

CyBOK

The Cyber Security Body Of Knowledge



Open Source CyBOK Practical Challenges and Learning Resources; and Hacktivity Cyber Security Labs

Dr. Z. Cliffe Schreuders

contact@cybok.org
www.cybok.org

Capture the Flag (CTF) for Cyber Security Education

Using hands-on hacking challenges is an effective way of engaging learners, **but building challenges is hard work.**

Typically, a created CTF challenge is **manually** created for one event and can only be used once.



SecGen: Open source framework

SecGen generates randomised VMs, meaningful security challenges, and CTF scenarios.

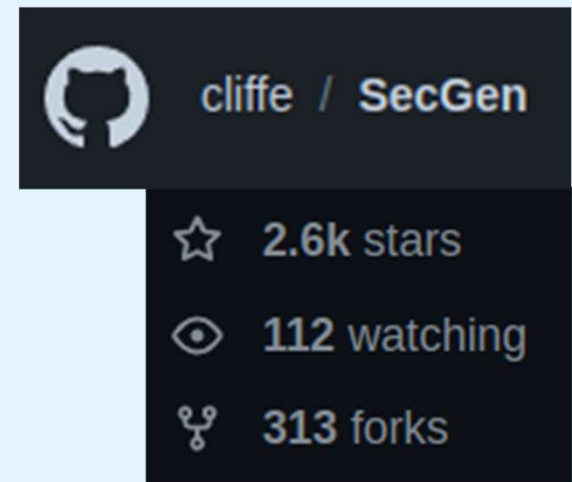
Randomisation – unlike any alternative

Code-based – rather than manual configuration

Modular design

Used internationally by universities, clubs, and events.

<https://github.com/cliffe/SecGen>



Hacktivity Cyber Security Labs

Hacktivity Cyber Security Labs is our online platform powered by SecGen.

Provides access to hacking challenges and learning content, and manages VMs.

Online lab platform, with gamification, leaderboards, easy access to VMs and security challenges.

69,282 CTF flags solved by 1849 users.

<https://hacktivity.co.uk>

Hacktivity
Cyber Security Labs


 **CYBER
+ ASAP** | Academic
Startup
Accelerator
Programme

A huge open source library of content mapped to CyBOK

150+ Labs and multi-step CTFs, with randomised CTF challenges

CyBOK enables us to understand what areas of knowledge are covered by modules

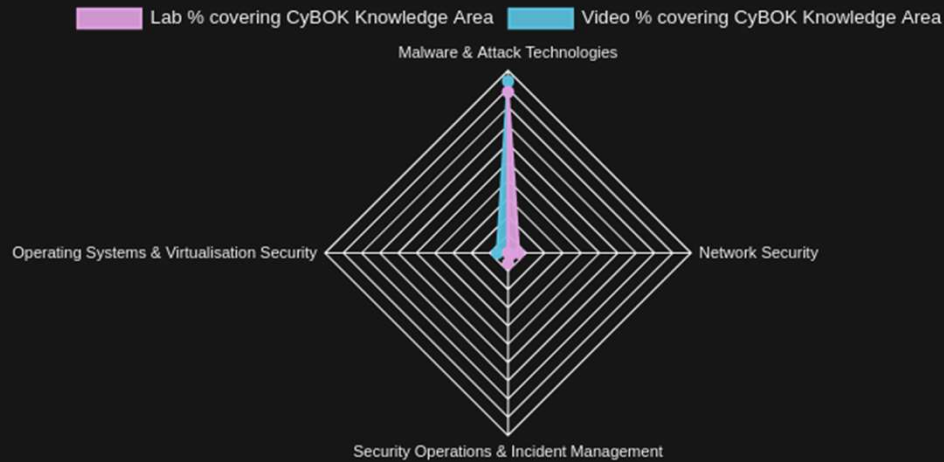
```
<CyBOK KA="AAA" topic="Authorisation">
  <keyword>access control</keyword>
  <keyword>enforcing access control</keyword>
  <keyword>ACCESS CONTROL - DAC (DISCRETIONARY ACCESS CONTROL)</keyword>
  <keyword>Vulnerabilities and attacks on access control misconfigurations</keyword>
</CyBOK>
<CyBOK KA="OSV" topic="Primitives for Isolation and Mediation">
  <keyword>Access controls and operating systems</keyword>
  <keyword>Linux security model</keyword>
  <keyword>Unix File Permissions</keyword>
  <keyword>Filesystems, inodes, and commands</keyword>
  <keyword>umask</keyword>
</CyBOK>
<CyBOK KA="OSV" topic="Role of Operating Systems">
  <keyword>mediation</keyword>
</CyBOK>
```



