USB Attack Workshop

Soldering Skills & Basic Keystroke Injection Attacks

[HakCat @ Hackaday Supercon]
Alex Lynd 11/6/2022

Who am I?

Hi! I'm Alex Lynd, a hardware developer & cybersecurity content creator!

- Hacking & InfoSec Videos on Hak5
- Full-Stack Product Designer @ HakCat
- I work on open-source projects like the USB Nugget, and specialize in prototyping with microcontrollers.
- Signals Intelligence & WiFi Hacking research

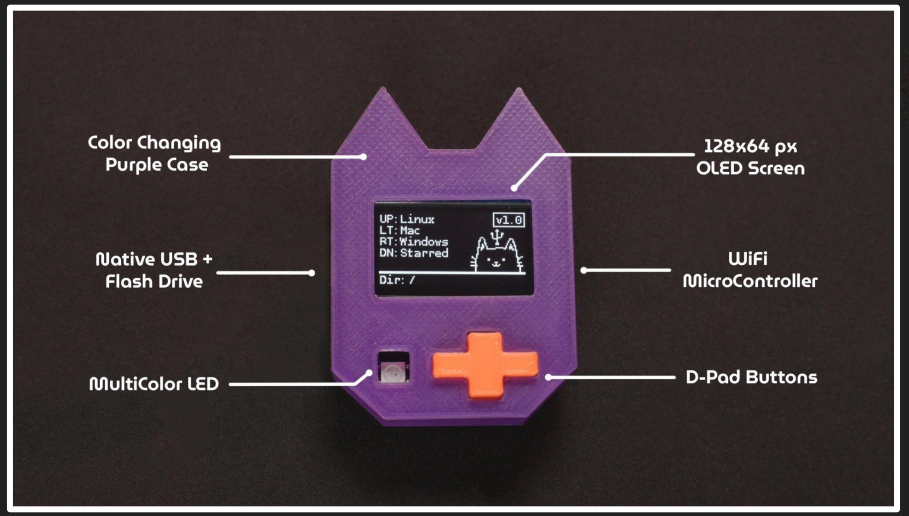
What we're doing today

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

What is the USB Nugget?

The USB Nugget is a cat-themed device that makes it easy to quickly create, run, and monitor USB attacks!

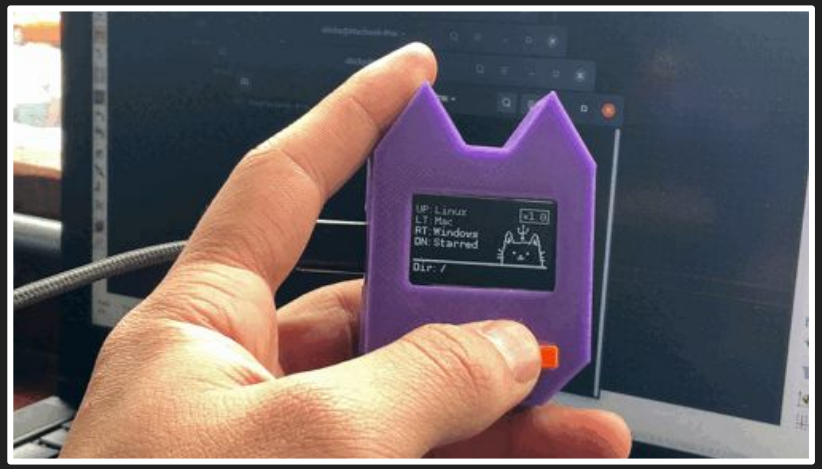
- 128 x 64 Display
- Reactive RGB LED
- D-Pad buttons
- Plug & Play Hardware
- WiFi Capable
- Native USB: Host & Device



What is the USB Nugget OS?

The USB Nugget OS lets you run keystroke injection attacks while getting reactive cat-themed feedback on-screen!

- Reactive feedback: LED & Screen
- Supports DuckyScript Classic
- Built-in USB Flash Drive
- Remote attacks with WiFi
- Emulate USB devices



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**

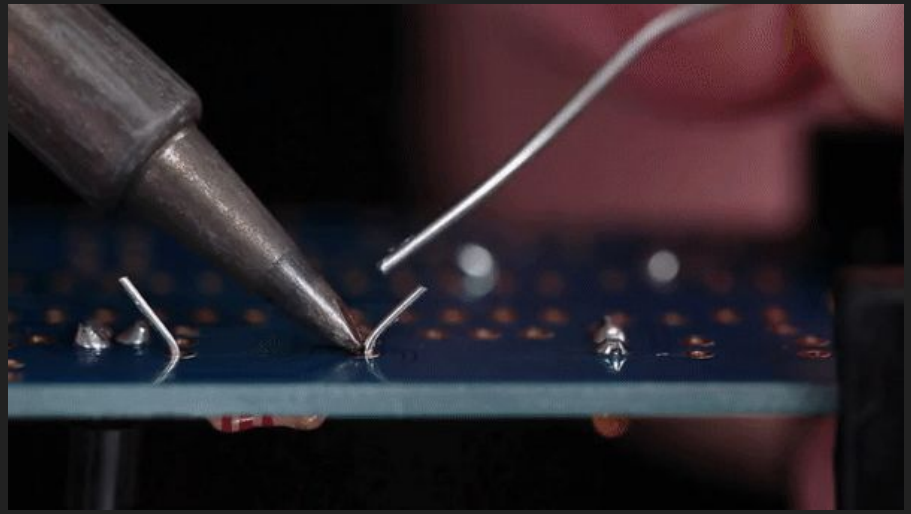
Soldering Skills Class

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.



