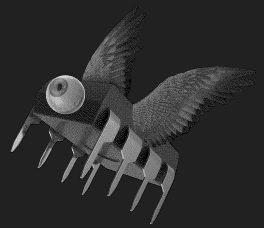
USB Attack Workshop

Soldering Skills & Basic Keystroke Injection Attacks

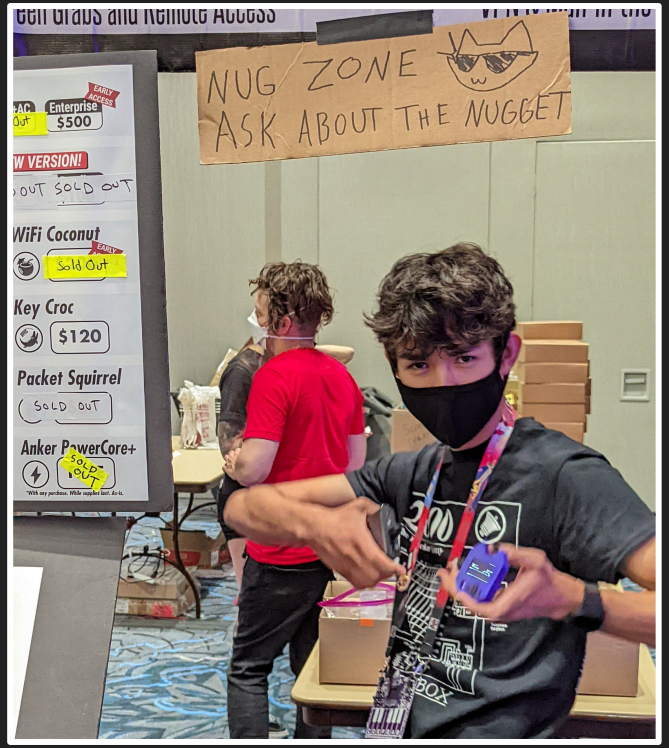


[Alex Lynd @ Open Hardware Summit]
Alex Lynd 04/28/2023

My Work

- **Hardware Hacker** - IOT & Wireless Security
- **Content Creator -** Hacking Tutorials @ Hak5
- **Instructor** - I teach & host workshops and stuff

alexlynd.com • lyndlabs.io



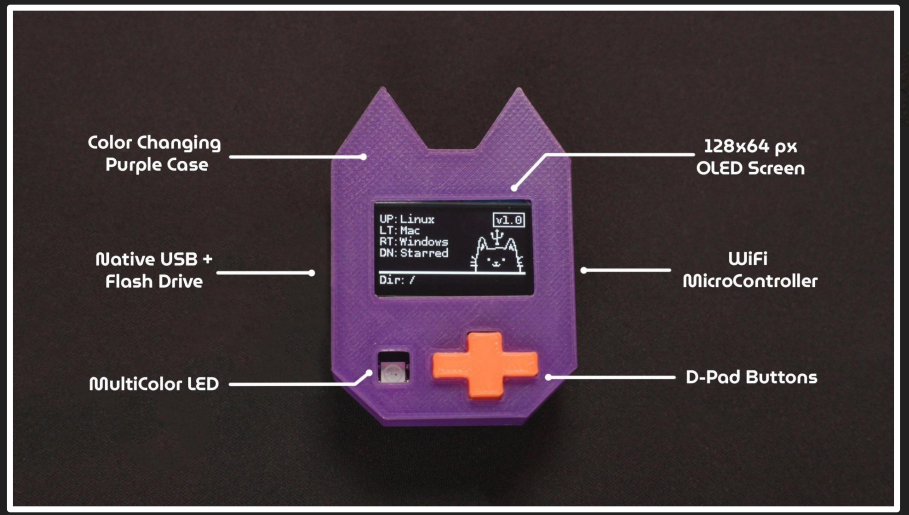
What we're doing today

- 🖥️ Learning about USB attacks: methods & tools
- 🐱 Soldering your own USB Nugget
- ⌨️ Writing keystroke injection scripts!

What is the Nugget?

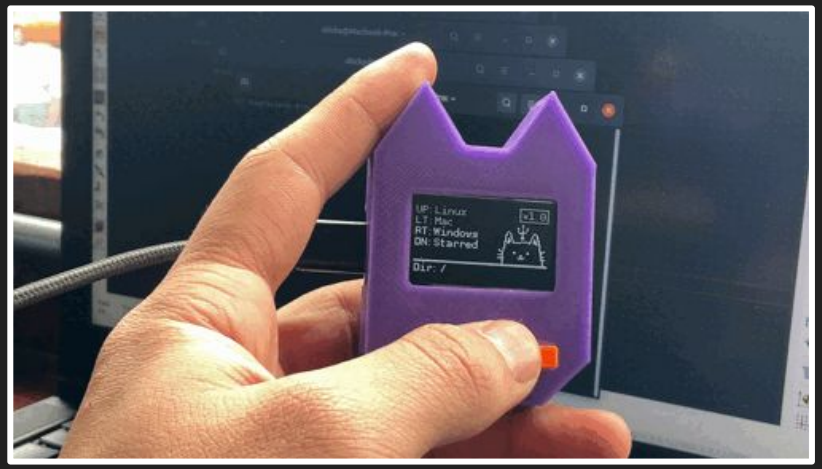
The Nugget is a cat-themed console that makes it fun to learn hacking!

- Hardware Prototypes
- CircuitPython
- WiFi Hacking
- USB Hacking



What is the USB Nugget?

- **Run USB Attacks**
- **Emulate Keyboards & More**



Features:

- DuckyScript
- LED & Screen Feedback
- Flash Drive
- WiFi Interface

What's under the hood?

The USB Nugget is powered by the **ESP32-S2** microcontroller which offers:

- **WiFi** (AP & Client mode)
- **Native USB**
  - Emulate USB Devices
  - Flash Storage
- **Easy Hardware Expansion**

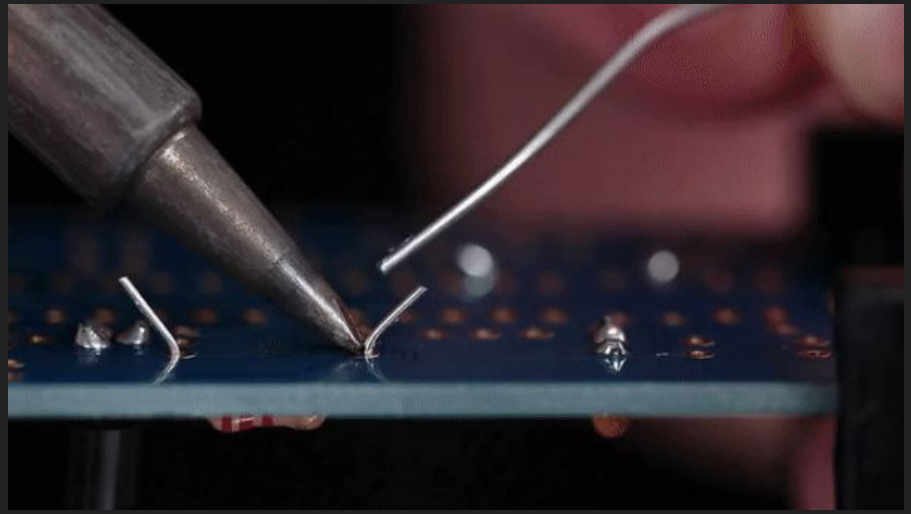
Soldering Skills Class

1 Hour - Build your own USB Nugget!

What is Soldering?

Soldering is an assembly technique that lets us mount components on circuit boards.

- **Solder** is used to attach components to the PCB.
- A **soldering iron** is used to heat up the circuit board *and* the components at the same time.
- Solder hardens and lets us create a stable electrical connection.



