USB Attack Workshop

Beginner-Intermediate
Keystroke Injection Fundamentals

[HakCat x Null Space Labs]
Alex Lynd 9/10/2022

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

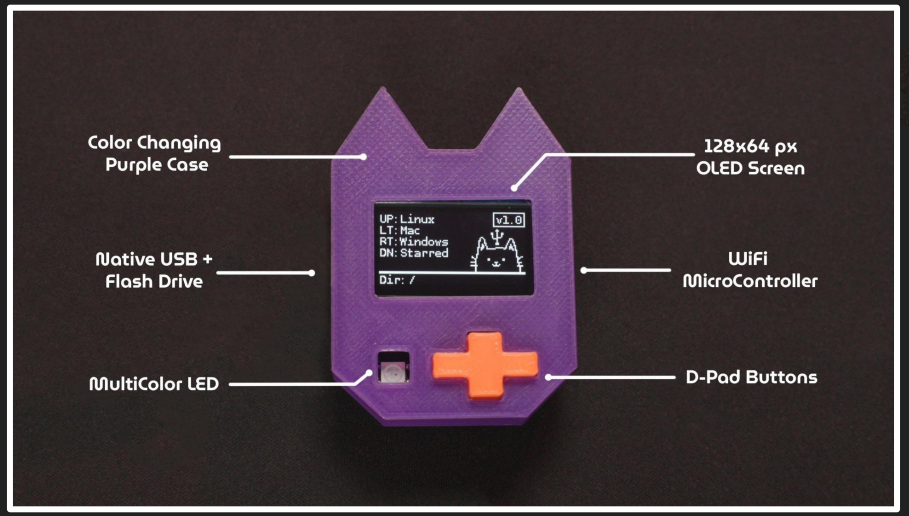
What we're doing today

- 🖥️ Learning about USB attacks: methods & tools
- 😺 Learning to use the USB Nugget
- ⌨️ Writing keystroke injection scripts!
- 👨‍💻 Learning & applying the "hacking methodology"
- 🏆 Competing in a mini hackathon

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!

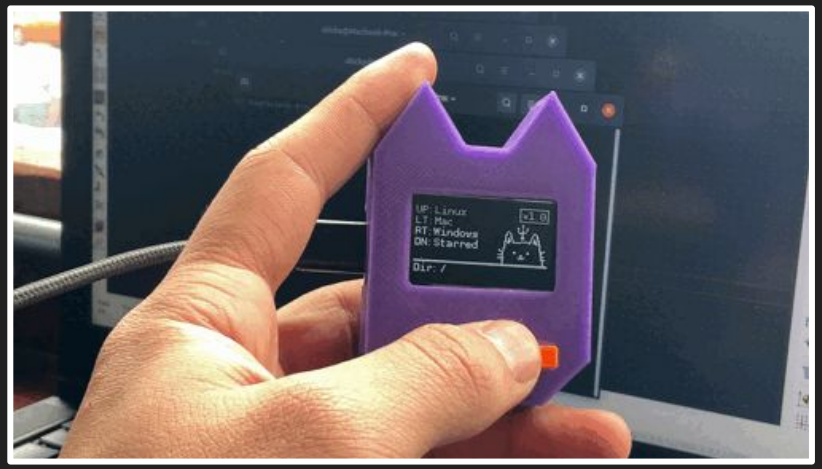
- 128 x 64 Display
- Reactive RGB LED
- D-Pad buttons
- Plug & Play Hardware
- WiFi Capable
- Native USB: Host & Device



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 power by the **ESP32-S2** microcontroller which offers:

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

USB Attack Class

1 Hour

What are USB Attacks?

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

Human Interface Device (HID) attacks specifically emulate "trusted" human devices like keyboards.

- A Nugget can pretend to identify itself as a **keyboard** & type out pre-programmed malware in seconds.
- A Nugget can pretend to be a **mouse** & inject unwanted movement on a victim computer.
- A Nugget can pretend to be a **USB ethernet adapter** in order to steal & log network traffic.

⌨ What is Keystroke Injection?

Keystroke Injection Attacks emulate a USB keyboard, and type out pre-programmed commands & keypresses in seconds.

- Computers inherently trust keyboards
- Anything can be automated with hot-key combos & keypresses
- Can be used to open & navigate programs, download malware, modify & steal files

Why use USB Attacks?

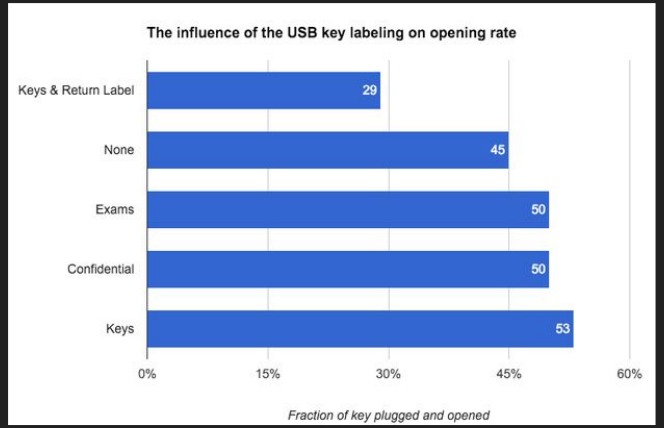
USB Attacks take advantage of physical access to a target computer, and can deliver payloads in seconds.