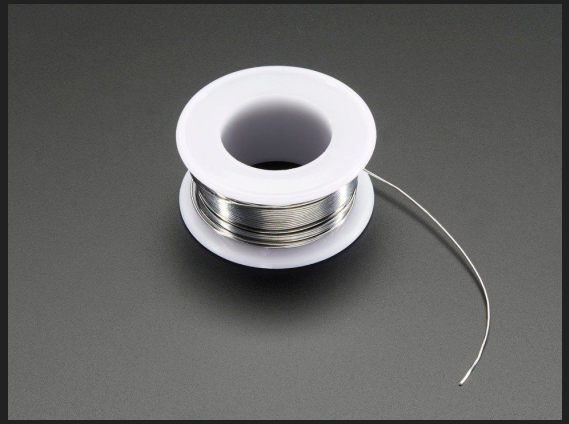
Soldering through hole components

Common Soldering Tools

Soldering Iron

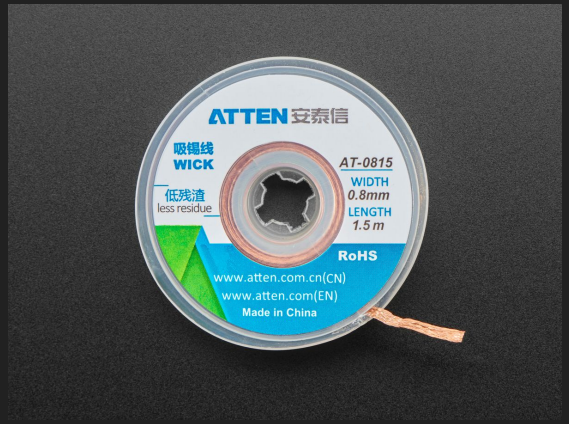
Solder Sucker *(for screw-ups)*

Soldering Materials



Solder

Solder Flux

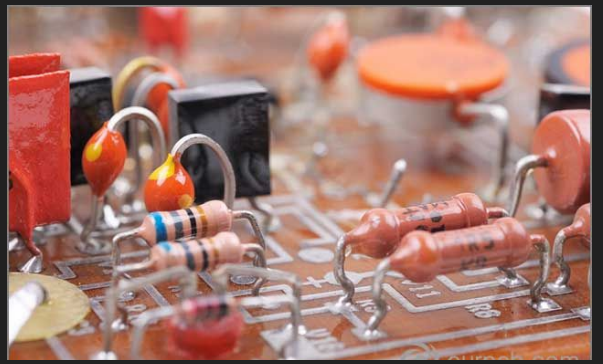


Solder Wick

Soldering techniques

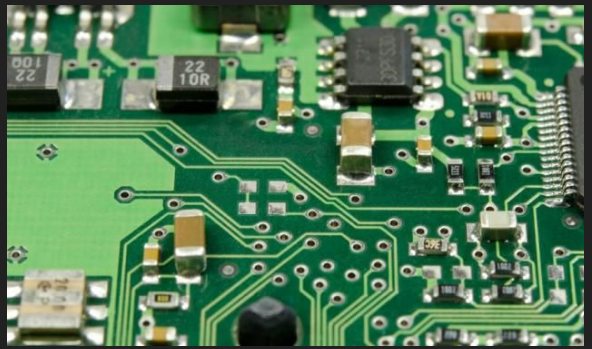
Through-hole (THT)

- Easy to assemble by hand
- Bigger components
- Parts mounted *through* board

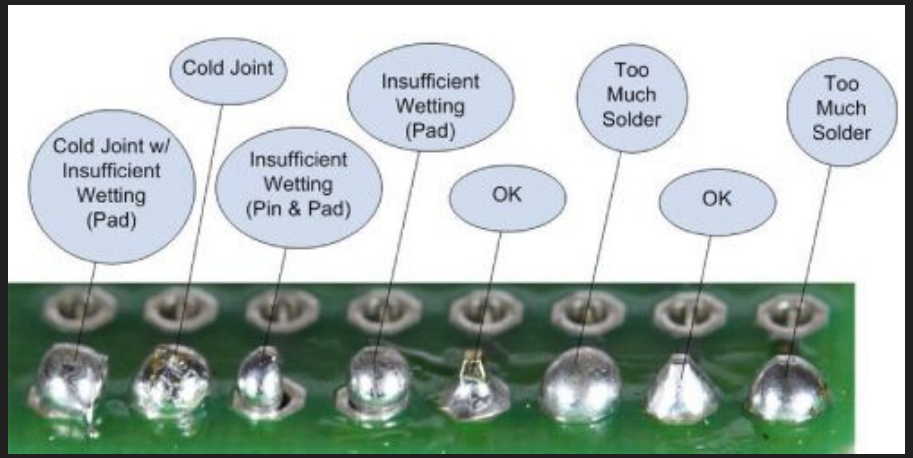


Surface Mount (SMD)

