UWE Bristol | University of the West of England

CISSE

Phil Legg,
Alan Mills,
Ian Johnson

Teaching Offensive and Defensive Cyber Security in Schools using a Raspberry Pi Cyber Range

UWE cyber Gold Award

in association with National Cyber Security Centre

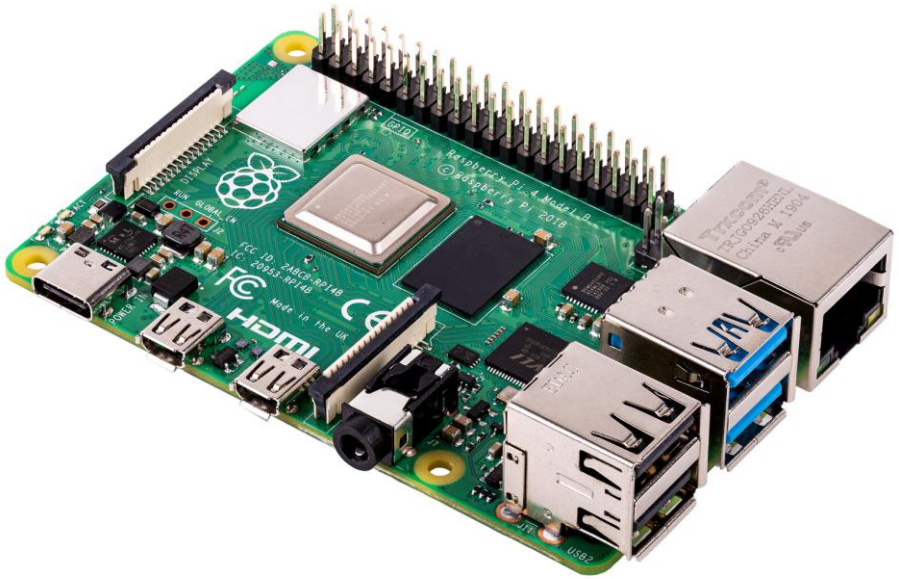
Department for Digital, Culture, Media & Sport

Academic Centre of Excellence in **Cyber Security Education**

14th November 2022

Overview

1. Problem statement
2. Proposed Pi Lab environment
3. Use case for teaching
4. Discussion and Conclusion



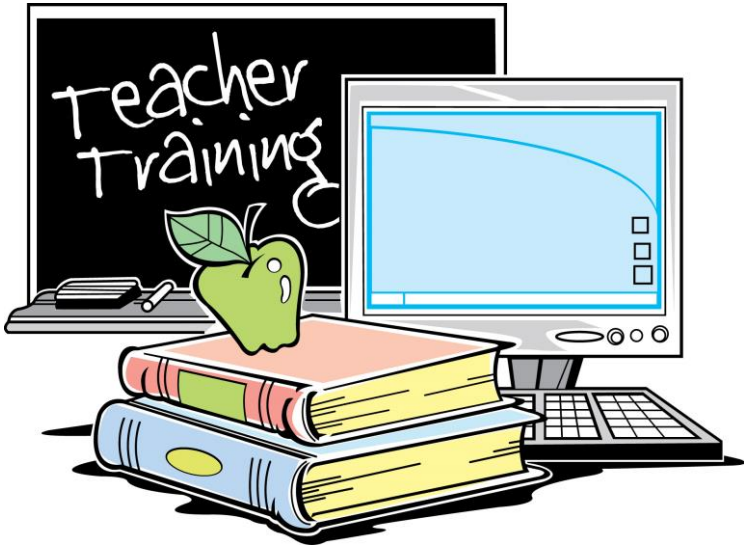
Problem Statement

- We hosted a set of teacher workshops to best understand the challenges they face, and to **co-create** practical teaching materials.
- Teachers remark on lack of time, lack of resources, and in some cases, lack of confidence.
- Constrained by curriculum demands that do not allow time to explore topics in sufficient detail with clear practical examples.