Common Attack Vectors:

- Running a payload on an unattended laptop by plugging in a USB Nugget
- Dropping malicious USB drives in a parking lot
- Preventing a screen from locking by plugging in a device that jiggles the mouse

Does this actually work?

- Yes! A study showed that 48% of USB drives left on a university campus were plugged in



Users Really Do Plug in USB Drives They Find

Matthew Tischer[†] Zakir Durumeric[‡†] Sam Foster[†] Sunny Duan[†]
Alec Mori[†] Elie Bursztein[◇] Michael Bailey[†]

[†] University of Illinois, Urbana Champaign [‡] University of Michigan [◇] Google, Inc.
{tischer1, sfoster3, syduan2, ajmori2, mdbailey}@illinois.edu
zakir@umich.edu elieb@google.com

***Abstract*—We investigate the anecdotal belief that end users will pick up and plug in USB flash drives they find by completing a controlled experiment in which we drop 297 flash drives on a large university campus. We find that the attack is effective with an estimated success rate of 45–98% and expeditious with the first drive connected in less than six minutes. We analyze the types of drives users connected and survey those users to understand their motivation and security profile. We find that a drive's appearance does not increase attack success. Instead, users connect the drive with the altruistic intention of finding the owner. These individuals are not technically incompetent, but are rather typical community members who appear to take more recreational risks than their peers. We conclude with lessons learned and discussion on how social engineering attacks—while less technical—continue to be an effective attack vector that our community has yet to successfully address.**

I. Introduction

The security community has long held the belief that users can be socially engineered into picking up and plugging in seemingly lost USB flash drives they find. Unfortunately, median time to connection of 6.9 hours and the first connection occurring within six minutes from when the drive was dropped. Contrary to popular belief, the appearance of a drive does not increase the likelihood that someone will connect it to their computer. Instead, users connect all types of drives unless there are other means of locating the owner—suggesting that participants are altruistically motivated. However, while users initially connect the drive with altruistic intentions, nearly half are overcome with curiosity and open intriguing files—such as vacation photos—before trying to find the drive's owner.

To better understand users' motivations and rationale, we offered participants the opportunity to complete a short survey when they opened any of the files and read about the study. In this survey, we ask users why they connected the drive, the precautions they took, demographic information, as well as standard questions to measure their risk profile and computer expertise. We find that attack was effective against all sub-populations at Illinois. The majority of respondents connected a drive to locate its owner (68%) or out of curiosity (18%).

(a) Unlabeled drive (b) Drive with keys (c) Drive with return label (d) Confidential drive (e) Exam solutions drive

Fig. 1: **Drive Appearances**—We dropped five different types of drives. We chose two appearances (keys and return label) to motivate altruism and two appearances (confidential and exam solutions) to motivate self-interest, as well as an unlabeled control.

Real Life Scenario: Fin7 USB Mailing Attack

The Fin7 Cybercrime group mailed malicious USB drives that installed ransomware onto targets' computers

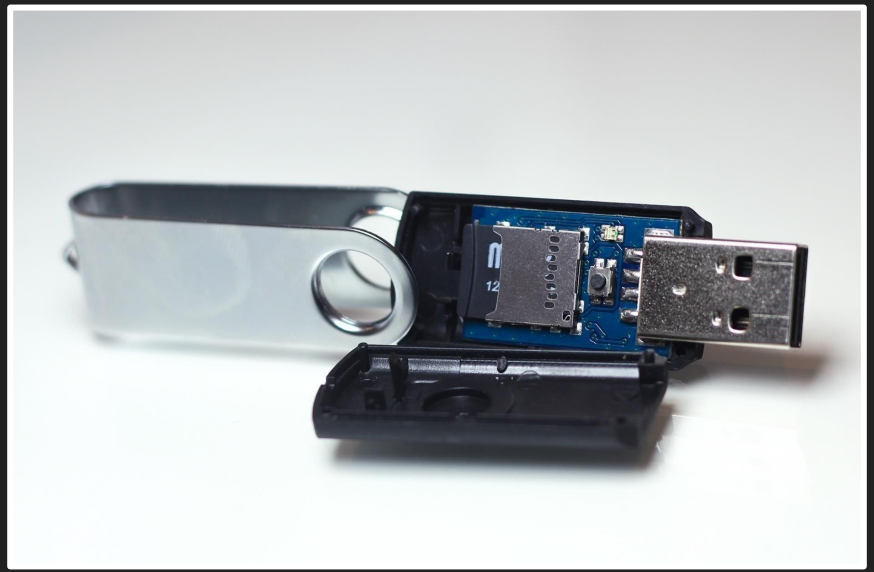
- Impersonated Amazon / Health Services
- Disguised as enticing package: fraudulent gift card, thank you letter, USB
- Employed social engineering to deploy payload