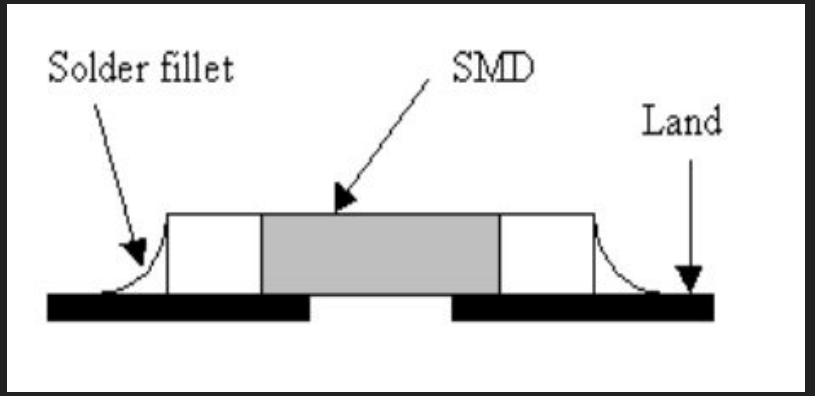
- Cheaper parts but **smaller**
- Easier for machines to assemble
- Components mounted on the surface of PCB
- Sometimes needs specialized tools



Good solder joints

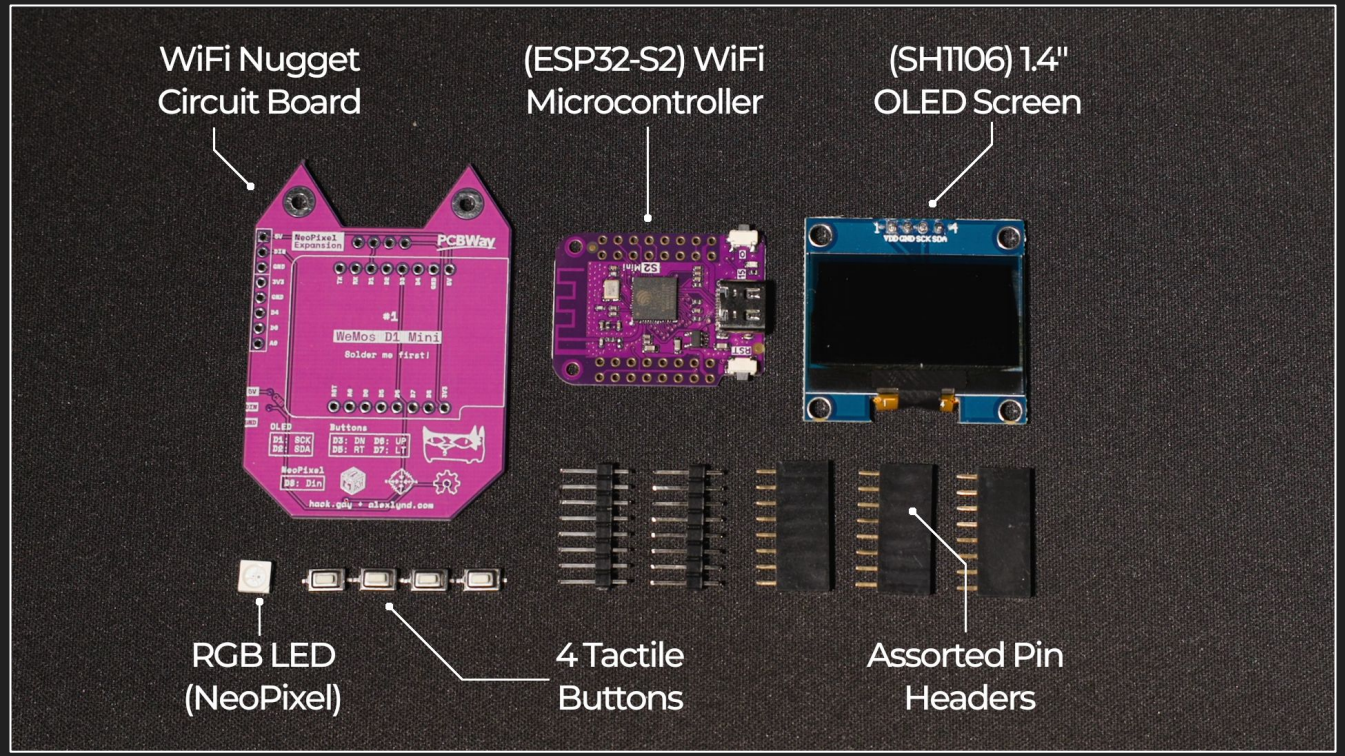


Through-hole joints



Surface mount pads

What's in your Nugget Kit



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?

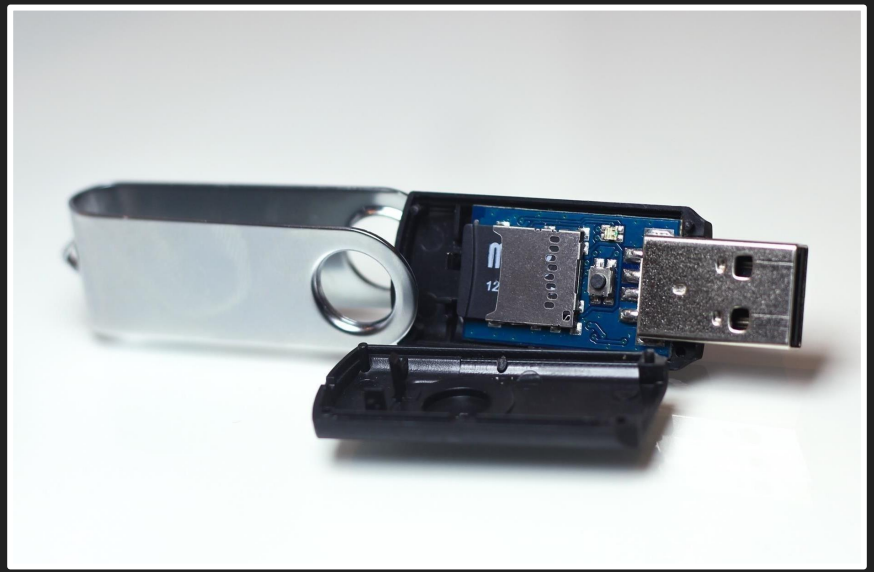
Keystroke Injection Attacks emulate a USB keyboard, in order to type out pre-programmed commands.