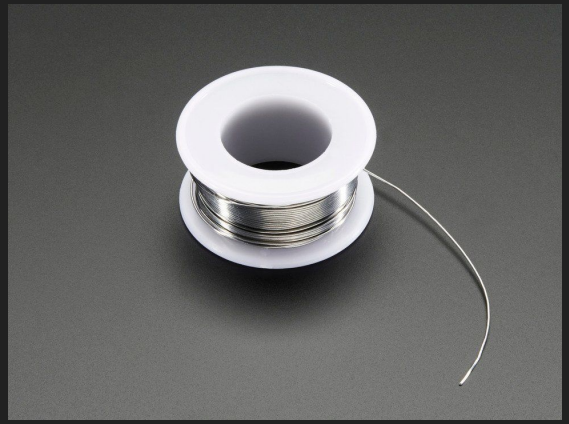
Soldering through hole components

Common Soldering Tools

Soldering Iron

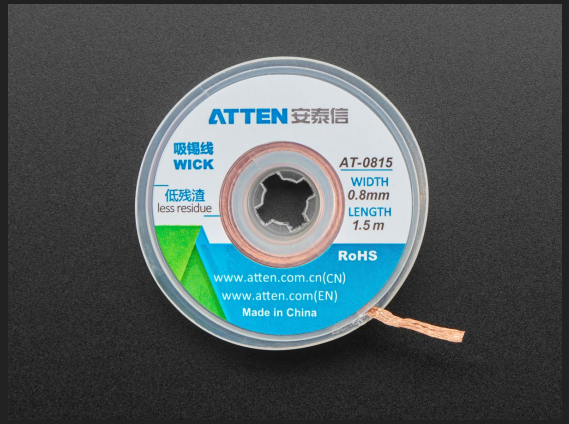
Solder Sucker *(for screw-ups)*

Soldering Materials



Solder

Solder Flux



Solder Wick

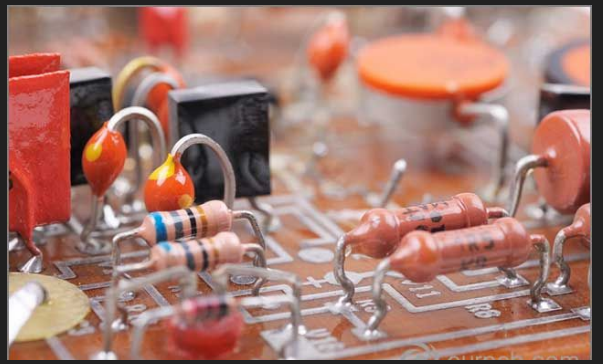
Soldering techniques

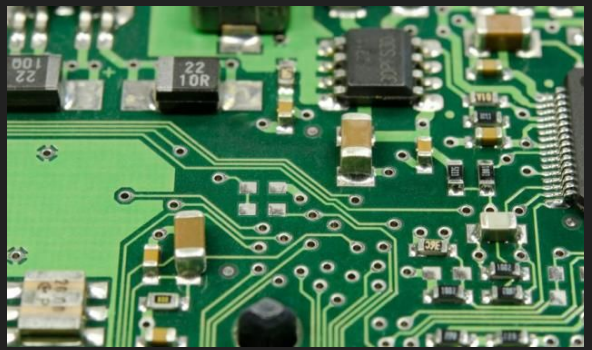
Through-Hole (THT)

- Hand Assembly
- Big Components

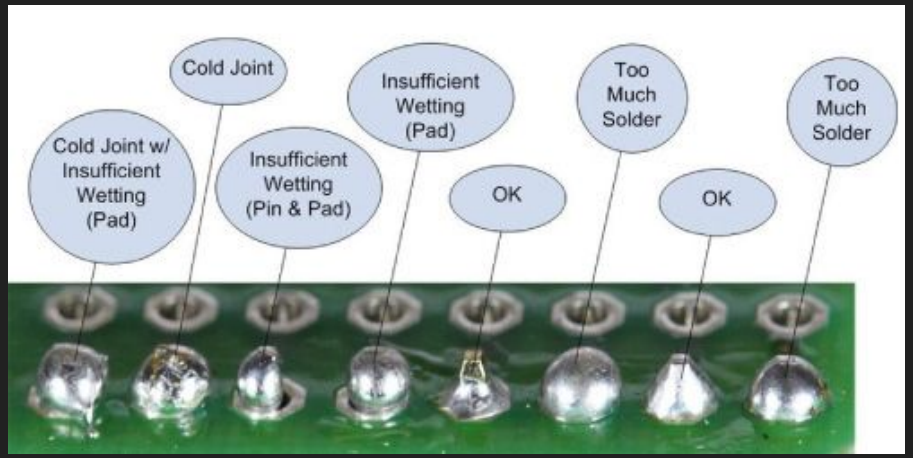
Surface Mount (SMD)