Problem Statement

- **Can we provide a "starting block" for teachers to build from, to develop their own practical teaching resources?**

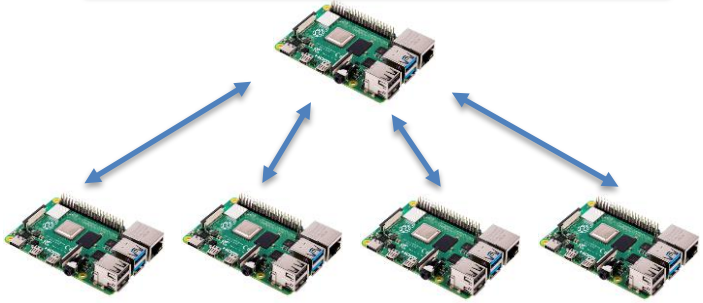
- **Can we support this at multiple levels of teacher confidence?**
  - **A low confident teacher may just want the prepared "starting block".**
  - **A high confidence teacher could extend this much further.**



UWEcyber Pi Lab

- Portable solution - not reliant on any school infrastructure
- Single and multiple machine setup – can be used for individual and group learning
- Easy to rebuild – a safe environment to tinker without fear
- Cost-effective – RPi4 starts approx. $35
- Networked – pre-configured for RPi access point for offensive/defensive exercise.

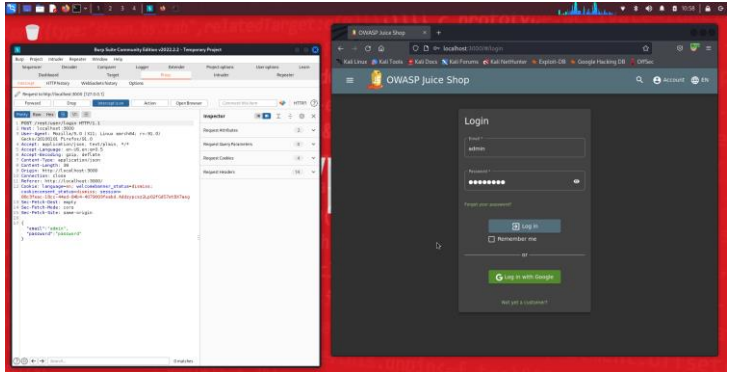
Wireless Access Point PiLab Image

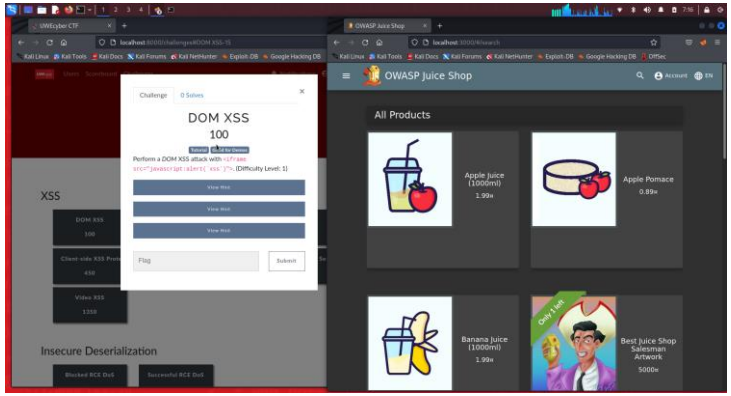


Multiple Student PiLab Images

UWEcyber Pi Lab – Pre-install

- We pre-configure the PiLab with existing tools:
  - Kali Linux is the base OS for UWEcyber PiLab image
  - Docker container deployment
  - "OWASP Juice Shop" container
    - Suitable for demonstrating Injection and Brute Force attacks
  - "CTFd" container
    - Enable student competitions on Juice Shop
  - Burp Suite and other additional tools