- 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 Darren Kitchen of Hak5
- Uses a simple scripting language to emulate a keyboard
- Exploded in popularity and was featured on shows like Mr Robot
- Simple device capable of supporting a single payload



🦆 What is DuckyScript?

Duckyscript is a simple language for scripting keyboard-based HID attacks.

- Each DuckyScript command resides on a new line
- Commands are written in ALL CAPS
- Most commands invoke keystrokes, key-combos or strings of text
- Others commands create delays or pauses

Full Screen Windows 10 Update

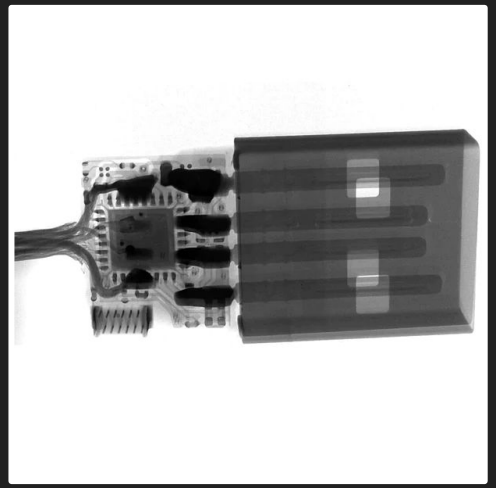
```
1 DELAY 3000
2 GUI r
3 DELAY 100
4 STRING https://fakeupdate.net/win10ue/
5 ENTER
6 DELAY 3000
7 F11
```

Bash Bunny

- Low-profile but a little more conspicuous
- Can emulate multiple types of USB devices like ethernet
- Can run 2 payloads
- Has a built-in filesystem & flash drive to easily exfiltrate victim files

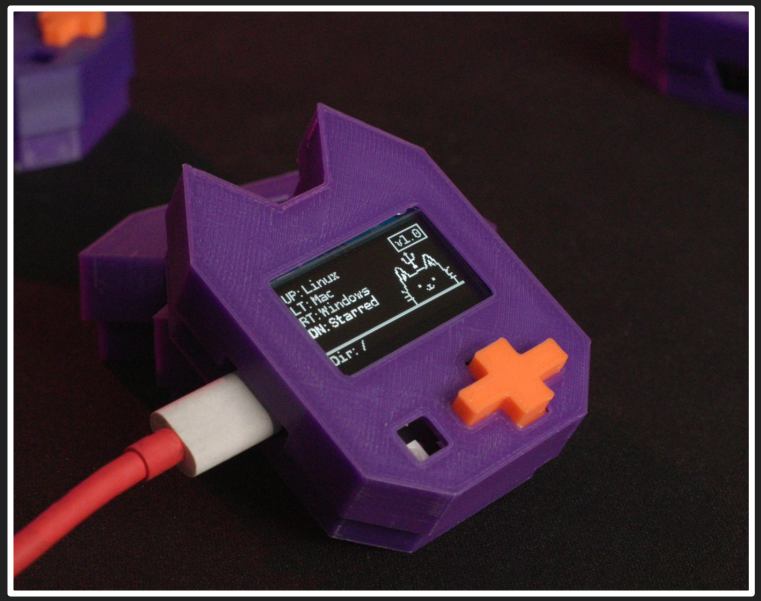
OMG Cable

- Looks like a regular charging cable
- Comes in different USB form factors
- Built-in WiFi control
- Some versions record keystrokes
- Can perform HID attacks



🐱 USB Nugget

- Beginner-friendly
- Debug payloads
- Reactive feedback
- “Unlimited” payloads
- WiFi capability