Real Life Scenario: Fin7 USB Mailing Attack

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

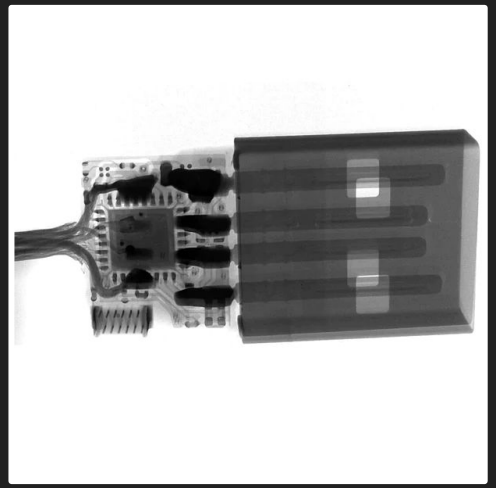
```
1 DELAY 3000
2 GUI r
3 DELAY 100
4 STRING https://fakeupdate.net/win10ue/
5 ENTER
6 DELAY 3000
7 F11
```

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

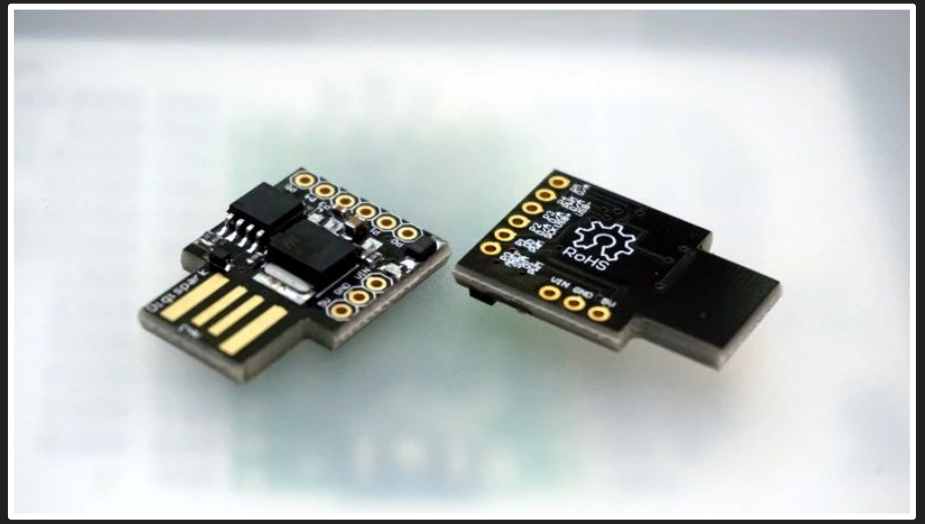
OMG Cable

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



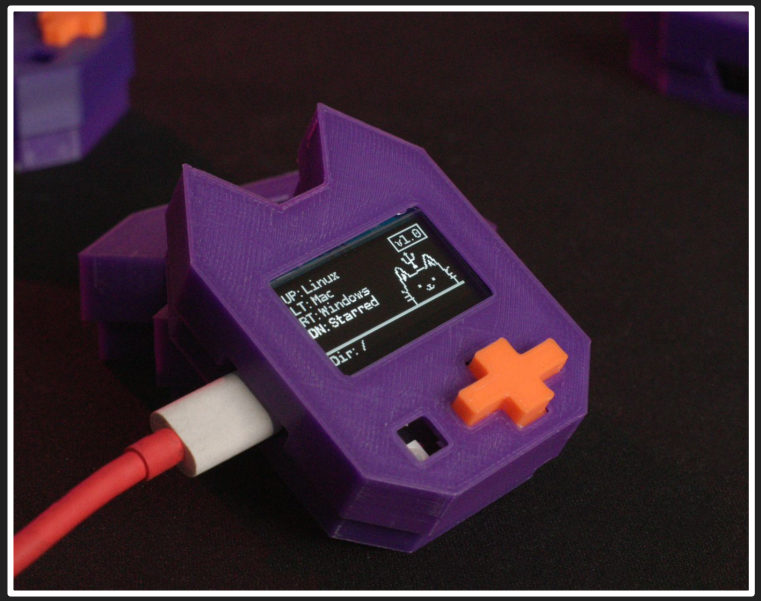
Diy Alternative: DigiSpark BadUSB

- $3
- Disposable
- Hard to program
- Single payload



🐱 USB Nugget

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



Hacking with the USB Nugget

1 Hour

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**.

- Use **up & down** to navigate files & folders
- Use **right** to select a folder / payload
- Use **left** to go back

How to Add Payloads

The USB Nugget has built-in flash storage!

