**Flipper Zero - badUSB**

**What is the use case for this?**

Accessing the shell means having control over much of the computer. Connecting the flipper zero to a computer to execute commands is a quick way to make it vulnerable to networked attacks. Methods like creating a reverse shell can be done with a badUSB.

**Creating a Reverse Shell**

* See Slides for badUSB script
* Find an appropriate payload (or create your own) and edit it with your own attacker box IP and netcat listening port.
  + <https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md>
* Create a local server to host the payload
  + php -S 0.0.0.0:80 -t [directory]
* Set up a listener on the attacker machine.
  + while true; do nc -l -p 1337; done
* Execute payload on the victim machine by using the Flipper to input reverse shell commands.
* The attacker machine now has a shell to the victim machine.
* More info at <https://docs.flipperzero.one/bad-usb>