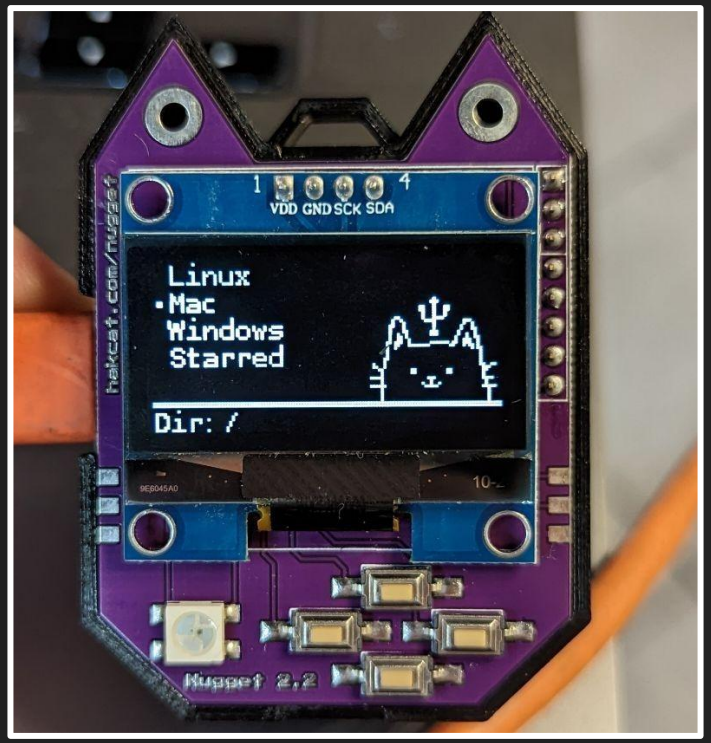


Hacking with the USB Nugget

1 Hour

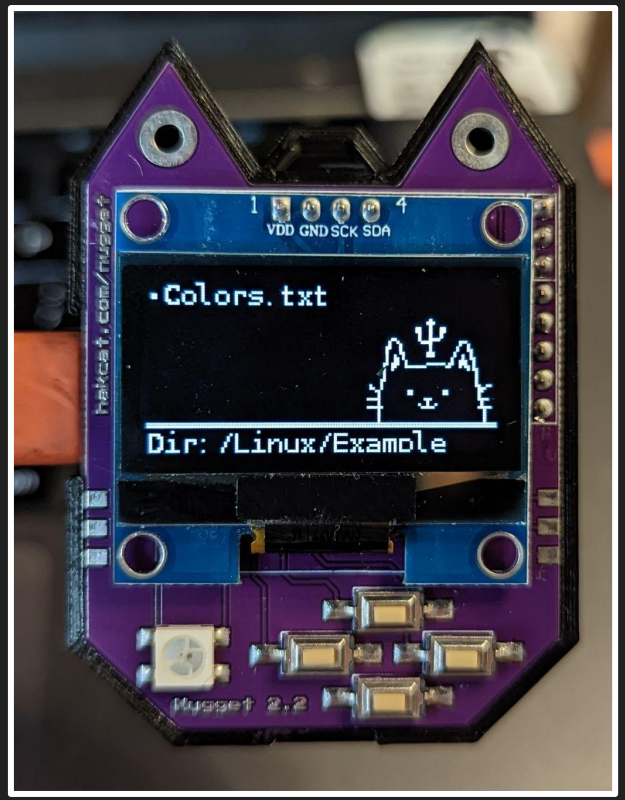
How to Navigate the Menu

- Use **up & down** to navigate files & folders
- Use **right** to select a folder / payload
- Use **left** to go back
- The current directory is shown at the bottom of the screen



How to Run Payloads

- The Nugget comes with test programs!
- Try running the example **color tester** payload by using the D-Pad to choose your operating system.
- Then select the *example* folder, and run **colors.txt**.



How to Add Payloads

The USB Nugget has 4 MB of built-in USB storage!

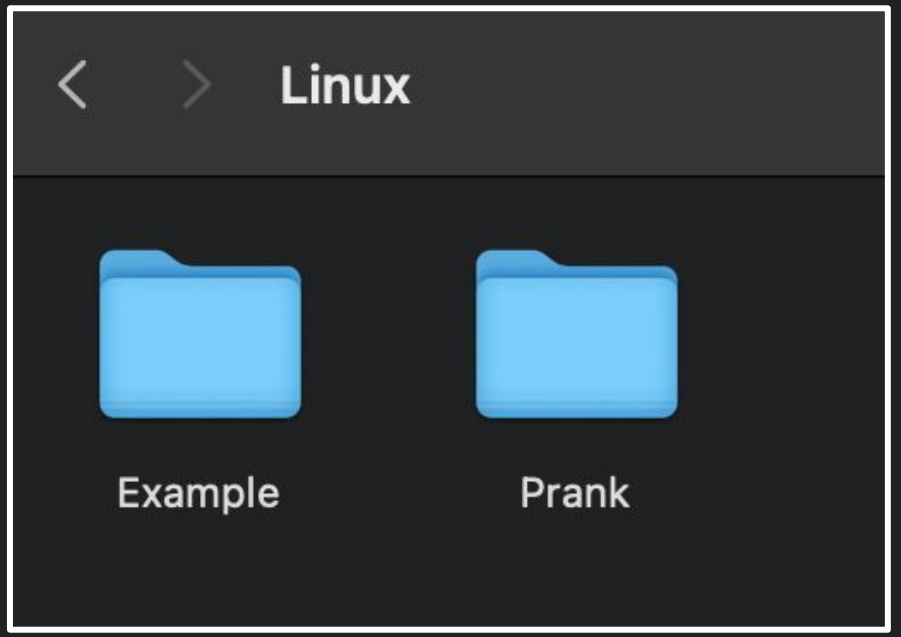
1. Plug it into your computer via USB, and wait for the **NUGGET** drive to mount.
2. Create & categorize folders to organize your payloads
3. Drag a .txt payload into a folder to save it to your Nugget!

File Naming Convention

It's recommended to organize payloads by under a target operating system & payload category folder.

