Ethical Student Hackers

Bad USB 2

AGM Application

https://forms.gle/an5opmCGFdaAQex98

Want to be part of our AMAZING committee?

Sign up NOW

Our AGM will be the 20th April, the first Monday

After Easter.

ROLES AVAILABLE

Our Roles are:

- President
- Secretary
- Treasurer
- Inclusions Officer (Electric Boogaloo edition!)
- Competitions Officer
- Technical Officer

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

Alumni Fund

The funding for these Malduinos was provided by the Alumni of TUOS

Thank you very much!

This is expensive kit, please respect it and look after it. Each unit costs £35 (plus delivery!). Please respect them.

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

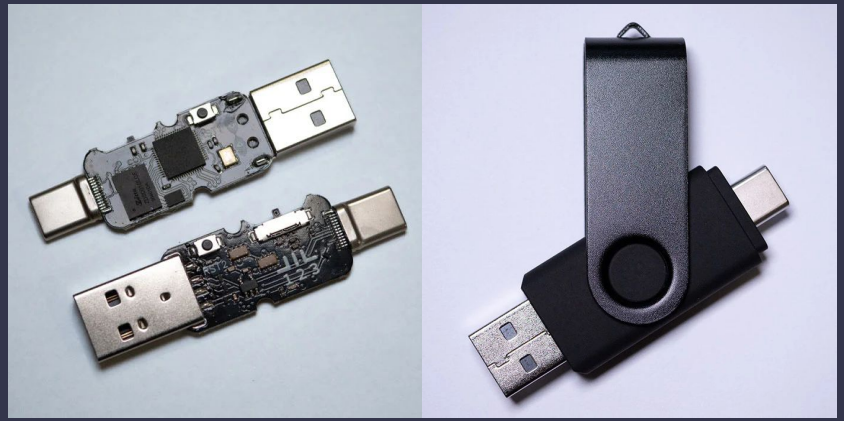
- Disable ports - hardware and software
- Require confirmation for new devices
- Antivirus and firewall
- Disabling unnecessary tools

Malduino Practical

We are using Malduino 3s, which are arduino based BadUSBs

They have 128MB of flash storage so you can extract small files

They around £35 each, much more expensive than the digisparks (please don't break them)



How to use the Malduinos

Each Malduino has a switch with three options.

Options 1 and 2 correspond to scripts, which will execute as soon as you plug them in.

Option 3 allows you to access the scripts and preferences file.

The script can be edited with any text editor (e.g vscode, notepad)

On the preferences file, change “default_layout” to GB

Tasks

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

DuckyScript Documentation:
https://docs.hak5.org/hak5-usb-rubber-ducky/duckyscript-quick-reference/

Malduino Script Documentation:
https://docs.maltronics.com/badusb-scripting/the-basics

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

Inclusions Concerns

If there's anything preventing you from enjoying our sessions, please let our Inclusions Officer know. You can contact them by email or fill in the form below:

jgledhill2@sheffield.ac.uk

https://forms.gle/Qct6Wyfesv8dWmej7

AGM Application

https://forms.gle/an5opmCGFdaAQex98

Want to be part of our AMAZING committee?

Sign up NOW

Our AGM will be the 20th April, the first Monday

After Easter.

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!