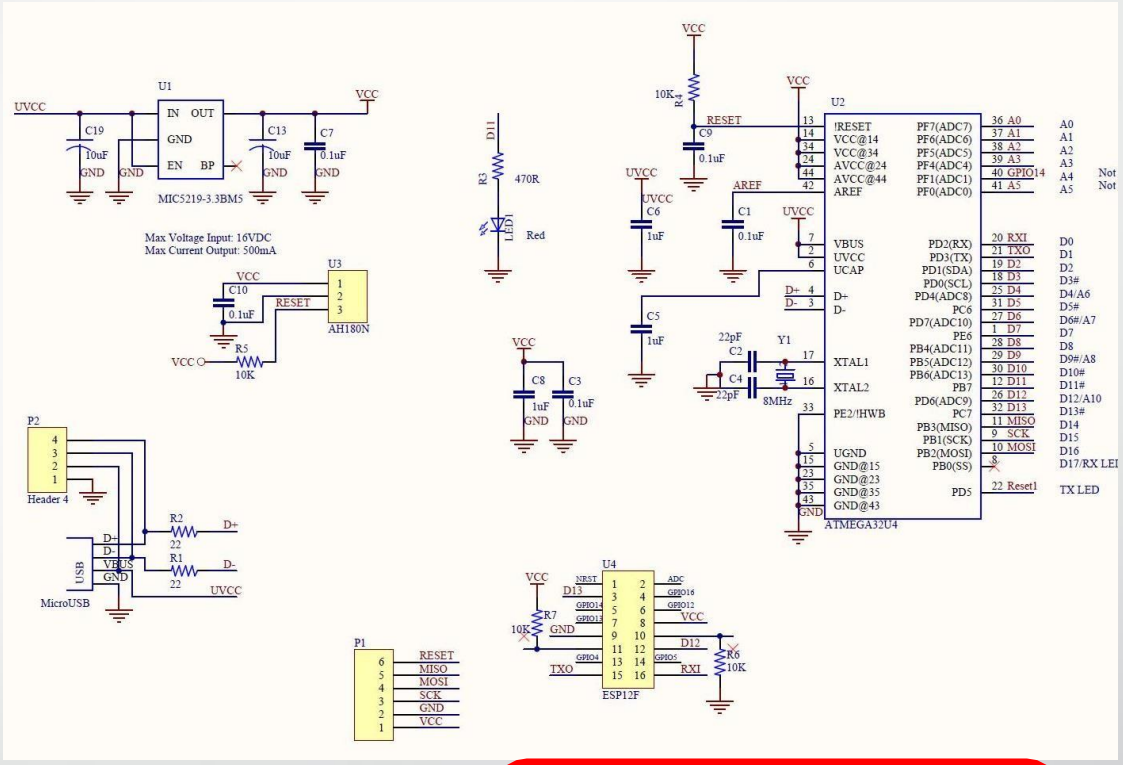
Ressa F.

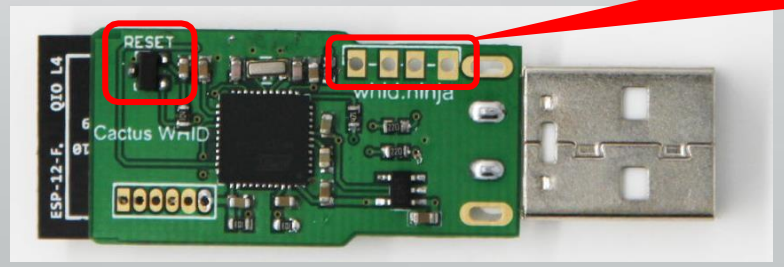
WHID Injector – Schematics & Specs

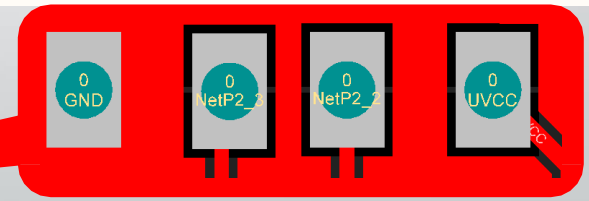
Linux Day 2022

- **Atmega 32u4**
  - Arduino-friendly
- **ESP-12**
  - WiFi (both AP and Client modes)
  - TCP/IP
  - 4MB Flash