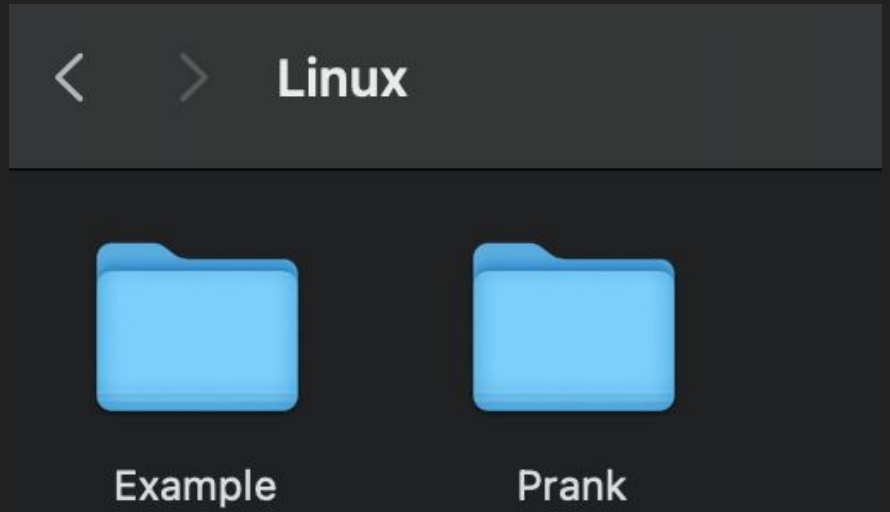
1. Plug it into your computer via USB, and wait for the **NUGGET** drive to mount.
2. You can create & categorize folders to organize your payloads
3. Drag over your .txt payload into a folder to save it to your Nugget!

File Naming Convention

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

Suggested categories:

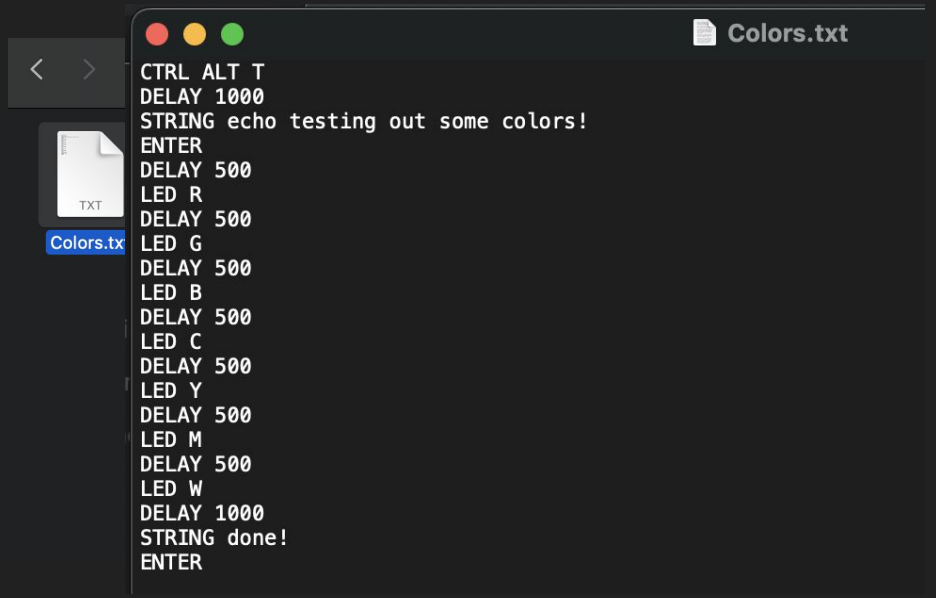
- Credentials
- Mobile
- Phishing
- Prank
- Exfiltration
- Prank
- Recon
- Remote Access



How to Create & Edit Payloads

Simply click on a .txt payload to open & edit it! You can use any text editor, but your built-in one should work.

Try changing the output of the colors.txt string!



Writing Your First Payload

Get Started Creating Attack Payloads!

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, lets 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:

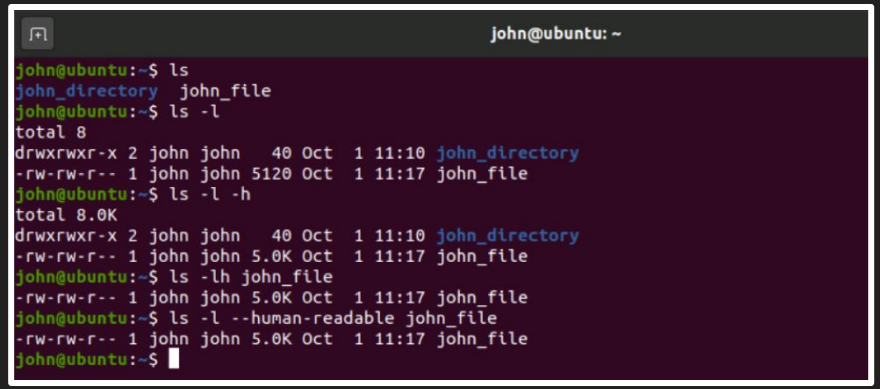
1. Open a web browser
2. Open a Youtube video url
3. Turn up the volume
4. Play video in full-screen