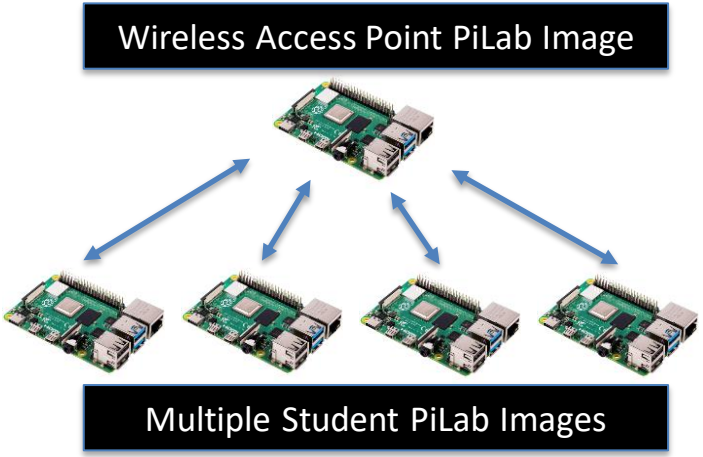




Multi-machine case study

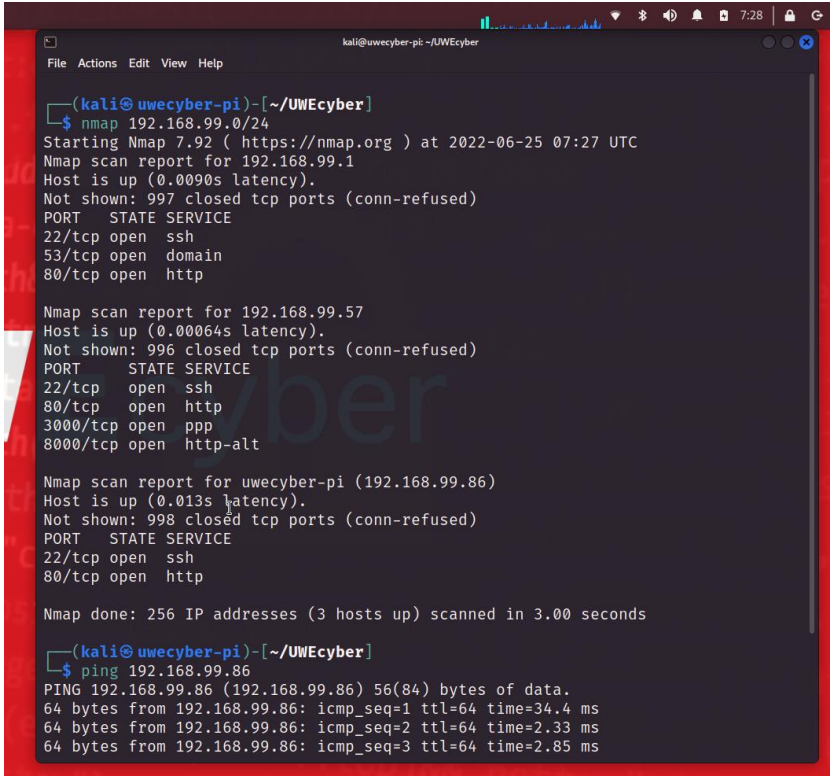
- **What about a multi-machine use case?**

- We provide a simple case study that teachers can follow as part of a structure lesson on offensive and defensive security