- **Pinout for weaponizing USB gadgets**
- **HALL Sensor for easy unbrick**



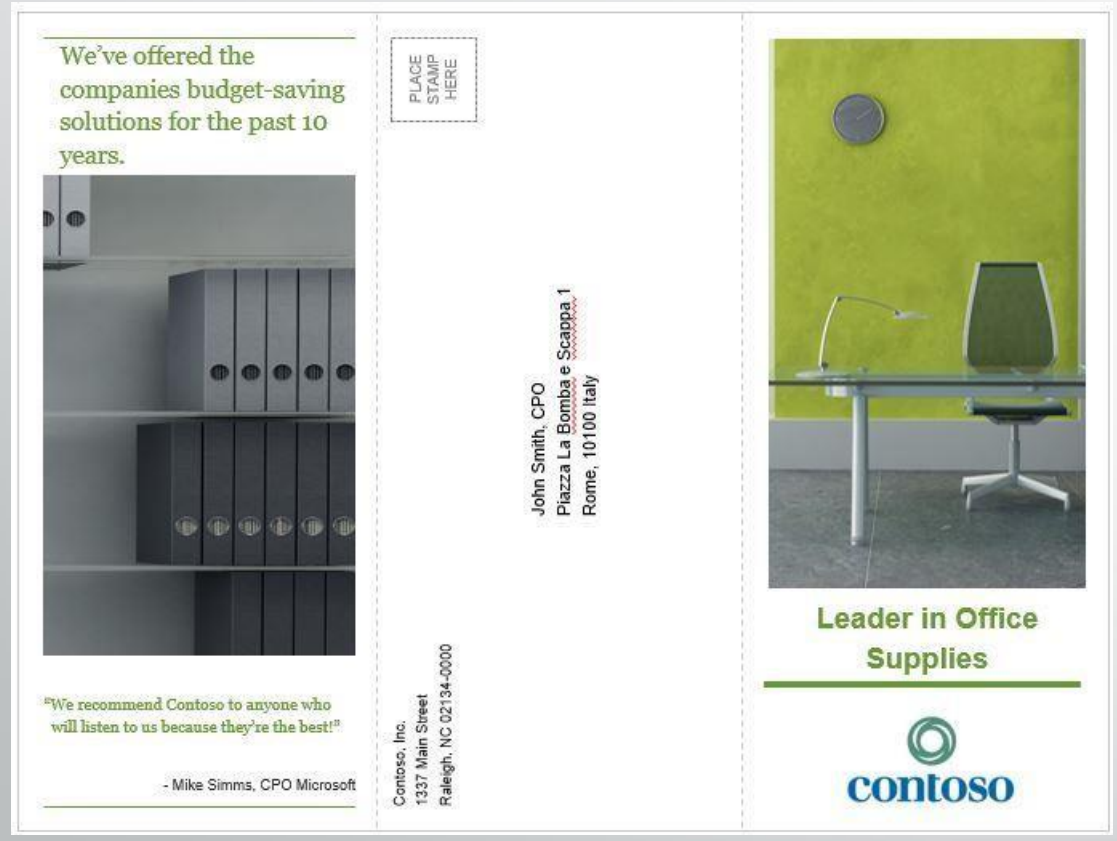




Ressa F.

Weaponizing USB Gadgets

Weaponizing USB Gadgets



Ressa F.

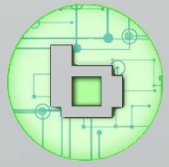
Cos'è?