- Cheaper
- Easier for machines

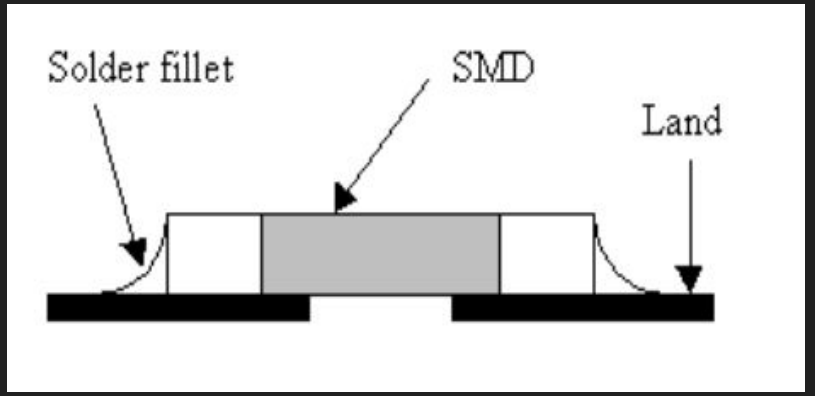




Good solder joints

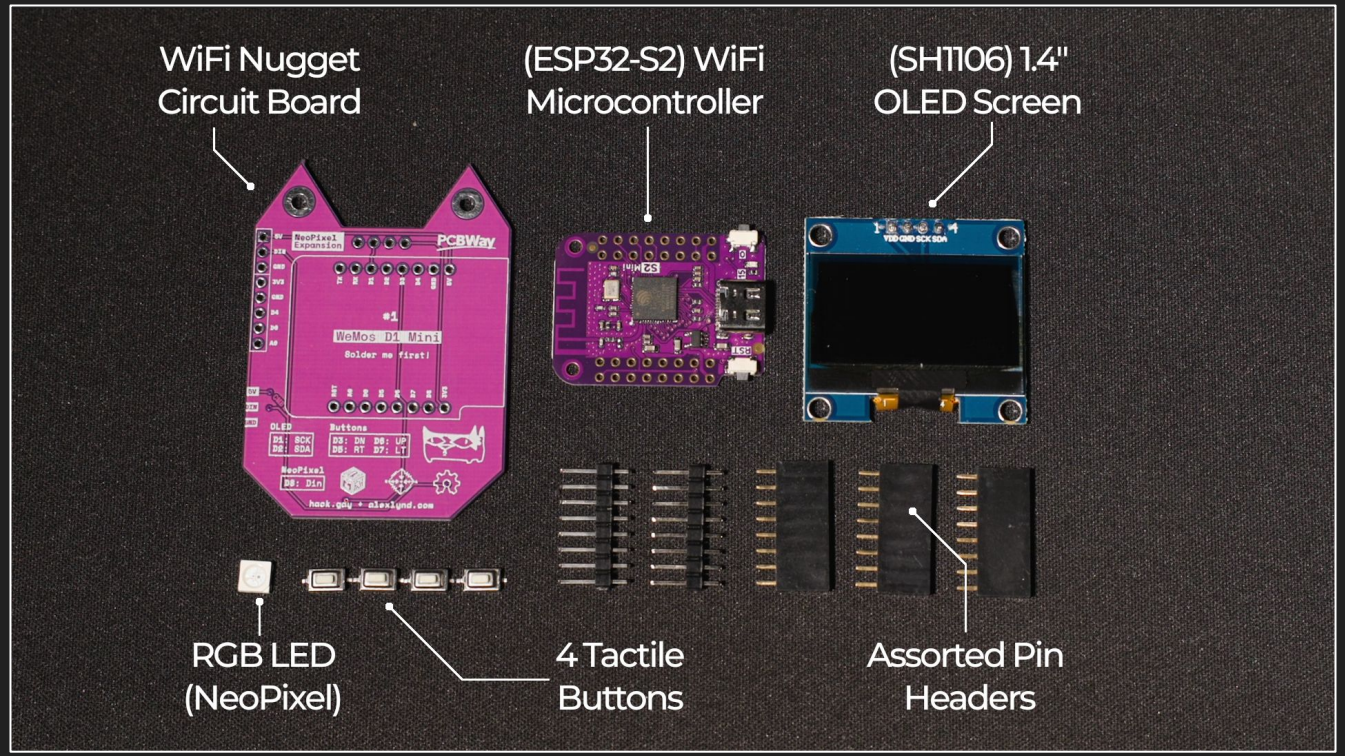


Through-hole joints

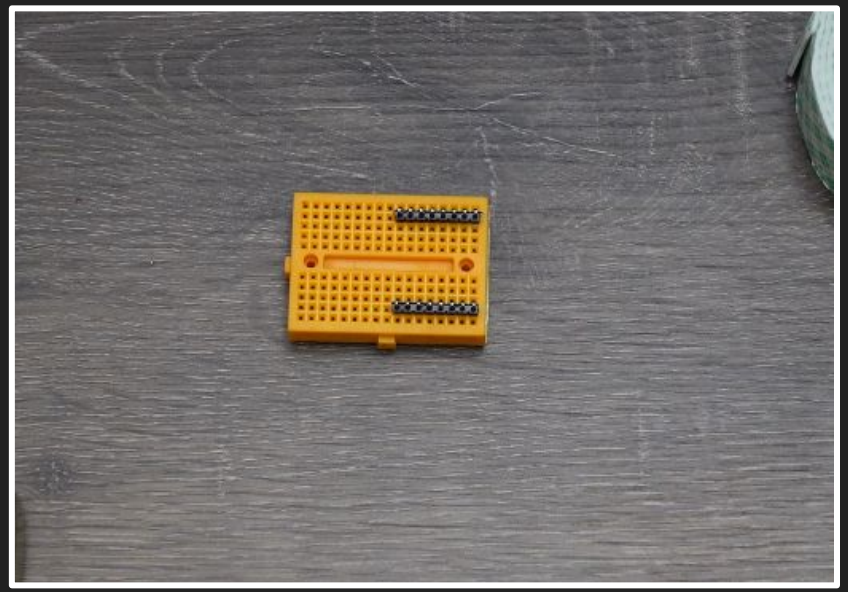


Surface mount pads

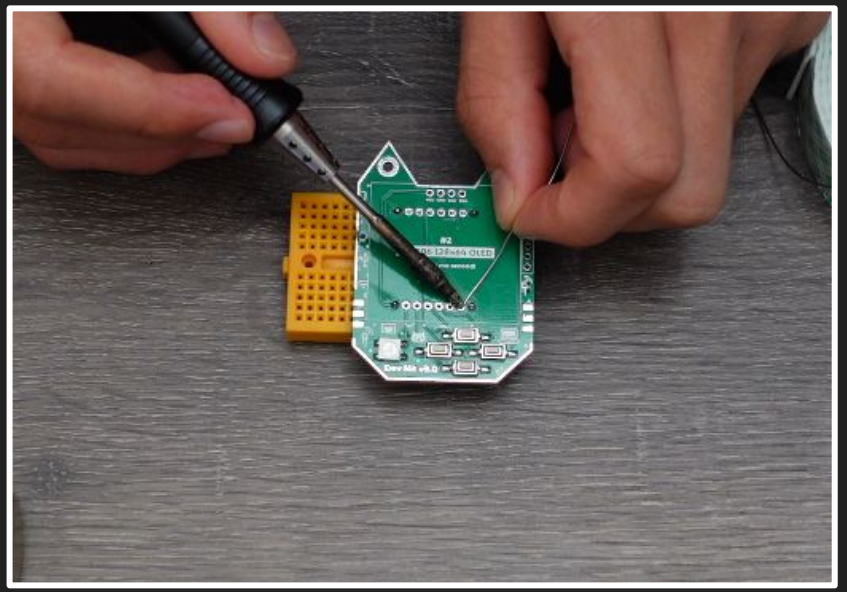
What's in your Nugget Kit



1. Prep the Headers

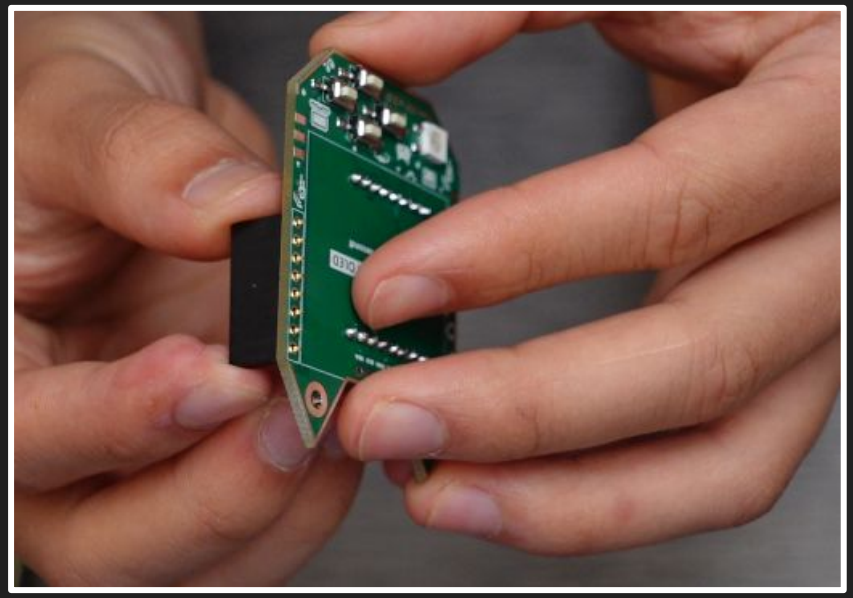


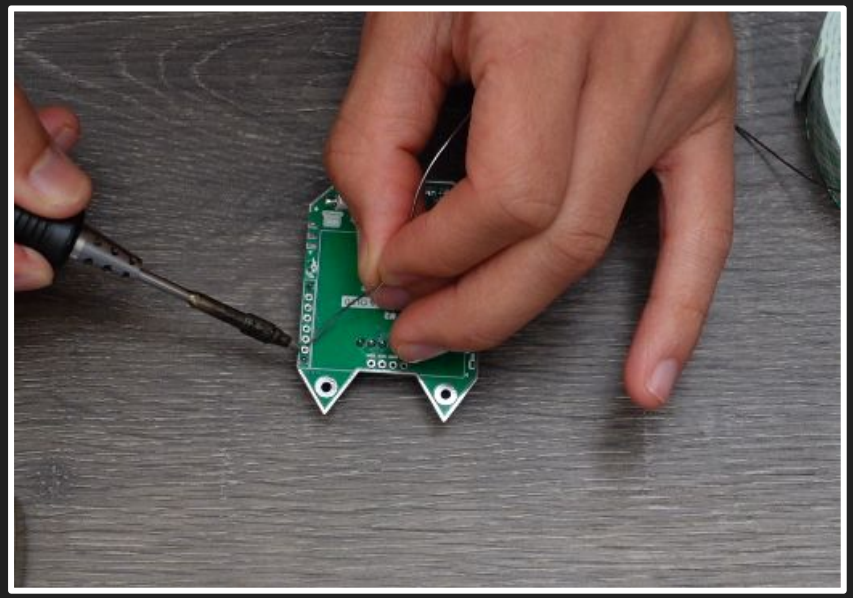
Insert Male Headers Long Side Down