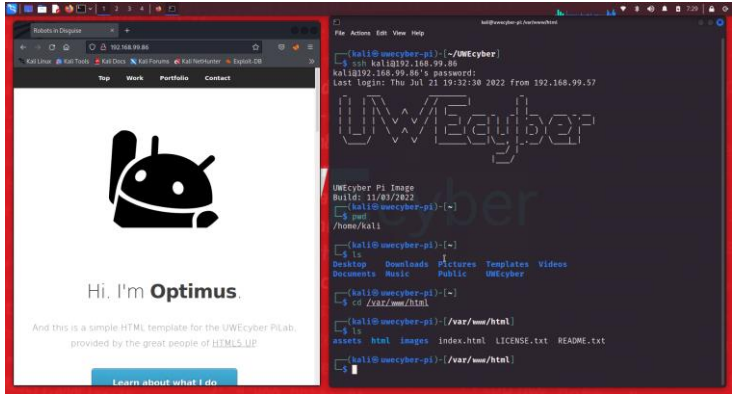
Multi-machine case study

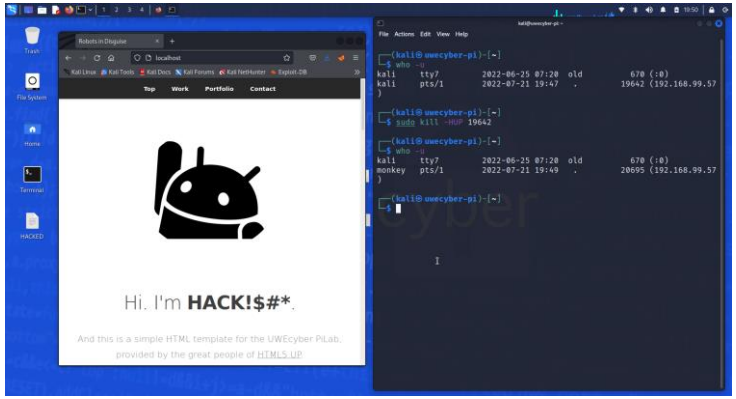
- **Nmap (Network Mapper)**
  - Students can scan the network to identify other connected devices, and to uncover what service ports are available on these devices.
  - Teacher may have allocated an attacking "red" team, and a defensive "blue" team for the purpose of the directed activity.



Multi-machine case study

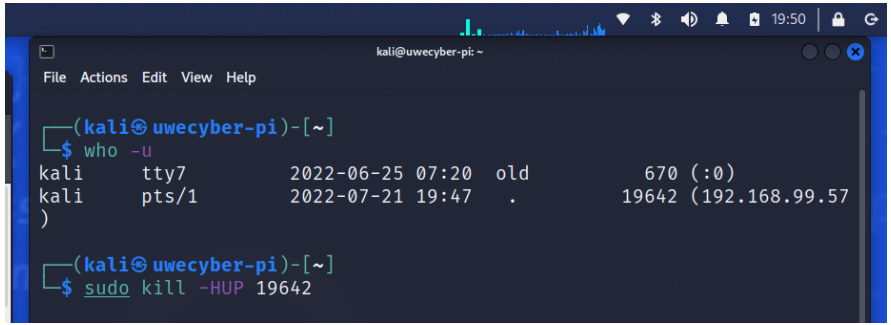
- **Remote Access and Defacement Attack**
  - All devices begin with the default kali:kali credentials.
  - Initial reconnaissance scan can be used to identify the web server running on each PiLab device.
  - Attacking team can try to "deface" the website of the defensive blue team by gaining access via SSH, and modifying the index.html page being served.





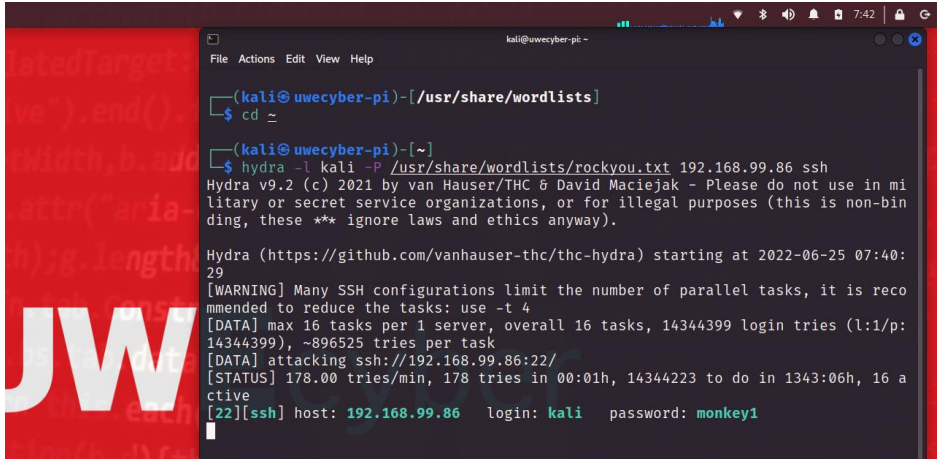
Multi-machine case study

- **Defensive strategy**
  - Blue team may be able to find "who" is connected by SSH.
  - They can then also "kill" their network connection.
  - They may want to change their password with "passwd".
  - For the purpose of the structured activity, *we would encourage the teacher to issue a known password* – e.g., this could be randomly drawn from a hat or similar.