- WHID Injector usb è, detto in parole semplici, una Rubber duck di Hak5 con connessione Wi-Fi, quindi più evoluta.
- In pratica è una chiavetta USB che utilizza un modulo WiFi ESP-12S con una connessione ad un microcontrollore 32u4.
- Questo dispositivo consente l'invio di sequenze di tasti e script interattivi tramite WiFi a una macchina di destinazione, e quindi compie delle azioni nel pc della vittima
- Il dispositivo ha 4 MB (ne possiamo utilizzare fino a 3) di memoria flash che servono sia a memorizzare il firmware sia payload.
- Quando viene inserita in un pc esso la rileva come Tastiera HID.

Human Interface Devices

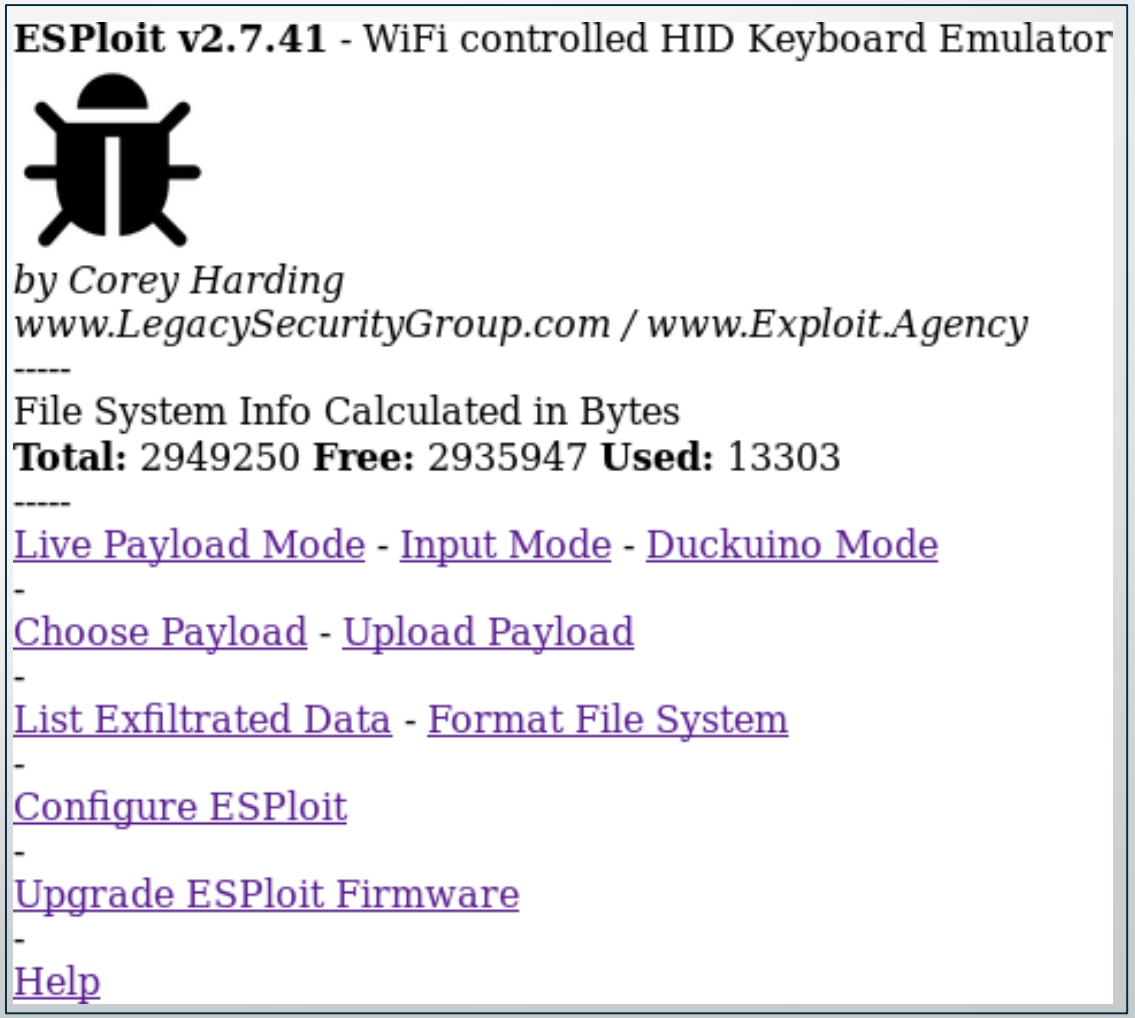
"A **human interface device** or **HID** is a type of computer device usually used by humans and takes input and gives output to humans." – Wikipedia