Place Nugget w/ Buttons Facing Up

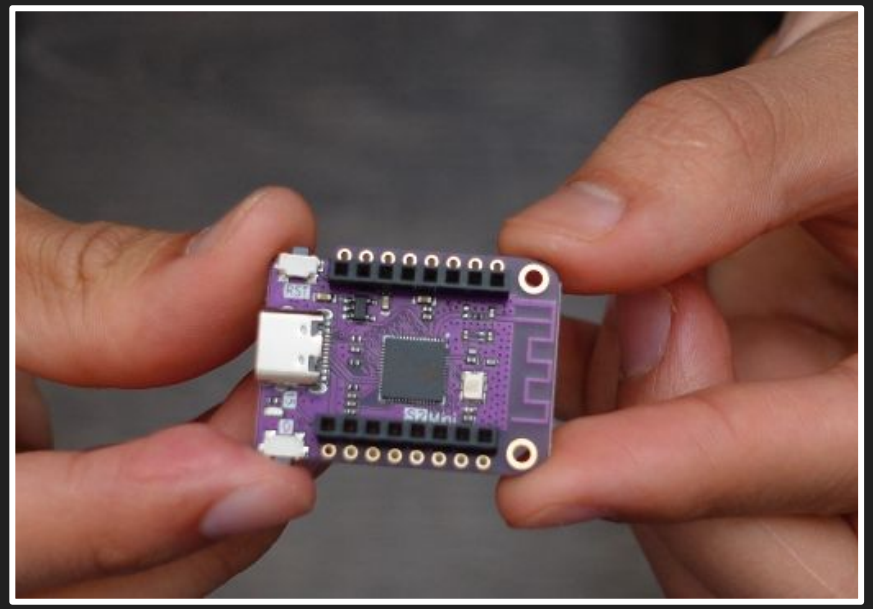
2. Expansion Header



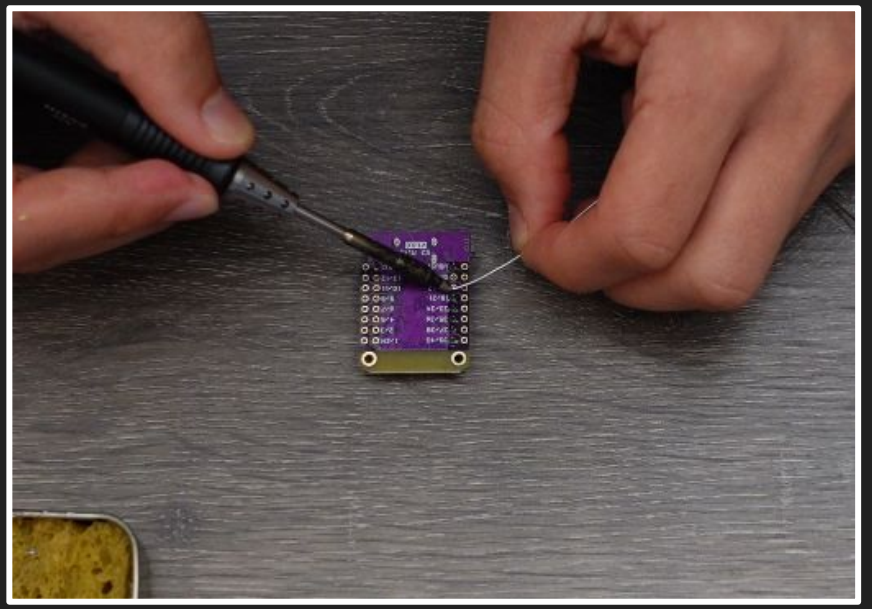


Insert the Long Female Pin Header, and rest the Nugget flush on a flat surface

3. Prep the Microcontroller

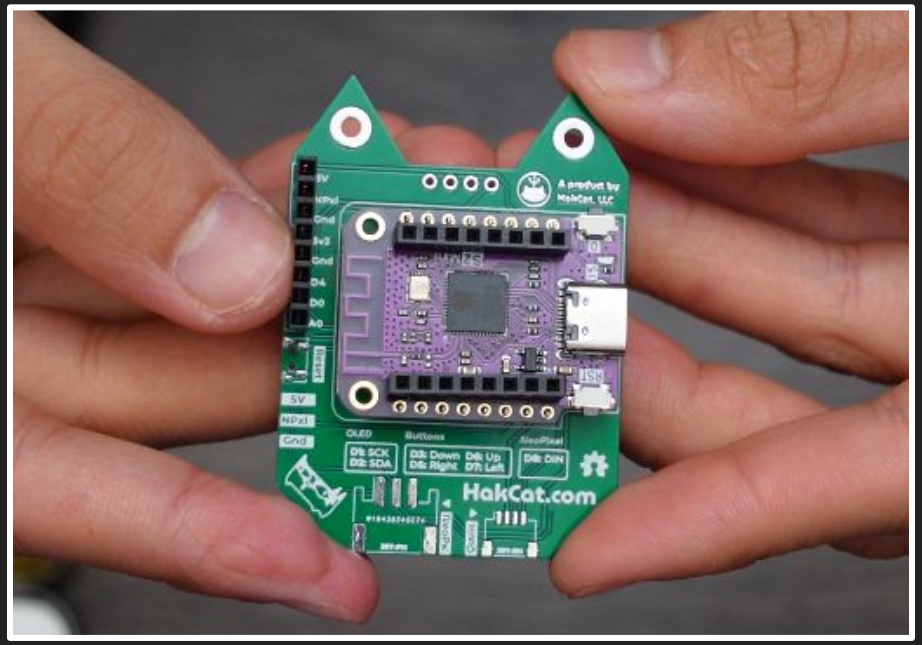


Insert Short Pin Headers on inside rows.

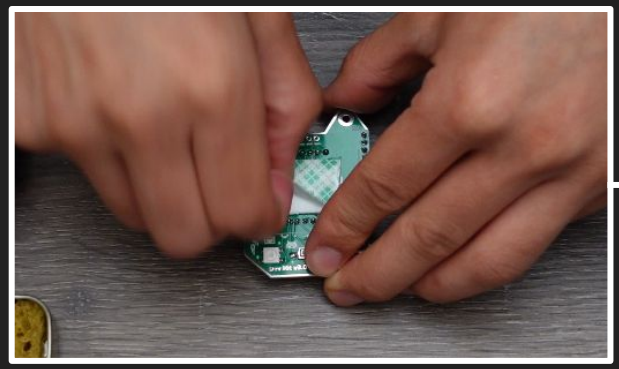


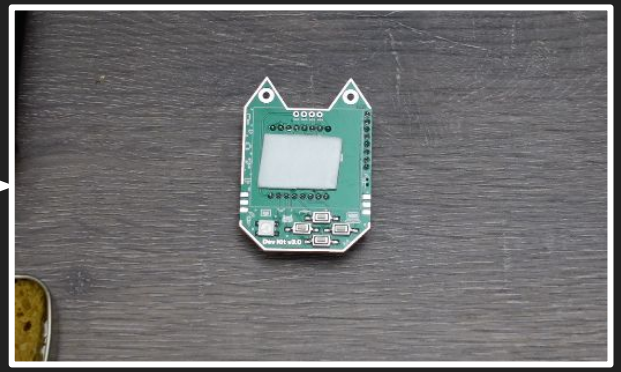
Lie flush on table and solder!