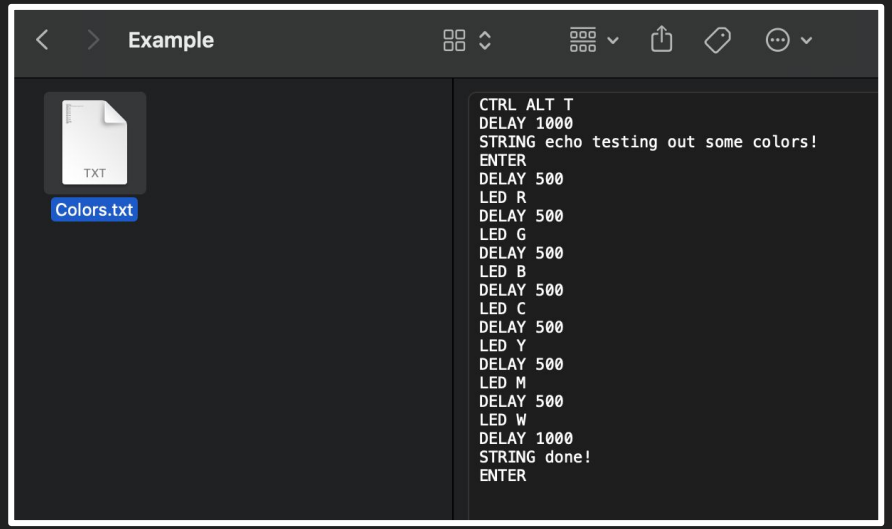
Suggested categories:

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



How to Create & Edit Payloads

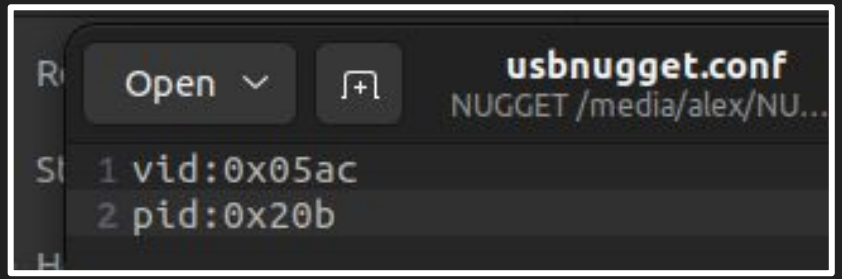
- Click on a .txt payload to open & edit it.
- You can use any text editor, any built-in plaintext editor should work.
- **Try changing the output of the colors.txt string!**



Config File: HID Emulation

We can emulate common USB / HID vendors!

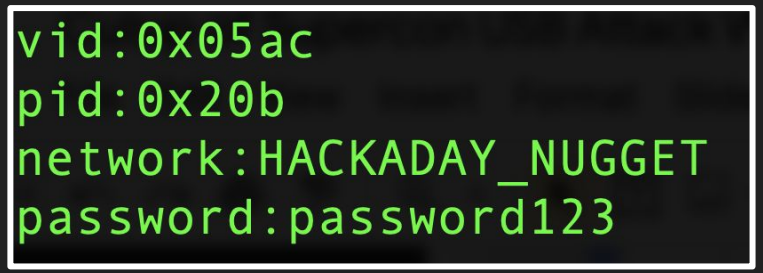
- Open the **.usbnugget.conf** file
- By default, we emulate an Apple Keyboard to prevent MacOS systems from flagging the Nugget
- USB vendor list: http://www.linux-usb.org/usb.ids
- Try changing the VID/PID, and reset your Nugget for the change to take effect!



VID: Vendor ID
PID: Product ID

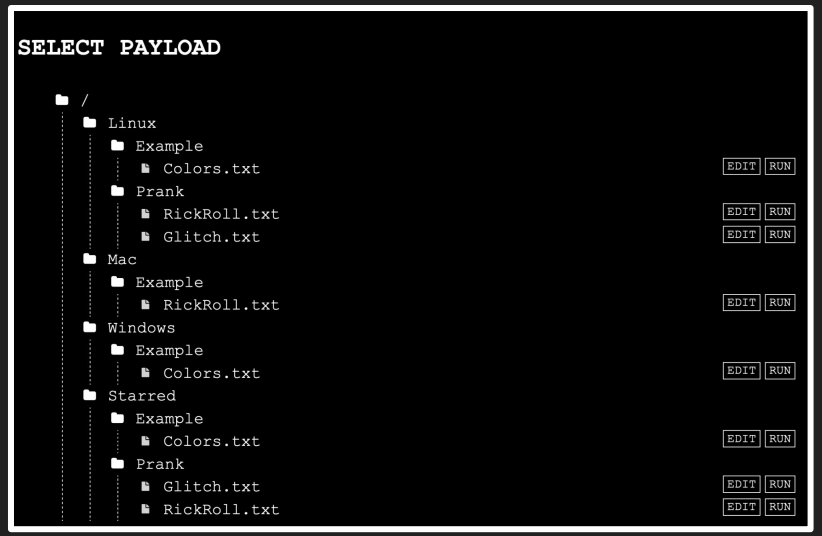
Change Wi-Fi Interface

- To use the web interface, create a network name unique to your Nugget!
- Open the **.usbnugget.conf** file in a text editor.
- **Do not add a space!** :(
- **Save and restart your Nugget.**