- Keyboard, Mouse, Game Controllers, Drawing tablets, etc.
- Most of the times don't need external drivers to operate
- Usually whitelisted tools DLP
- Not detected by Antiviruses

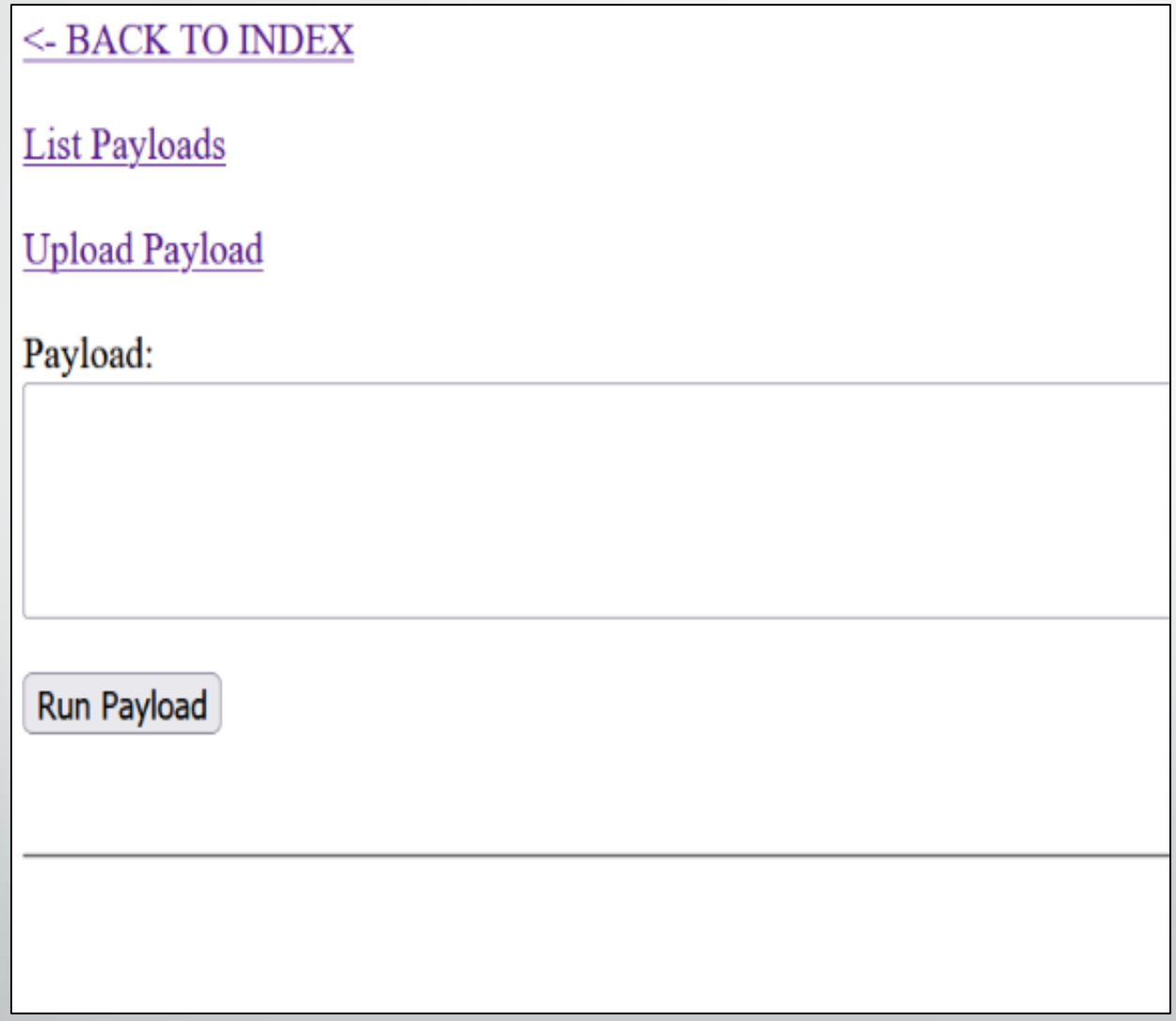


Software Frameworks – ESPloitV2 GUI

Si controlla con interfaccia web



Live payload mode



Input mode

<- BACK TO INDEX

InputMode

Note: On configuaration page set "Delay Before Starting a Live Payload:" to "0" under "Payload Settings:" to avoid a delay when using Input Mode.

Print:

Send Text

Mouse Up Left Click Left Click Right Down Right Click

ArrowKeys Up Left Enter Right Down

Tab Alt+Tab Shift+Tab

PrintLine:

Send Text+Enter

Function Keys: F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12

Misc Keys: ESC HOME END INSERT DEL BACKSPACE SPACE BAR PAGE UP PAGE DOWN

Win: GUI-Key GUI+r cmd+EnterKey osk+EnterKey Alt+F4 Ctrl+Alt+Del Ctrl+Shift+Esc

Mac: Right of Left Shift Key, z Left of Right Shift Key, /

Linux: Alt+F2, Application Finder gnome-terminal+EnterKey CTRL+c CTRL+x

Bios: F1 F2 F8 F12 DEL ESC

Duckuino Mode

Linux Day 2022

<- BACK Convert Run Payload

```
DELAY 750
GUI r
DELAY 1000
STRING powershell Start-Process notepad -Verb runAs
ENTER
```

```
CustomDelay:750
Press:131+114
CustomDelay:1000
Print:powershell Start-Process notepad -Verb runAs
Press:176
```

i - Done parsed 6 lines in 2ms

Choose Payload

<- BACK TO INDEX

File System Info Calculated in Bytes
Total: 2949250 **Free:** 2919381 **Used:** 29869

Upload Payload

Live Payload Mode

Display Payload Contents	Size in Bytes	Run Payload	Download File	Delete Payload
/payloads/inject.bin	106	Run Payload	Download File	Delete Payload
/payloads/infomation.bin	9982	Run Payload	Download File	Delete Payload
/payloads/information.txt	6217	Run Payload	Download File	Delete Payload
/payloads/duck_text.txt	7912	Run Payload	Download File	Delete Payload
/payloads/prova2.txt	100	Run Payload	Download File	Delete Payload
/payloads/pay.txt	1479	Run Payload	Download File	Delete Payload

Upload Payload

<- BACK TO INDEX

List Payloads

Live Payload Mode

Upload Payload:

Sfoglia... Nessun file selezionato. Upload

Format File System

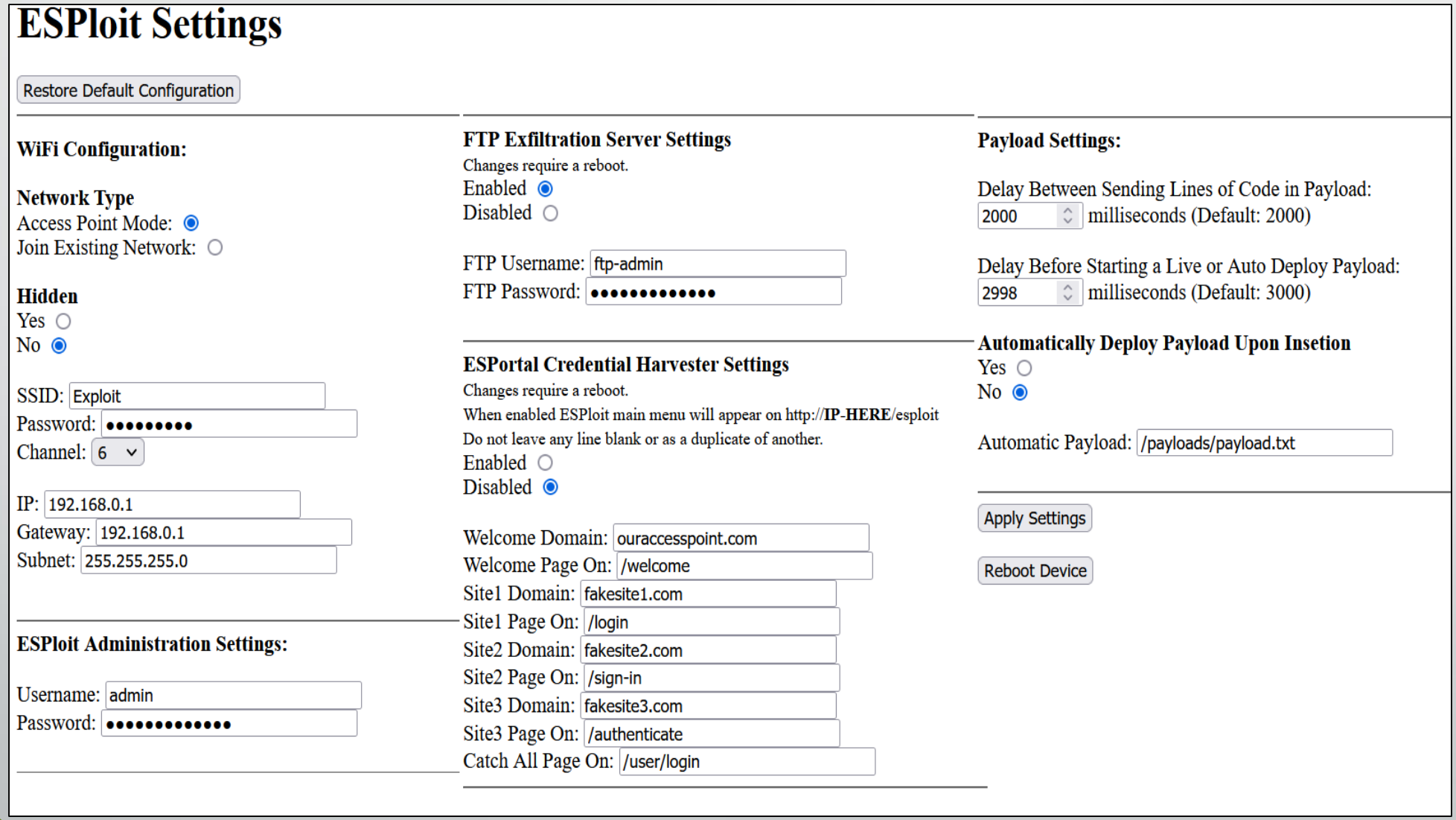
<- BACK TO INDEX

This will reformat the SPIFFS File System.

Are you sure?

YES - NO

Configure ESPloit



Oggi vedremo in azione quest'oggetto con vari payload

- Esfiltrazione credenziali social in particolare Facebook
- Spegnimento schede di rete su pc vittima
- Disabilitare antivirus del pc vittima
- Svuotamento cestino del pc vittima
- Ottenere informazioni sul pc vittima

Grazie