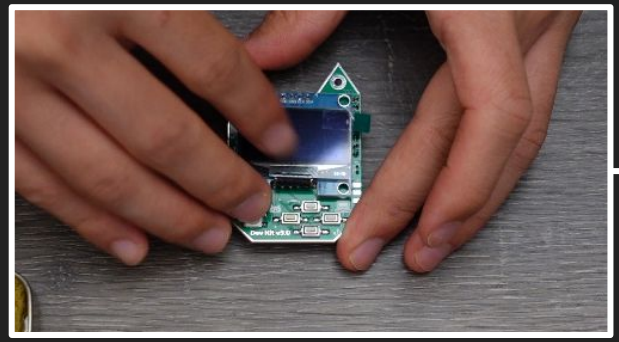
4. Solder the Microcontroller

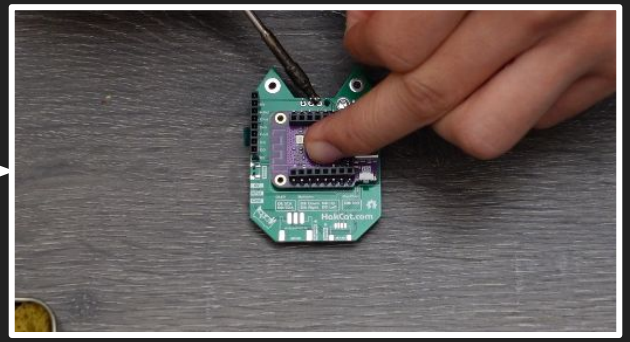


5. Mount & Solder the Screen

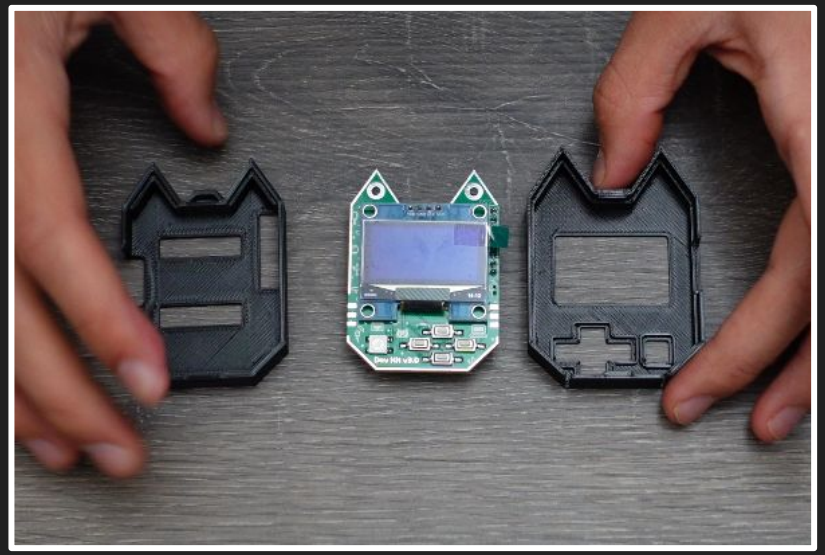








6. Snap on the Case!



Your Nugget is Ready to Hack!

USB Attack Class

1 Hour

🖥️ What are HID Attacks?

Human Interface Device attacks emulate USB devices in order to deliver malicious content to a computer.

HID attacks specifically emulate “trusted” human devices like keyboards.

🖥️ What can be emulated?

- ⌨️ A **keyboard** can type out pre-programmed malware in seconds.
- 🖱️ A **mouse** can move to keep a victim's screen unlocked.
- A **usb ethernet** adapter can trick computers into re-routing traffic

⌨ What is Keystroke Injection?

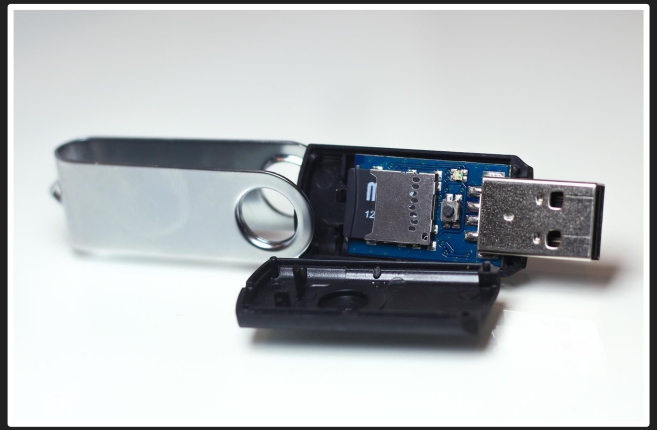
Keystroke Injection Attacks emulate a USB keyboard, in order to type out pre-programmed commands.

- Computers inherently trust keyboards
- Anything can be automated with hot-key combos & keypresses
- Open & navigate programs, download malware, modify & steal files in seconds

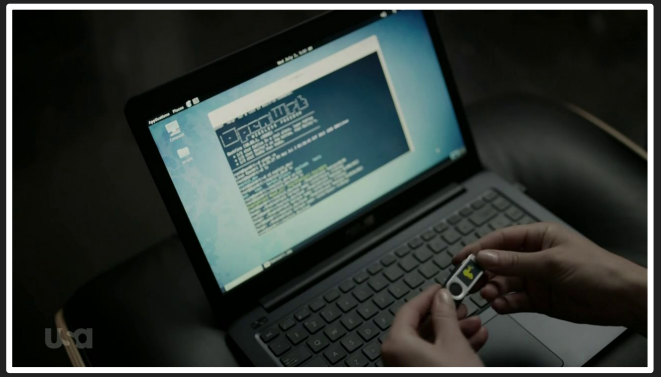
Common USB Attack Tools

🦆 USB RubberDucky

- First keystroke injection tool, created by Hak5
- Exploded in popularity, featured on shows like Mr. Robot



- ✅ Looks like a flash drive!
- ✅ Simple scripting language
- ❌ Single payload



DuckyScript

A simple language for scripting keyboard-based HID attacks.

- Line-by-line instructions

3 Basic Commands:

- Type Strings!
- Press Key Combos
- Delays or Pauses

Full Screen Windows 10 Update

```
DELAY 3000
GUI r
DELAY 100
STRING https://fakeupdate.net/win10ue/
ENTER
DELAY 3000
F11
```

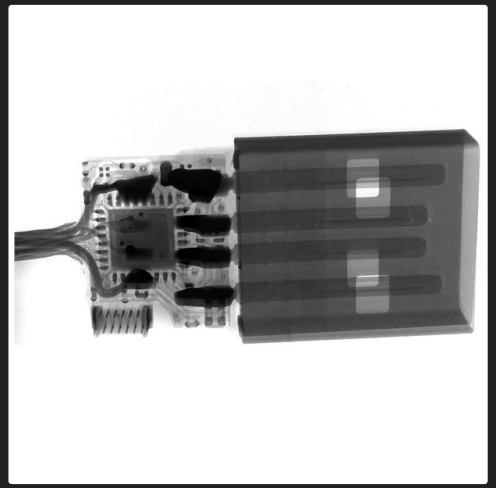
Latest DuckyScript 3.0 allows OS detection & programming logic!

Bash Bunny

- ✅ Flash Storage for Exfiltration
- ✅ Emulate Keyboards, Network Devices, and more!
- ✅ Bluetooth Geofencing
- ✅ Runs Linux
- ❌ Chonky

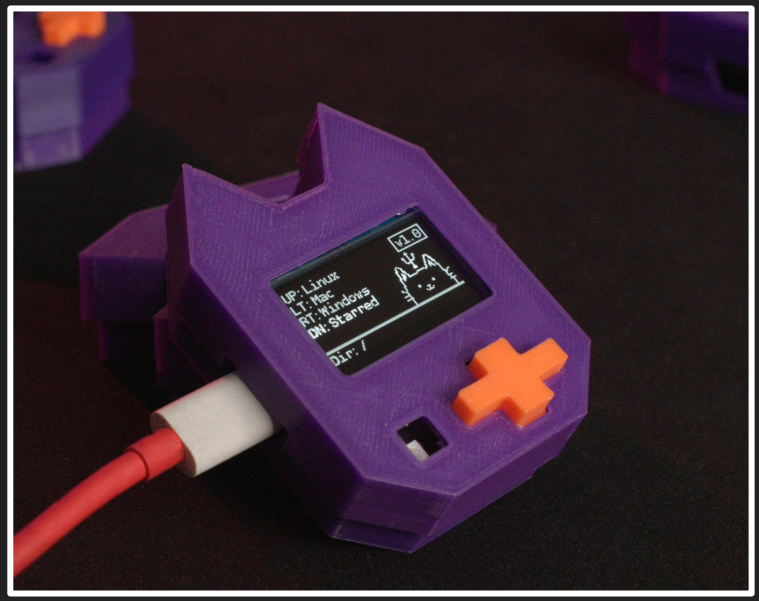
😈 OMG Cable

- ✅ Looks like a charging cable
- ✅ Run attacks over WiFi
  - Geofencing
  - Remote Scripting
- ✅ HID Attacks & Keylogging
- ❌ Inconvenient to program :(



🐱 USB Nugget

- Beginner-focused
- Reactive design
- Easy Debugging



Features:

- Uhh its cute
- Web Interface
- Flash Drive (Payloads & Exfil)

