Ethical Student Hackers

Bad USB

SHEFFIELD ETHICAL STUDENT HACKERS

The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.

- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.

- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.

- Relevant UK Law: https://www.legislation.gov.uk/ukpga/1990/18/contents

Code of Conduct

- Before proceeding past this point you must read and agree to our Code of Conduct - this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.
- Code of Conduct can be found at https://shefesh.com/downloads/SESH%20Code%20of%20Conduct.pdf

Arduino IDE

We will be using the arduino IDE later in this session. Please start installing it now.

https://www.arduino.cc/en/software

In-person attacks

In person attacks can be done to make exploitation easier, as it can increase the attack surface of your target.

Many in person attacks require you to be in restricted areas (Where all the juicy data is!), while some just require you to trick someone into doing something (Social Engineering).

Some in person penetration testing techniques include tailgating into a facility, lock picking, RFID cloning, bypassing security gates and dropping malicious USB's

Hotplug attacks

- By default, most operating systems trust peripherals that are plugged into a computer, as the computer expects the user to be using them in order to input data. However this is not always the case and we can exploit this!
- There are a large number of ‘hotplug attacks’ that can be performed on computers simply by plugging a device into them. The most notable examples are made by the penetration testing company Hak5 that include (https://hak5.org/collections/hotplug-attack-tools):
    - USB Rubber Ducky - A ‘dumb’ device that emulates a keyboard, has no contextual awareness
    - Bash Bunny - A smart device that can emulate keyboards, USB mass storage, is a mini linux box, BLE, Ethernet emulation,
    - Shark Jack - A mini linux box, interface via ethernet, perform recon
    - Plunder bug LAN tap - Ethernet passthrough device to packet sniff connections

Images from Hak5 (Hak5.org)

Keyboard Emulators

These are some of the most common hotplug attacks. Why? Variability

A keyboard emulator acts exactly like a physical keyboard. But can type far faster than a human can!

This makes them perfect for:

- Getting very quick root/administrator reverse shells
- Automating time consuming tasks
- Quickly disabling windows defender
- Run a keylogger (via a script)
- Grab WiFi credentials

They're programmable, meaning you can create your own custom scripts to run and execute (or take some from GitHub)

Preventing attacks

Human behaviour

- Education on devices
- Access and visibility of IT services
- Dedicated secure areas
- Physical security (including surrounding areas) and reporting suspicious behaviour

Technical Solutions

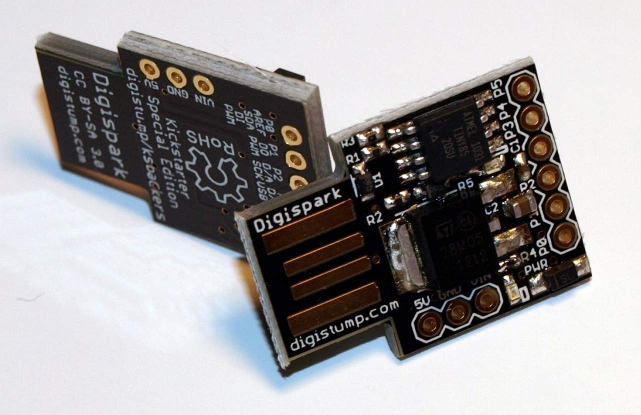
- Disable ports - hardware and software
- Require confirmation for new devices
- Antivirus and firewall
- Disabling unnecessary tools

DigiSpark Practical

Digiparks are small USB microcontrollers, a tiny computer that is programmed to do one or two tasks.

They have limited storage so cannot be used to read data off a computer

They are cheap, around £3-4



DigiSpark Setup

For Windows, use https://startingelectronics.org/tutorials/arduino/digispark/digispark-windows-setup/

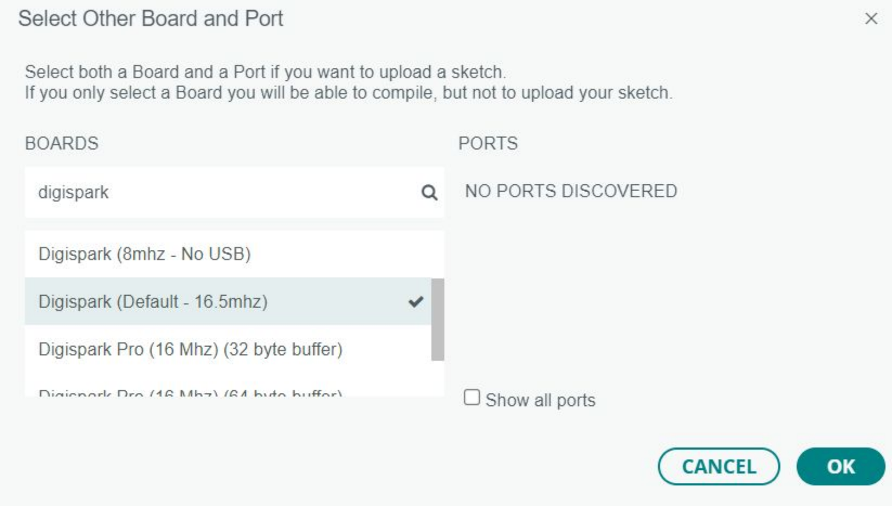
- Install Arduino IDE
- Install additional board configuration
- Install drivers

For Linux, use https://startingelectronics.org/tutorials/arduino/digispark/digispark-linux-setup/

Troubleshooting notes:

- For Linux, you may not have to add yourself to the `dialout` group if it doesn’t exist for you already
- You may also have to install the `libusb compat` library for the code to compile
  - Previously using Arch Linux's pacman has worked, pacman -S libusb-compat
- https://raw.githubusercontent.com/ArminJo/DigistumpArduino/master/package_digistump_index.json - if the link in the tutorial doesnt work

Setup a DigiSpark Continued



Select Other Board and Port

Select both a Board and a Port if you want to upload a sketch.
If you only select a Board you will be able to compile, but not to upload your sketch.

BOARDS

digispark

- Digispark (8mhz - No USB)
- Digispark (Default - 16.5mhz) ✓
- Digispark Pro (16 Mhz) (32 byte buffer)
- Digispark Pro (16 Mhz) (64 byte buffer)

PORTS

NO PORTS DISCOVERED

□ Show all ports

This is the board you want to select before you put the digispark into your computer.

Once the program is uploaded, take the device out of the computer. The next time you put the device into any computer, the program will run.

Tasks

- Display hello world on the screen
- Open the command prompt/terminal
- Run a terminal command - BE CAREFUL WITH THIS!!

Stuck? This can help (ignore the setup section)

https://securityqueens.co.uk/digispark-programming/

List of key mappings: Lines 66 - 130
https://github.com/digistump/DigisparkArduinoIntegration/blob/master/libraries/DigisparkKeyboard/DigiKeyboard.h

Some cool DigiSpark scripts (RUN AT OWN RISK): https://github.com/CedArctic/DigiSpark-Scripts

Feedback

Please leave your feedback :) We want to know what we can do to improve.

Please leave constructive and honest feedback only.

https://forms.gle/VTYd74K5BHqbC7F68

Upcoming Sessions

What's up next?

www.shefesh.com/sessions

Compsoc collab

DRM

Cryptography (same day as the AGM)

Psychology collab - social engineering

Any Questions?

www.shefesh.com

Thanks for coming!