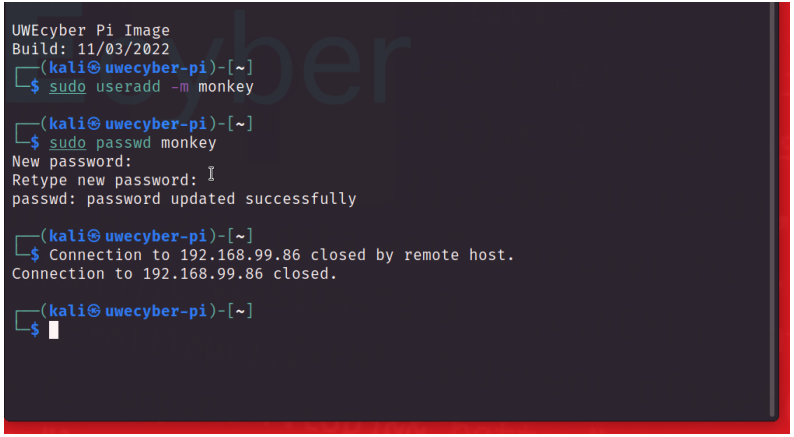
Multi-machine case study

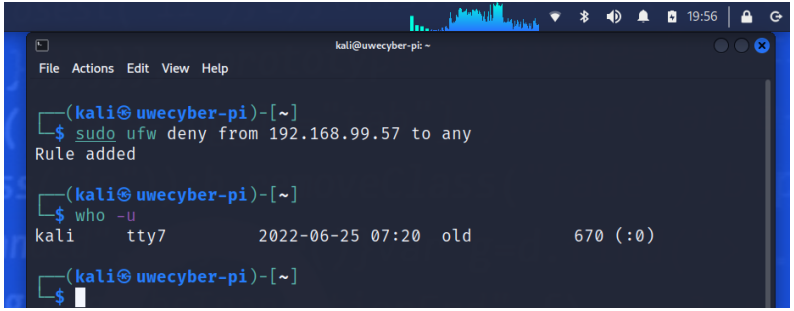
- **Brute Force Password Attack**
  - The red team can use “Hydra” to brute force the new password for the blue team SSH.
  - Since the password appears in a known breach list, we can uncover this.



Multi-machine case study

- **Additional Tasks**
  - Red team could also create a new user on the target machine for the blue team to identify.
  - Blue team could "kick" the attackers off the system again, and could hide the SSH server on a different port.
  - Blue team may use ufw (uncomplicated firewall) to block the malicious IP address completely





Discussion

- Teachers liked the platform and the extensibility offered, whilst also having some pre-prepared activity to get started with.
- Use case is intended to be a relatively simple attack-defend scenario whilst also giving scope to teachers to tailor it for specific age range in their class.
- Use case covers a wide variety of *fundamentals* including IP addresses, networking basics, and linux command line tools.
- Group-based tasks as well as single user tasks (e.g., Juice Shop) appeal to teachers as extension activities for students to explore.

Resources

- All Pi Lab SD card images, and associated workshop materials available online at:

  http://www.cems.uwe.ac.uk/~pa-legg/resources/teachers/

- We would be keen for the community to make use of this material, and to provide comments and feedback on how it can be improved further.

Thank you for listening

Prof. Phil Legg
Professor in Cyber Security
Co-Director of UWEcyber
(NCSC Academic Centre of Excellence in Cyber Security Education)

Phil.Legg@uwe.ac.uk
http://www.plegg.me.uk
http://go.uwe.ac.uk/phil