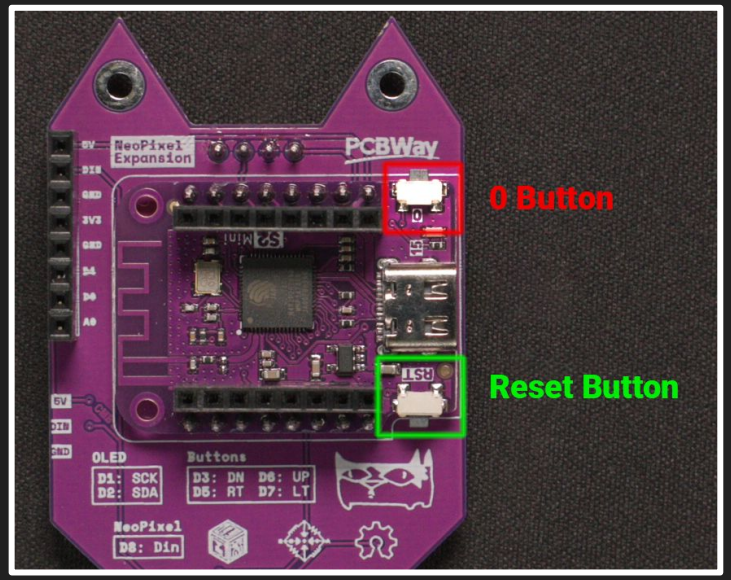
Hacking with the USB Nugget

1 Hour

Flashing the Firmware

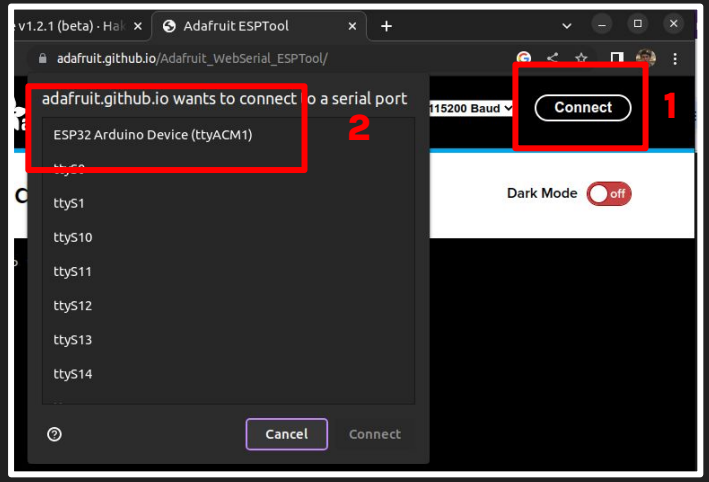
Let’s place your Nugget in “Flash Mode”!

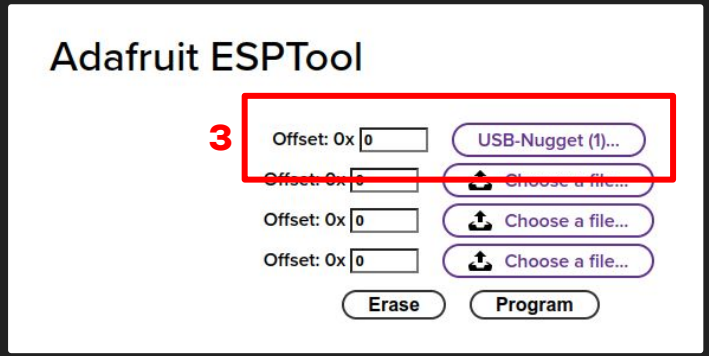
1. **Hold Down** the Boot / 0 Button
2. **Press** & release the Reset Button
3. **Release** the Boot / 0 Button
4. It’s ready to go!



Flashing the Firmware

1. Download the USB Nugget Binary File
2. In a Chrome Browser, open the Web Flasher Utility
3. Connect to your Nugget, which should appear as an “ESP32” based device
4. Upload the binary file & program it to your board!

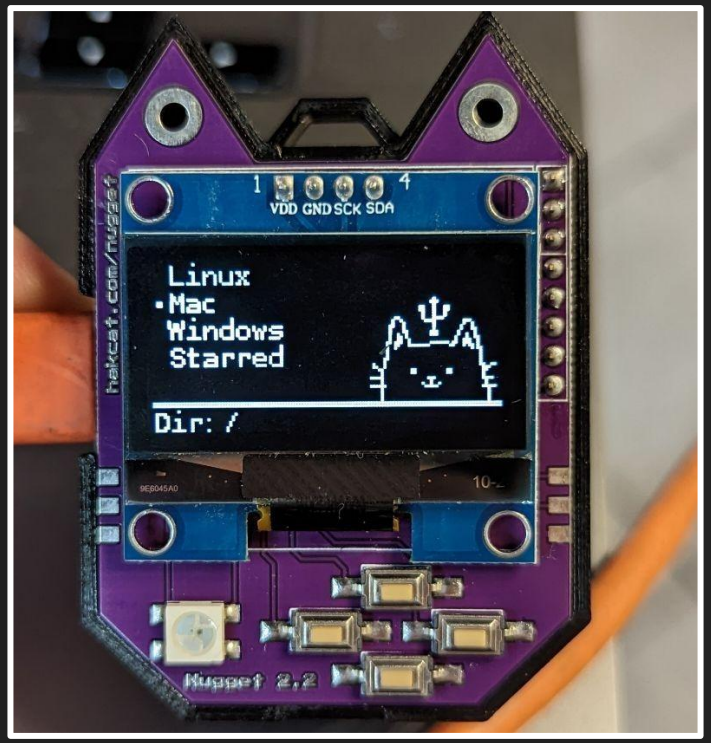




Navigating the Menu

- **Up / Down**: navigate files & folders
- **Right:** select a folder → payload
- **Left:** go back

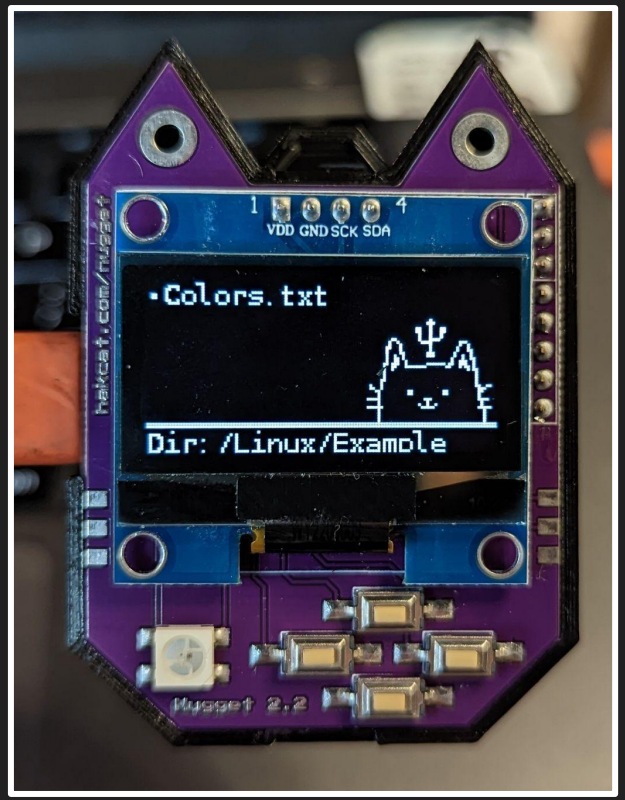
- **The current directory is shown at the bottom of the screen**



Running Payloads

Let’s test your Nugget!

- Select your **Operating System**
- Select the **Example** folder
- Run **colors.txt**.



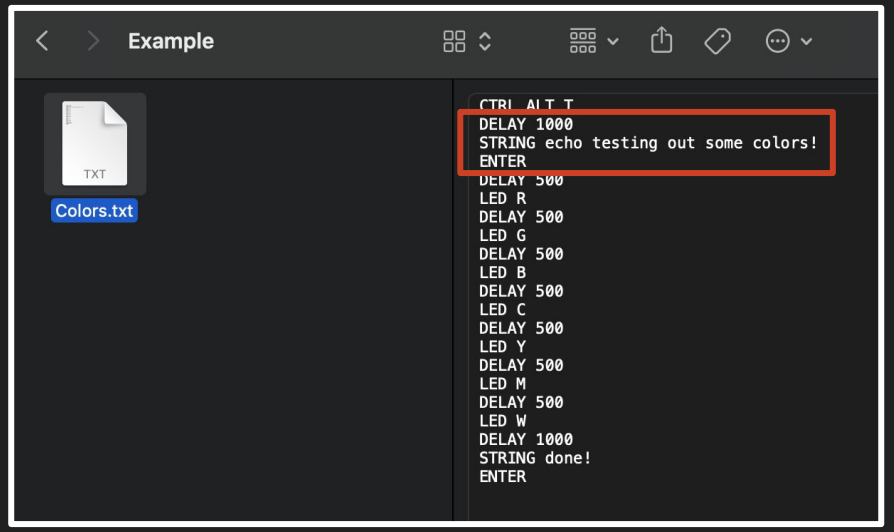
Filesystem & Payload Convention

The USB Nugget has 4 MB of Flash storage!