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

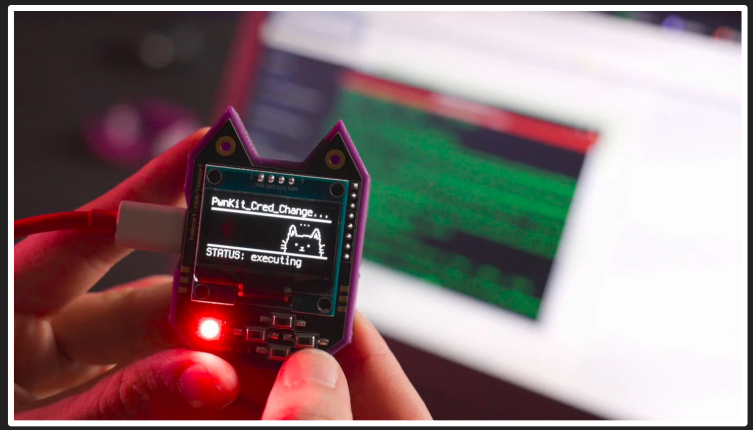
Quickest way to open a terminal on different operating systems.

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 move into a more optimized design that works quickly 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 Keyboard Shortcuts: https://www.windowscentral.com/best-windows-10-keyboard-shortcuts

Linux Keyboard Shortcuts (Debian): www.computerhope.com/ushort.htm

MacOS Keyboard Shortcuts: https://support.apple.com/en-us/HT201236

Raspberry Pi OS Shortcuts:

https://defkey.com/raspbian-raspberry-pi-shortcuts https://defkey.com/raspbian-raspberry-pi-shortcuts

Intermediate Payloads

Get Started Creating Attack Payloads!

Payload 1: Ransom Message

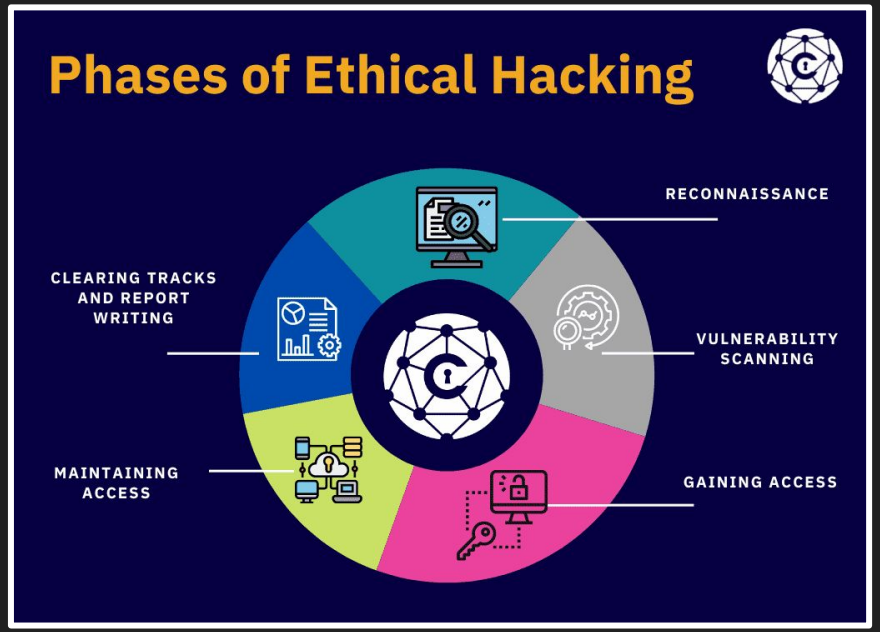
- Open a terminal window
- Use volume keys or a command to turn up the volume
- Use “say” or “espeak” to demand a dogecoin ransom to be paid
- Open a full screen browser window to a fake ransomware window:
  - https://www.cryptoprank.com/#/crypto

Hint: function keys can be used to raise the volume.

Terminal commands can also be used.

The Phases of Hacking & Methodology

1. **Reconnaissance**
   a. Scope out the victim
   b. Determine attack surfaces
2. **Scanning & Enumeration**
   a. Find all potential targets
   b. Scan for vulnerabilities
3. **Gain Access**
   a. Run exploit code / deploy payload
4. **Maintain Access**
   a. Install persistent tools like C2
   b. Exfiltrate data
5. **Cover Tracks**
   a. Delete logs, clear history, etc



Example: PwnKit Demo

1. **Reconnaissance**: Find a Linux machine
2. **Scanning**: Is it vulnerable to PwnKit?
3. **Gain Access**: Run the exploit code!
4. **Maintain Access**: Install backdoor
5. **Cover Tracks**: Close all tabs & clear logs!

Payload 2: Bee Movie Stager Script

The objective is simple. Download the entire bee movie script onto the victim's desktop as a text file!

What methods can we use to do this?