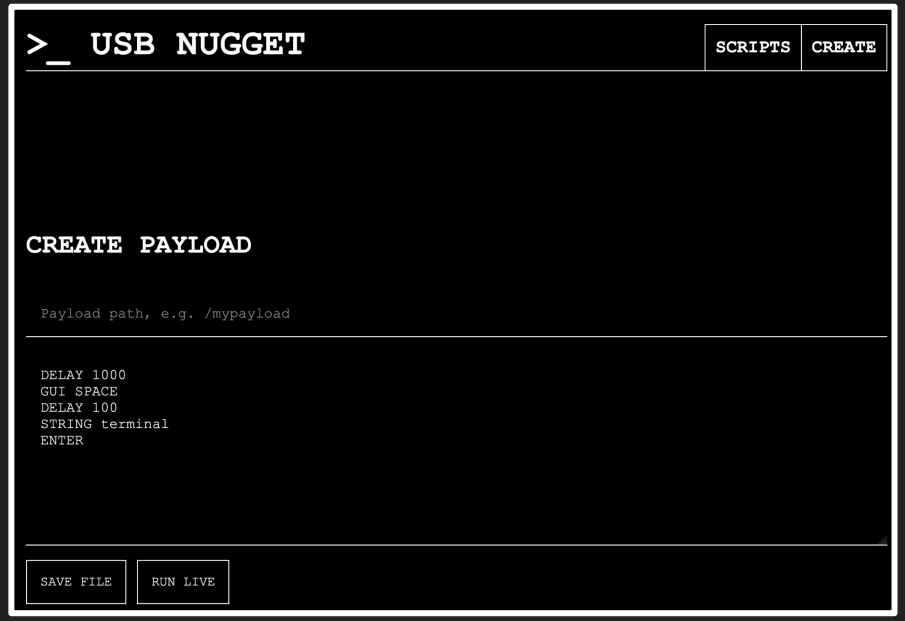
Access the Web Interface

- Join the Wi-Fi AP you set on your Nugget
- In a browser, navigate to: **http://192.168.4.1**
- The web interface allows you to run stored payloads or write new ones!



Write a Payload via Web Browser

1. Click “Create” to write a new payload.
2. Type some DuckyScript, then click “run live” to see it run!
3. To save, add a path like: /Linux/category/payload.txt
4. Hit Save



Payload Challenge

Make your own payload!

Payload Methodology: Work Backwards

Let’s write our first payload!

For this example, we’re going to create a classic RickRoll.

When writing a keystroke injection payload, we need to work backwards from what we want to accomplish. This is the general methodology:

1. **Determine End Goal**
2. **Establish Intermediate Steps**
3. **Create Pseudo-Code**
4. **Refine DuckyScript**

Step 1: Determine the End Goal

First, let's figure out the end goal of our payload.

Easy! We want to RickRoll the victim, by playing the classic “Never Gonna Give You Up” music video.

Step 2: Establishing Intermediate Steps

Next, we need to figure out which programs to be launched, and what key actions need to happen.

In our case, we need to:

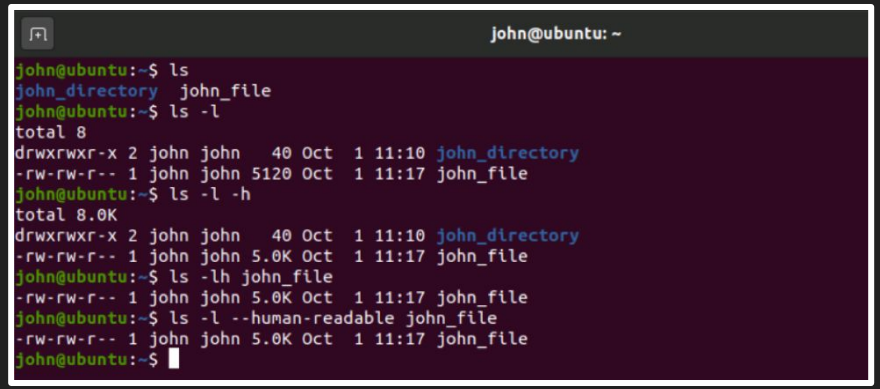
1. Open a web browser
2. Open a Youtube video url
3. Turn up the volume
4. Play video in full-screen

Payload Methodology: Command Line

The fastest way to do bad things on a computer is by opening a terminal or powershell / command prompt window.

You can:

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



Terminal Shortcuts

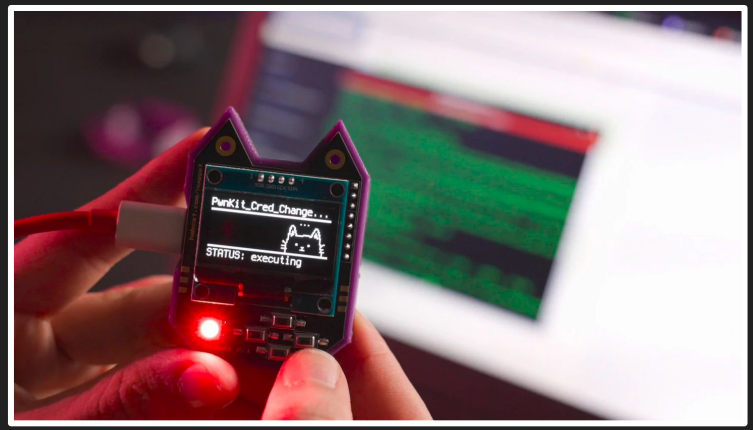
Quickest way to open a terminal on different operating systems.

Linux: CTRL ALT T

Mac: GUI SPACE

Windows:

- GUI R - opens run dialog
- cmd - types a program
- ENTER - opens command prompt



Step 3: Writing PseudoCode

Finally, lets reduce our steps to 3 basic functions using only keyboard actions:

- **Things to type**
- **Key combos to press**
- **Delays**

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

Methodology: 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.

