Hackademia 2025

Hackademia 2025 is Lancaster University's student run cybersecurity conference. They welcome participants of all backgrounds, regardless of whether that's a student or professional, infosec or not, anyone and everyone can come and learn.

The day started with a keynote from Jamie Ohare, 'Wrestling with Expectations', where he talked about cyber security career journeys. Jamie started out by pointing out that for university students' good grades and staying out of trouble does not guarantee a job. Success comes from making the most of your (uni) time. It's important to have an awareness of the opportunities around you, take action on those opportunities and give back to the communities and networks that help you.

Jamie had some good tips for students.   Such as Github has a student developer pack, there is a Cyberfirst bursary, a Blackhat scholarship and Objective by the sea scholarship. Also, he suggested attending conferences. There were lots of suggestions so he did ask that people remember you can't do them all. Do those that align with your aspirations but do try new things too.

Jamie has come helpful resources on getting started in the industry such as 'your career in cyber security' which can be found here: https://oha.re/.

Next up was James Bore who wants people to 'Stop buying new shit.' Apart from his book. You can buy that.

James went on to advise there's been a lot of research on the amount that should be spent on cyber security and, unsurprisingly, a lot of that research is sponsored by cybersecurity tools vendors. Who of course want you to spend more money on security tools.

There are some things James feel people should know before spending money on these things. You should know your estate and all the tools you have, and you should know what your tools are for. You need to be able to provide metrics on what the change from the new tool will provide.

The fundamental challenges have changed from the 1970s Ware report which is a report on Security Controls for Computer Systems. Requirements highlighted in that report such as access control, authentication and security as a fundamental design requirement are still relevant today.

Laurie Ibbs talked us through the timeline of the Salt Typhoon Incident next.   The most devastating breach in telecom history to date.

Lauri works for a company that is currently working on next gen 5g telecoms so understanding these types of events is important. Laurie explained that in Oct 2024 AT&T was attacked. In Nov 2024 the

FBI and CISA reported attribution. It was found that the initial access was VPN exploitation and Proxy logon. These were not zero days just exploits that were not patched. In Dec 2024 a hardening guide for communications infrastructure was published. Them in Jan 2025 the treasury sanctioned Chinese company.

There were at least 9 telecoms companies involved in the breach. A single breached admin password gave access to 1000,000 routers.

Have lessons been learned? Possibly not considering one of Salt Typhoons favourite flaws is still on 91% of exchange servers.

After this talk it was time for lunch. Greggs sausage rolls and a variety of pasties. Delicious.

Sel Robertson was up next with ‘Calling The BLUF’ about communication in a SOC. Effective communication is efficient communication that allows decision makers to have the full picture and reduces delays and misunderstandings.

The five important parts of the communication are what, where, when, who and why. What have you found, what was the activity, who is involved in what you are reporting and is affected by it and where did the actions take place. The why covers what makes it something that the receiver of the report needs to care about, what’s the possible impact.

BLUF your messages means to Bottom Line Up Front so put the important information first then the explanation after. Be clear and concise but be sure to include what needs to be known, what needs to be done and when it needs to be done.

Isaac Harrison talked to us about ‘Kryptos, the art of cryptography’ next. Kryptos is a sculpture by the American artist Jim Sanborn located on the grounds of the Central Intelligence Agency (CIA) headquarters, in Langley, Virginia. Within the sculpture is encrypted text that are part of four cryptographic challenges. Three of these have been solved whilst K4 remains undeciphered.

Isaac gave a demonstration on how long it would take to brute force the decryption and gave an explanation on how to establish if cryptographic text may be from English text, by looking at the frequency of letters in the English language. For example, U always follows Q.

Next up was Kirsty Duncan with ‘Bits bytes and Babel: Translating Cybersecurity Across Borders. Kirsty showed how the top passwords that are known to be used can suggest a particular country. UK is qwerty numbers and then the 5th most popular password is liverpool. Whereas France has azerty in the top used passwords while China was all numbers only. Romania has parola in the top 5.

Research suggests that 31% of passwords use purely numerical sequences and now things like films are coming into prevalence. For example, last year was Sladdin66 in one country and supermario12 in Austria. So the password itself gives clues as to the owner’s country.

Kirsty also explained how different cultures communicate differently. Some are task-based others are more relationship based. The UK would prefer communication from a role whereas China might prefer someone further up in the company hierarchy.

The final talk of the day was ‘Everything’s Fucked and We’re All Going to Die’ by Mike Whitehead. Mike started by pointing out that management tend to focus on the wrong things with vulnerabilities. Numbers rather than criticality.

There are too many vulnerabilities to work on without some context around them. There tends to be an over reliance on scanning which is reactive and not proactive. It’s important to remember that vulnerability scanners don’t know all the vulnerabilities. We tend to use the NVE (National Vulnerability Database) whilst other countries databases have more vulnerabilities listed, so these are being missed when using the NVE.

Things that can help with vulnerability management is Documentation. Policies are good but they need standards to back them up. Policies evolve and need to keep up with regulations changes and best practice changes. Whatever you do, for it to be effective, you need an accurate CMDB (Configuration Management Database). To help with prioritised use the Known Exploited Vulnerabilities (KEV) DB. This lists a subset of known vulnerabilities that have been actively exploited in the wild. And use risk-based vulnerability scoring, for example, as VPR in Tenable. Most importantly know your environment.

After that it was time for Closing remarks from Tom Blue and then over to a campus bar for pizza and people networking.