1. **Manual:** Typing out the WHOLE bee movie script
2. **Storage:** Copying a file from the Nugget flash drive
3. **Remote:** Use a command to download the script

Hint: The **curl** or **wget** command can be used to download remote files.

Payload 3: Data Exfiltration

How can we exfiltrate data from a victim device?

Similar to the previous script, this can be accomplished **locally** or **remotely.**

- **Locally** - Only works with physical access, but is quick & less conspicuous
- **Remote** - Better for long term access, but creates a lot of traffic

Let’s try it locally first!

Payload 3: Data Exfiltration

To test out our reconnaissance & enumeration skills, create a payload that does the following:

- Recursively list **all** files and folders in the user's home directory (or somewhere else)
- Save that list to a text file on the Nugget!
- Optional: save network info or nearby networks to another file

Hint: **ls** or **dir** can be used to list files / folders.

Payload Repository

For more payloads, check out these payload repositories:

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

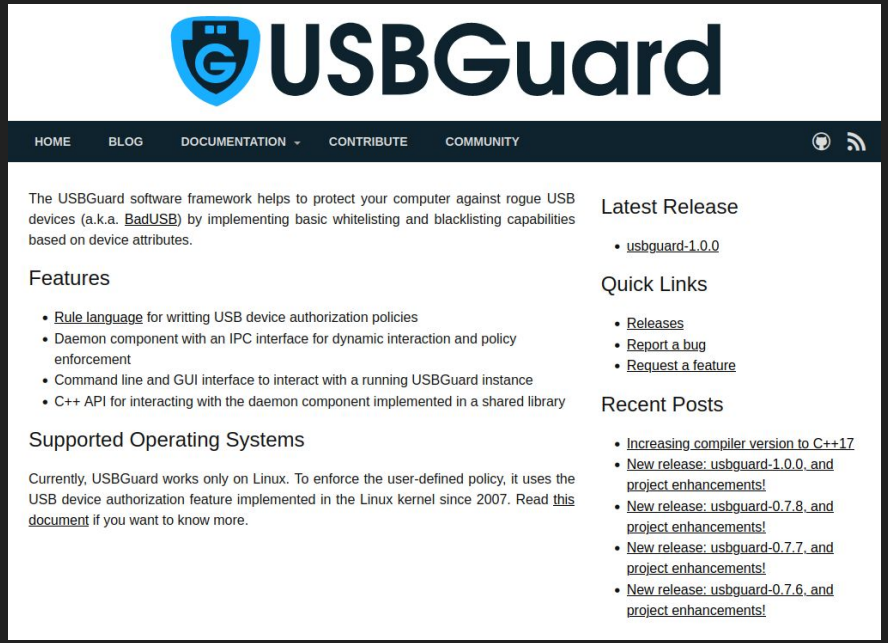
https://github.com/HakCat-Tech/USB-Nugget-Payloads

Taking it Further

Advanced Payload Ideas & Attacks

Mitigation

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



Advanced Data Exfiltration: CanaryTokens

This script uses a free online service called **CanaryTokens** as a simple data exfiltration server.

This allows us to plant a persistent piece of malware that phishes the user, and sends us the password when its obtained.

https://alexlynd.com/blog/easy-data-exfiltration-with-canarytokens/

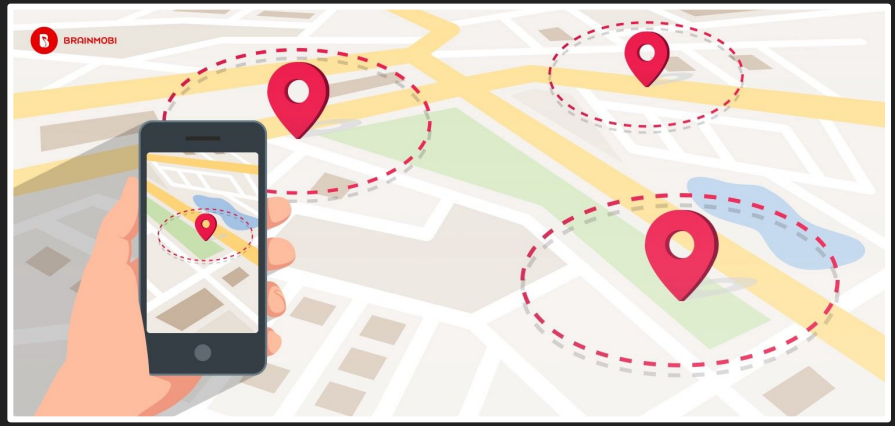
Advanced Data Exfiltration: Side-Channel

