Inaugural National Teaching Ethical Hacking Workshop

27th February 2025 at Abertay University

Schedule

Time	Location	Topic	Speaker
10:00	Abertay University, Old College Building, Rooms 2021 & 2022	Introduction	Jamie O’Hare (Abertay University)
10:15		Cyber Ranges for Cybersecurity Training*	Prof. Shahid Raza & Dr Jeremy Singer (University of Glasgow)
10:30		Procurement of a Cloud-based Virtual Hacking Lab*	Prof. Andreas Aßmuth (Kiel University of Applied Sciences)
10:45		OpenNebula: Our proposed VDI-based Hacklab	Dr Karl Van Der Schyff (Abertay University)
11:00		**Discussion**	
11:15		**Break**	
11:30		CHERI for Memory Safety: Research-Led Teaching in Cybersecurity	Dr Jeremy Singer (University of Glasgow)
12:00		Cyber Physical System Education Through Project Based Learning	Jenny Highfield & Alex Deverson (Cardiff University)
12:30		Revamping Our Core Penetration Testing Module	Luke Weatherby-Boon (Abertay University)
13:00		**Discussion**	
13:15		**Catered Lunch**	
14:00		Insights from a Black Hat EU Scholarship Experience*	Neil Moir (Abertay University)
14:15		Hacking, Ethics, and Exclusion*	Dr Natalie Coull & Jamie O’Hare (Abertay University)
14:30		**Discussion**	
14:45		**Break**	
15:00		Creating Authentic Command Line Interfaces in LaTeX	Jamie O’Hare (Abertay University)
15:15		Developing Dynamic Linux Privilege Escalation Challenges with Docker	Jonathan White & Alan Mills (University of the West of England)
15:45		**Discussion**	
16:00		Wrap-up	Jamie O’Hare (Abertay)

Subject to Change, *Placeholder titles

Each session concludes with an open discussion for questions and dialogue.

Abstracts

Session 1 – Teaching Environments

Cyber Ranges for Cybersecurity Training

Prof. Shahid Raza & Dr Jeremy Singer (University of Glasgow)

Academics from the University of Glasgow will present a 15-minute lightning talk on the role of Cyber Ranges in cybersecurity training and exercises. This session will explore how Cyber Ranges provide realistic, hands-on environments for enhancing cybersecurity skills.

Procurement of a Cloud-based Virtual Hacking Lab

Prof. Andreas Aßmuth (Kiel University of Applied Sciences)

Our university has procured a cloud-based virtual hacking lab for 2025. I will be using this from summer semester 2025 in the Introduction to IT Security and Digital Forensics courses. I will report on my initial experiences with this new virtual hacking lab.

OpenNebula: Our proposed VDI-based Hacklab

Dr Karl Van Der Schyff (Abertay University)

This talk will introduce our proposed Virtual Desktop Infrastructure (VDI)-based Hacklab, built using OpenNebula. The session will explore how this setup for intended use in our teaching, discussing the advantages of leveraging OpenNebula for deploying virtualised lab environments, enabling hands-on learning, and facilitating realistic cyber exercises.

Session 2 – Teaching Practice

CHERI for Memory Safety: Research-Led Teaching in Cybersecurity

Dr Jeremy Singer (University of Glasgow)

At the University of Glasgow, we anticipate delivering a new Masters in Cybersecurity starting Sep 25. We are currently putting the finishing touches to our degree programme structure and intended learning outcomes. We want to integrate compelling topics from our research projects into our Masters teaching. One such example, which I will outline in this presentation, is the study of new memory-safe processor hardware. With our students, we will motivate the need for spatial and temporal memory safety, then demonstrate how CHERI systems provide these facilities in a low-overhead manner. Practical demonstrations will involve Python code on an embedded FPGA development board.

Cyber Physical System Education Through Project Based Learning

Jenny Highfield & Alex Deverson (Cardiff University)

The presentation will discuss the pedagogical approach of project based learning. Undergraduate students at Cardiff University have been involved in cybersecurity research (Operational Technology) through paid research associate roles, where they then applied their learnt skills and projects to inspire their final year dissertation projects. This talk will discuss the approach and the outcomes.

Revamping Our Core Penetration Testing Module

Luke Weatherby-Boon (Abertay University)

This talk will explore the revamp of our core Penetration Testing module (CMP210/ CMP506), focusing on enhancing hands-on learning, real-world applicability, and industry alignment. We will discuss key updates, including the integration of modern attack techniques, emerging security tools, and interactive lab environments. The session will also highlight how we've incorporated feedback from students and industry professionals to create a more engaging and effective learning experience.

Session 3 – Beyond Teaching

Insights from a Black Hat EU Scholarship Experience

Neil Moir (Abertay University)

This talk offers a firsthand account of a student's journey to Black Hat EU through the prestigious scholarship program. Sharing personal experiences, challenges, and key takeaways, this session will provide a unique student perspective on attending one of the world's leading cybersecurity conferences. From engaging with top security professionals to exploring cutting-edge research and hands-on workshops, this talk will highlight the impact of the experience on both academic and professional growth.

Hacking, Ethics, and Exclusion

Dr Natalie Coull & Jamie O'Hare (Abertay University)

This talk explores the challenges faced by cybersecurity academics when students run afoul of non-academic disciplinary actions related to hacking. Whether driven by curiosity, ethical dilemmas, or misunderstandings about cybersecurity experimentation, these situations create complex challenges for both students and educators. Drawing from our own experiences, we will examine the ethical, legal, and institutional factors that come into play when addressing these cases. Most importantly, we will discuss how the cybersecurity academic community can collaborate to develop better approaches.

Session 4 – Teaching Practice

Creating Authentic Command Line Interfaces in LaTeX

Jamie O’Hare (Abertay University)

In this quick presentation, I will showcase a LaTeX-based approach to creating authentic command-line interface callouts for educational materials. By accurately mimicking real terminal outputs and prompts, this method bridges the gap between instructional content and practical implementation. The presented LaTeX code generates realistic, clean, and fully customisable command-line interfaces, enabling educators and students to provide examples that learners can copy and paste seamlessly into their native environments without formatting issues.

Developing Dynamic Linux Privilege Escalation Challenges with Docker

Jonathan White & Alan Mills (University of the West of England)

This presentation will outline a novel method for delivering personalised, hands-on assessments in Linux privilege escalation for cyber security students. By integrating Capture-the-Flag (CTF) style challenges into a dynamic Docker environment, we ensure that each student experiences a unique set of tasks while maintaining equivalence in difficulty and learning outcomes.

Building on prior laboratory exercises, students employ a range of skills such as enumeration, reconnaissance and brute forcing to progress through multiple user accounts, culminating in root access. For each of the five flags, several scenarios of comparable complexity are randomly selected and incorporated into a lightweight Docker container. This approach substantially reduces preparation overhead compared to traditional virtual machines, ensures rapid deployment on limited hardware, and minimises opportunities for academic misconduct.