1. Plug in your Nugget and open the **NUGGET** drive.
2. Use **folders** to organize your payloads
3. **Operating System → Category → Payload.txt**

Edit the Colors Payload

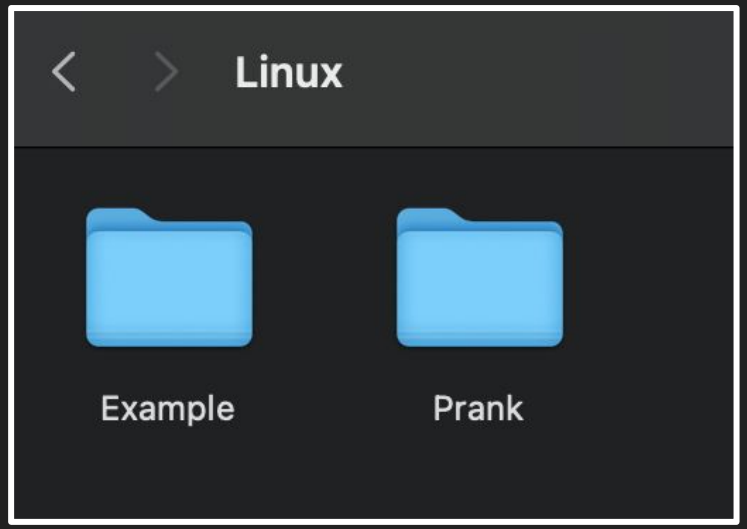
- Navigate to the **colors.txt** payload for your OS.
- Open it with your built-in text editor!
- **Change the output of the colors.txt string!**
- Save the file & run it!



Create a New Payload!

Suggested categories:

- Credentials
- Mobile
- Phishing
- **Prank**
- Exfiltration
- Prank
- Recon
- Remote Access



Create Your First Payload

👉 Tip: Work Backwards

Let's write our first payload! We're going to create a classic RickRoll.

Payload Methodology:

1. **End Goal:** What will it do?
2. **Intermediate Steps:** What programs /commands need to run?
3. **Pseudo-Code:** Outline
4. **DuckyScript**

Intermediate Steps

To execute the rickroll we need to:

1. Open a web browser
2. Open a Youtube video url
3. Turn up the volume!
4. Play video in full-screen

PseudoCode

Let’s take it a step further!

- **Keyboard shortcuts**
- **Terminal commands**
- **Things to type**
- **Delays!**

Delays are **essential** since the Nugget types extremely fast - and programs need time to open!

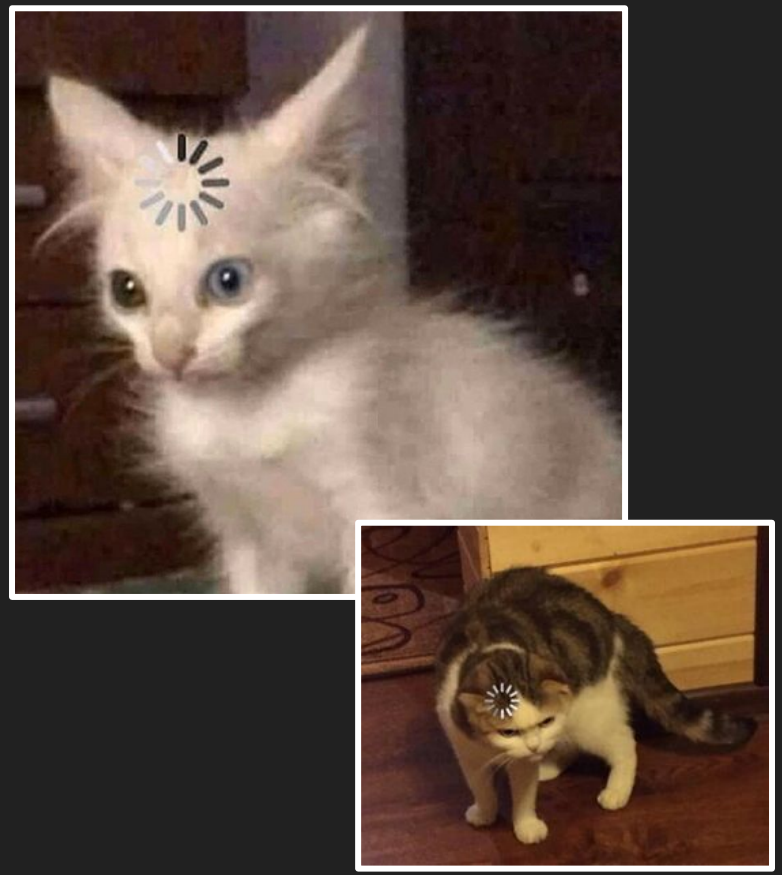
Example PseudoCode

- **Press a key combo** to open a search dialogue
- **Wait** for it to open
- **Type** in chrome / firefox
- **Press Enter**
- **Wait** for browser to open
- **Type** in the url
- **Press enter**
- **Wait** for url to load
- **Press a key** for full screen

Finally, let's turn your pseudocode into actual DuckyScript!

👉 Tip: Delays and Timing

- Delays make one-way scripts possible.
- Because microcontrollers work so quickly, many of the commands would not work without adding time for commands to finish.
- In testing, we should start out with generous delays and gradually optimize them without breaking anything.



Basic DuckyScript Commands

Commands:
REM
STRING
DELAY
DEFAULTDELAY
LED

Modifier Keys:
- CTRL or Control
- SHIFT
- ALT
- **GUI**

Standard Keys:
- a-z
- A-Z
- 0-9
- F1-F12

Key:
- ENTER
- MENU
- DELETE
- HOME
- INSERT
- UPARROW
- DOWNARROW
- LEFTARROW
- RIGHTARROW
- TAB
- END
- ESC
- SPACE
- PAUSE
- PRINTSCREEN
- CAPSLOCK
- NUMLOCK
- SCROLLLOCK
- PAGEUP
- PAGEDOWN

👉 Tip: HotKey Combos & Shortcuts

- Windows 10: https://bit.ly/2nH8IWk
- Linux (Debian): https://bit.ly/3hKs5Nu
- MacOS: https://apple.co/3EfZGGK
- Raspberry Pi OS: https://bit.ly/3TE77x1

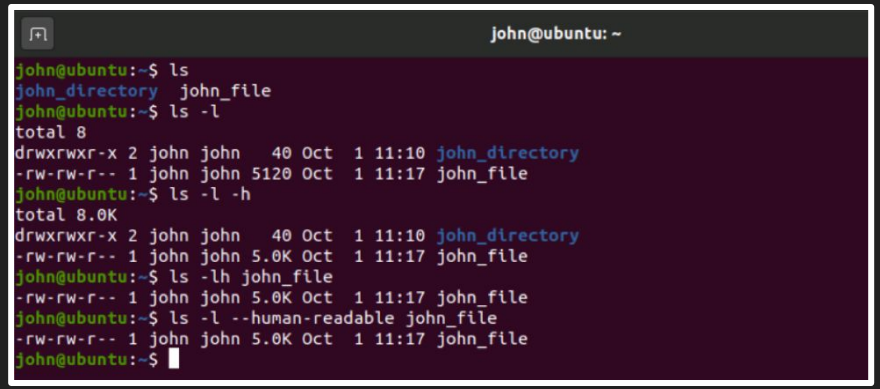
Payload Challenge:
Command Line Exercise

👉 Tip: Using the Command Line

The fastest way to do bad things on a computer is through terminal / powershell / command prompt.