- 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/

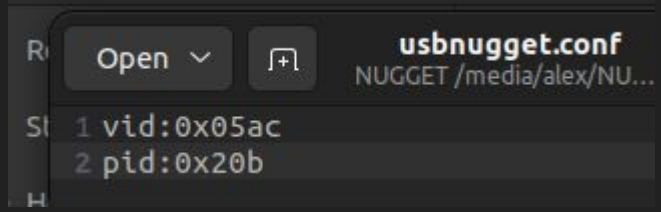
Other USB Attacks: Ethernet

- 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

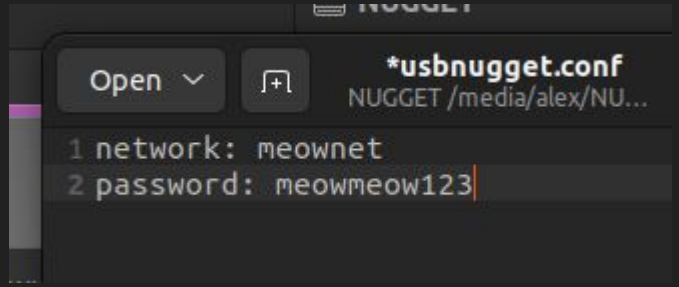
https://shop.hak5.org/blogs/bash-bunny/network-hijack-attacks-with-the-bash-bunny

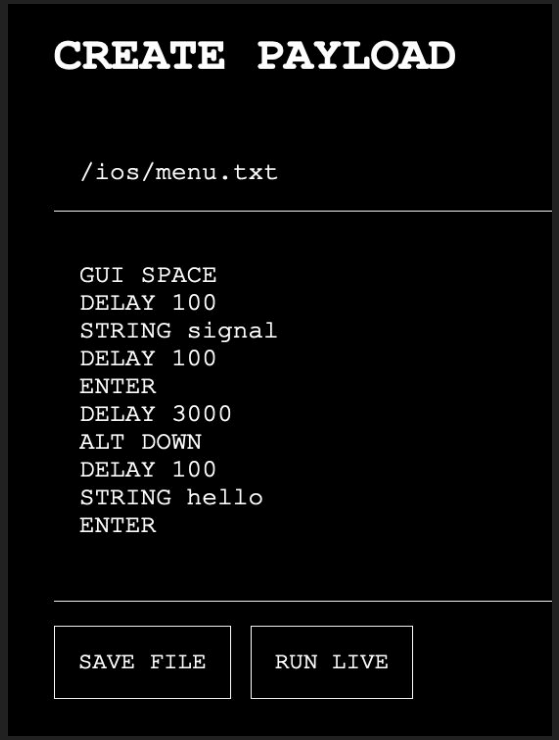
USB Nugget WiFi Interface & HID Emulation

Edit the usbnugget.conf file to set a custom hardware VID & PID:



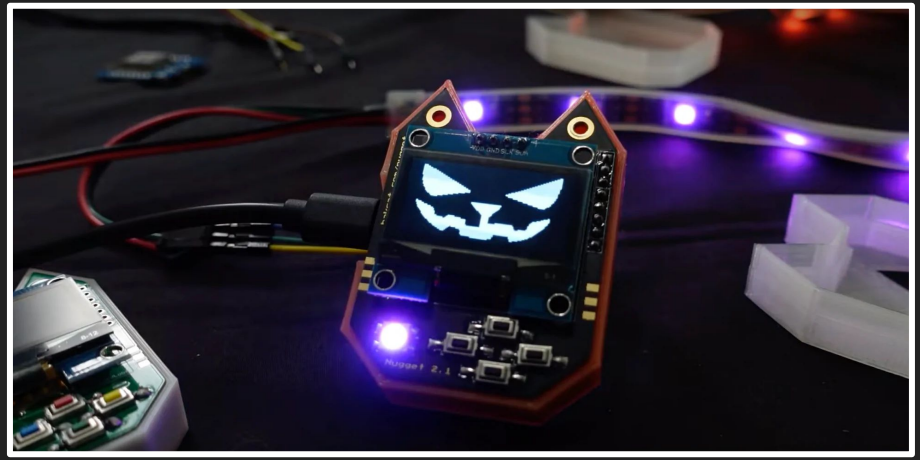
You can also edit the default WiFi credentials:





What else can the USB Nugget do?

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



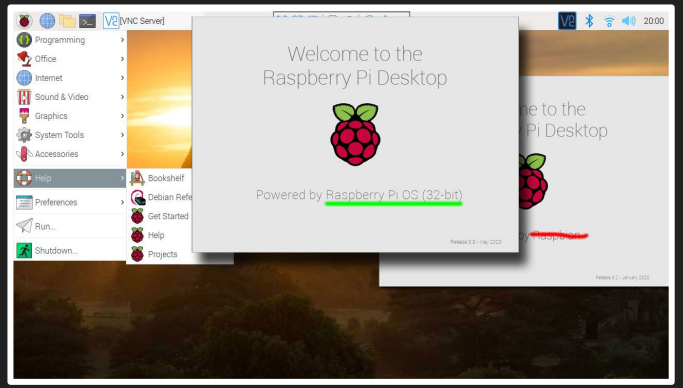
Mini Hackathon

30 Minutes

CTF: Design the Highest Scoring Payload

In our last section, we'll be working together to write payloads to win a prize!