Step 3: Example PseudoCode

- **Press a key combo** to open a terminal window
- **Wait** for Terminal to open
- **Type** in a command to launch chrome / firefox
- **Wait** for browser to open
- **Type** in the url
- **Press enter**
- **Wait** for url to load
- **Press a key** for full screen

Hint:

“start firefox” or “firefox” can be used to launch firefox from a terminal. You can also launch a url with this command.

Step 4: Refining the DuckyScript

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

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

Methodology: HotKey Combos & Short-cuts

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

Taking it Further

Payload Repository

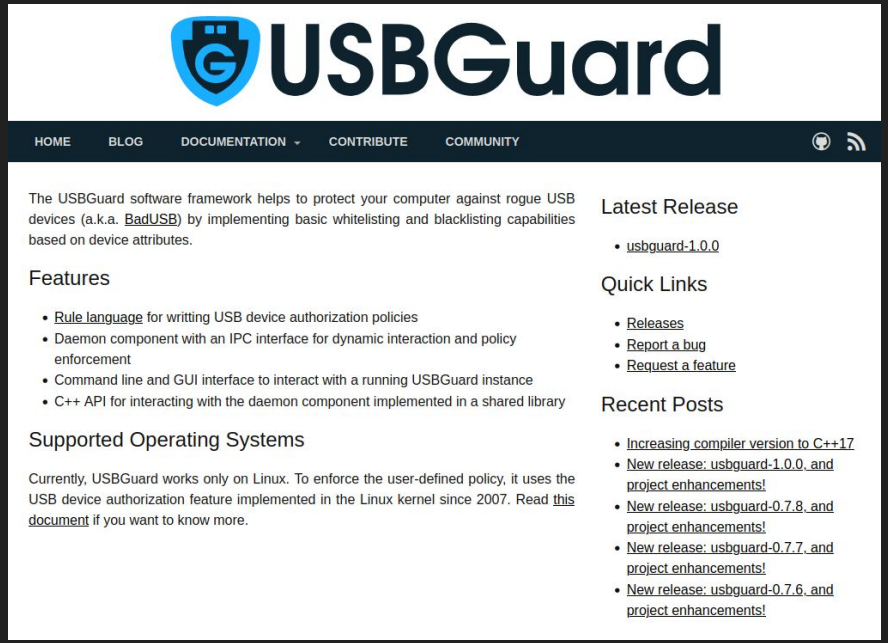
For more payloads, check out these payload repositories:

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



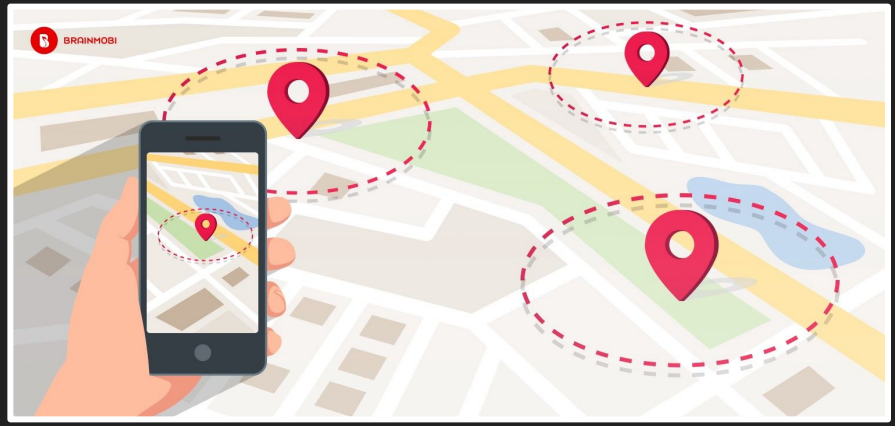
Advanced Data Exfiltration: Side-Channel

- 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/

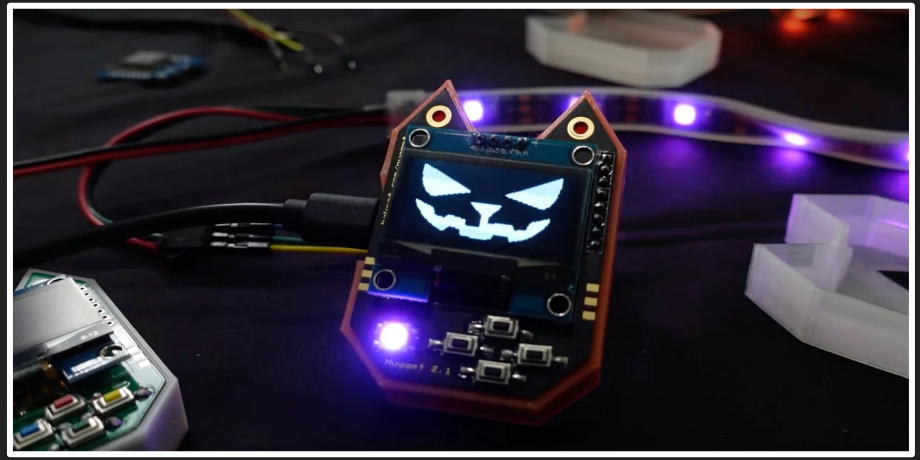
Other USB Attacks: Ethernet

- 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.