You can:

- Create & modify files
- Open applications
- Run networking commands
- And more!



👉 Tip: Terminal Shortcuts

Quickest way to open a terminal on different operating systems.

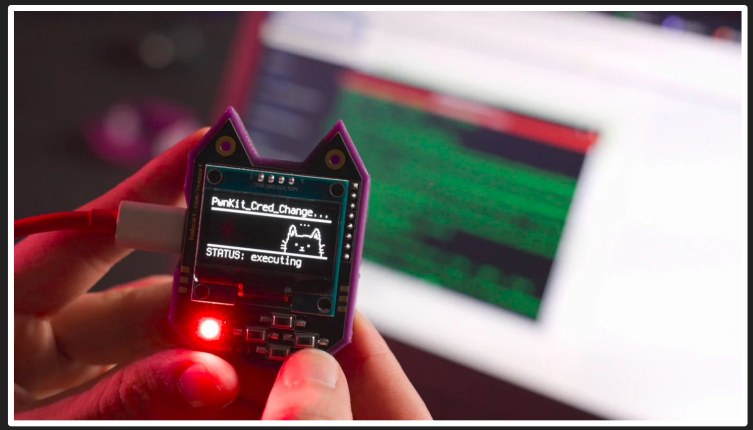
Linux: CTRL ALT T

Mac:

- CTRL SPACE
- terminal
- ENTER

Windows:

- GUI R
- cmd
- ENTER



😺 Challenge: Dogecoin Ransom Message

Open a fake ransomware site in full screen using a terminal, and read a ransom message demanding crypto!

Hint:

- Use “say” or “espeak” commands
- Function keys can enable fullscreen
- https://www.cryptoprank.com/#/crypto

Bonus: Turn up the volume & lock the computer

Taking it Further

Payload Repository

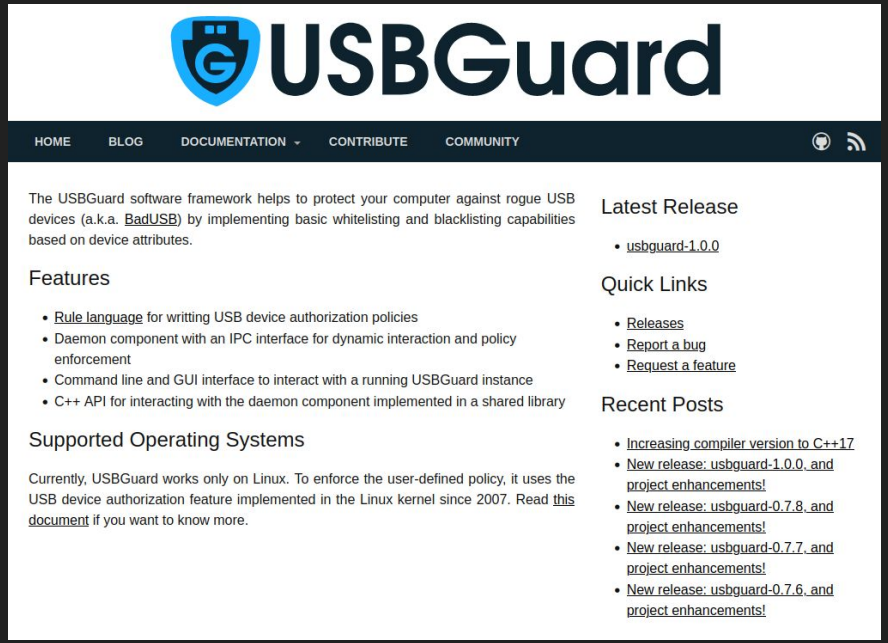
For more payloads, check out these payload repositories:

https://hak5.org/blogs/payloads/

https://github.com/HakCat-Tech/USB-Nugget-Payloads

Mitigation

- Don’t plug in random devices into your computer.
- Whitelisting / Blacklisting USB Devices
- USBGuard or other keystroke injection detection tools can look for fast keystrokes



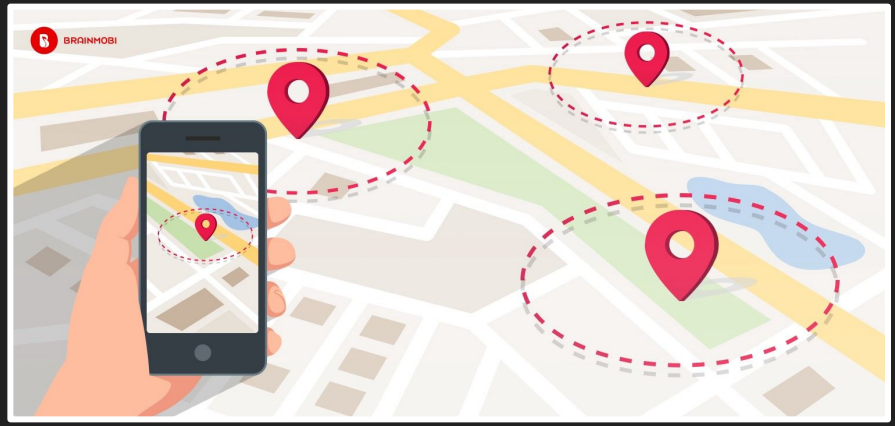
Advanced Data Exfiltration: Side-Channel

- Keyboards & HID devices have bi-lateral communication
- Computers can toggle CAPSLOCK or indicator keys
- We can use this to exfiltrate data in a protected environment by bitbang data via binary

GeoFence Attacks

GeoFence attacks can determine if specific people are nearby, by looking for the presence of their laptop / cell phone.

This can be done by looking for known WiFi or BlueTooth devices.



Mobile Attacks

Mobile phones (iOS and Android) also support HID keyboards!

Check out mobile payloads here:

https://github.com/hak5/usbrubberducky-payloads/tree/master/payloads/library/mobile

Real Life Scenario: Razer Admin Exploit

A Razer Synapse bug lets you get Windows admin privileges by plugging in a Razer mouse or keyboard.

https://www.bleepingcomputer.com/news/security/razer-bug-lets-you-become-a-windows-10-admin-by-plugging-in-a-mouse/

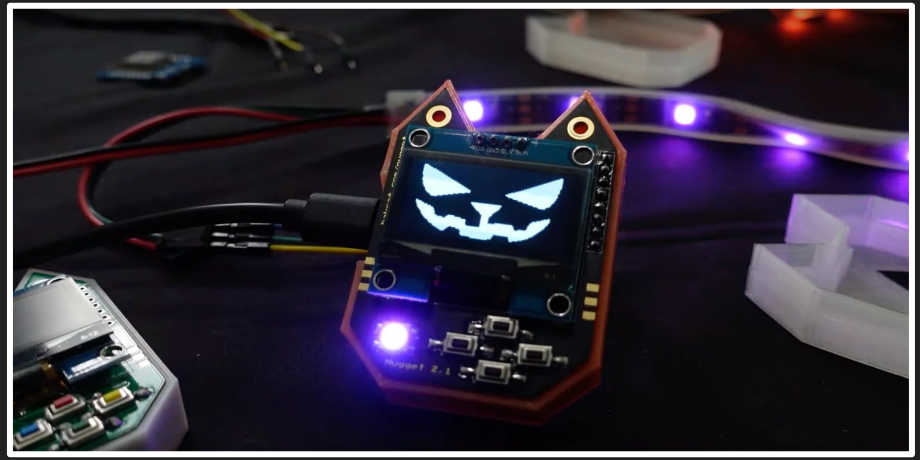
Other USB Attacks: Ethernet

- This Bash Bunny payload emulates a USB-ethernet adapter, and pretends to be the network gateway.
- This allows it to intercept network traffic.
- Works on locked computers

https://shop.hak5.org/blogs/bash-bunny/network-hijack-attacks-with-the-bash-bunny

What else can the USB Nugget do?

- Teach programming
  - CircuitPython
  - Arduino
- WiFi Reconnaissance
- Control Hardware / Sensors
- Run Community Projects
- Display animations



Thanks for coming!

Follow **@alexlynd** for upcoming events
& check out **hakcat.com** for more info.