- Our target is a Raspberry Pi computer running Raspbian.
- Your goal is to make a payload that does the most number of bad things.



Attack Criteria

For our final challenge, we'll be dividing into teams and working on HID attack scripts to achieve a number of specific goals.

Each team will get time to write their script, and then 90 seconds to plug in and run their script.

The team to earn the most number of points wins a prize! Points are awarded when a team achieves the actions below:

Points	File Operations	Flags	Destruction	Advanced (x 2 points)
10	Create a text file with a message	Display a message demanding bitcoins	Reboot or shut down the computer	Create a Cron Task
20	Delete a file	Change the Wallpaper	Kill the network connection	Download & execute a bash or Python file
30	Download a file to the desktop	Get a Grabify link hit from the target computer	Kill the computer (No boot)	Steal data via Grabify
40	Create a fork bomb	RickRoll in a browser window	Create startup task that shuts down computer	Join an (evil) Wi-Fi network
50	Steal a file off the computer	Change RPI's SSH MOTD Banner to your team name	Encrypt files or the file system (ransomware)	Netcat backdoor (remote access)

Bonus Payloads

- Exfiltrate all files containing “crypto” or “password” in the name - 30 points
- Exfiltrate network info to canarytokens - 40 points
- Create a cron job that exfiltrates something periodically - 50 points
- Download and run a python script from the internet - 30 points

Points	File Operations	Flags	Destruction	Advanced (x 2 points)
10	Create a text file with a message	Display a message demanding bitcoins	Reboot or shut down the computer	Create a Cron Task
20	Delete a file	Change the Wallpaper	Kill the network connection	Download & execute a bash or Python file
30	Download a file to the desktop	Get a Grabify link hit from the target computer	Kill the computer (No boot)	Steal data via Grabify
40	Create a fork bomb	RickRoll in a browser window	Create startup task that shuts down computer	Join an (evil) Wi-Fi network
50	Steal a file off the computer	Change RPI's SSH MOTD Banner to your team name	Encrypt files or the file system (ransomware)	Netcat backdoor (remote access)

Example Actions

- Steal a file
- Delete a file
- Write a file with a message in it
- Steal a hash
- Corrupt a hash
- Kill the computer
- Plant a keylogger
- Rickroll
- Join rogue Wi-Fi network
- Team ASCII banner
- Grabify link tracker
- Cron task
- Netcat backdoor
- Change background
- Auto-restart computer
- Auto-quit programs

Links to USB Rubber Ducky Payloads

- Payload - Non-Malicious Auto Defacer
- Payload - Lock Your Computer Message
- Payload - Ducky Downloader
- Payload - Ducky Phisher
- Payload - FTP Download / Upload
- Payload - Restart Prank
- Payload - Silly Mouse, Windows is for Kids
- Payload - Windows Screen rotation hack
- Payload - Powershell Wget + Execute
- Payload - mimikatz payload
- Payload - MobileTabs
- Payload - Ugly Rolled Prank
- Payload - XMAS
- Payload - Pineapple Assocation (VERY FAST)
- Payload - Remotely Possible
- Payload - Batch Wiper/Drive Eraser
- Payload - Generic Batch
- Payload - Paint Hack
- Payload - Local DNS Poisoning
- Payload - Deny Net Access
- Payload - RunEXE from SD
- Payload - Run Java from SD
- Payload - Download mimikatz, grab passwords and email them via gmail
- Payload - Hotdog Wallpaper
- Payload - Android 5.x Lockscreen
- Payload - Chrome Password Stealer
- Payload - Website Lock
- Payload - Windows 10 : Download & Change Wallpaper
- Payload - Windows 10 : Download & Change Wallpaper another version
- Payload - Windows 10 : Download and execute file with Powershell
- Payload - Windows 10 : Disable windows defender
- Payload - Windows 10 : Disable Windows Defender through powershell
- Payload - Windows 10 : Wifi, Chrome Dump & email results
- Payload - Windows 7 : Logoff Prank
- Payload - Netcat Reverse Shell
- Payload - Fake Update screen
- Payload - Rickroll
- Payload - Fast Meterpreter
- Payload - Data-Exfiltration / Backdoor
- Payload - Fake Update screen
- Payload - OSX Sudo Passwords Grabber
- Payload - OSX Root Backdoor
- Payload - OSX User Backdoor
- Payload - OSX Local DNS Poisoning
- Payload - OSX Youtube Blaster
- Payload - OSX Photo Booth Prank
- Payload - OSX Internet Protocol Slurp
- Payload - OSX Ascii Prank
- Payload - OSX iMessage Capture
- Payload - OS X Wget and Execute
- Payload - OSX Passwordless SSH access (ssh keys)
- Payload - OSX Bella RAT Installation
- Payload - OSX Sudo for all users without password
- Payload - MrGray's Rubber Hacks
- Payload - Copy File to Desktop
- Payload - Youtube Roll
- Payload - Disable AVG 2012
- Payload - Disable AVG 2013
- Payload - EICAR AV test

Thanks for coming!

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