Modules mapped to CyBOK

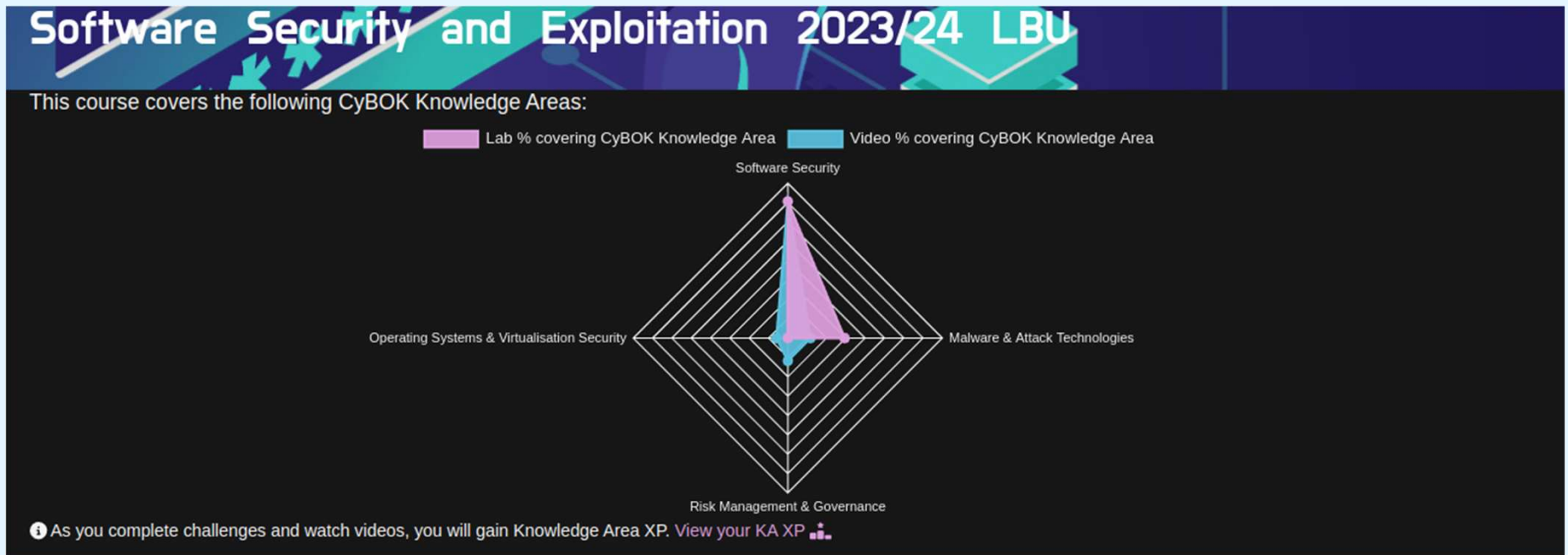
Reverse Engineering and Malware Analysis LBU 2023/24

This course covers the following CyBOK Knowledge Areas:



📌 As you complete challenges and watch videos, you will gain Knowledge Area XP. [View your KA XP](#) 📊

Modules mapped to CyBOK

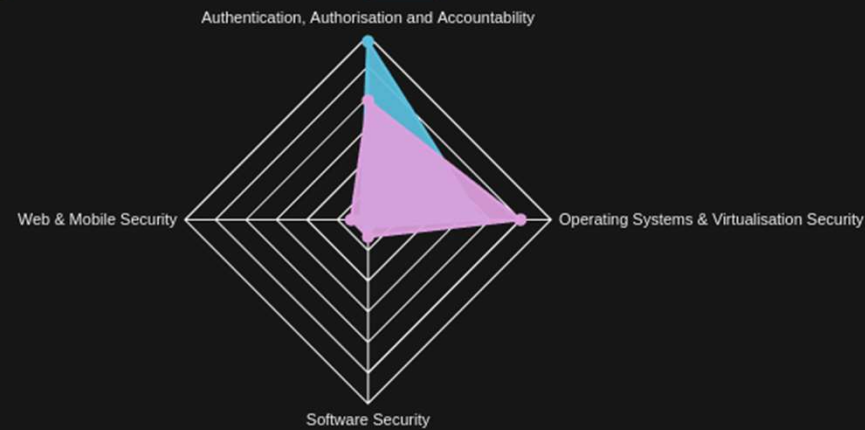


Modules mapped to CyBOK

Systems Security 2023/24 LBU

This course covers the following CyBOK Knowledge Areas:

■ Lab % covering CyBOK Knowledge Area ■ Video % covering CyBOK Knowledge Area

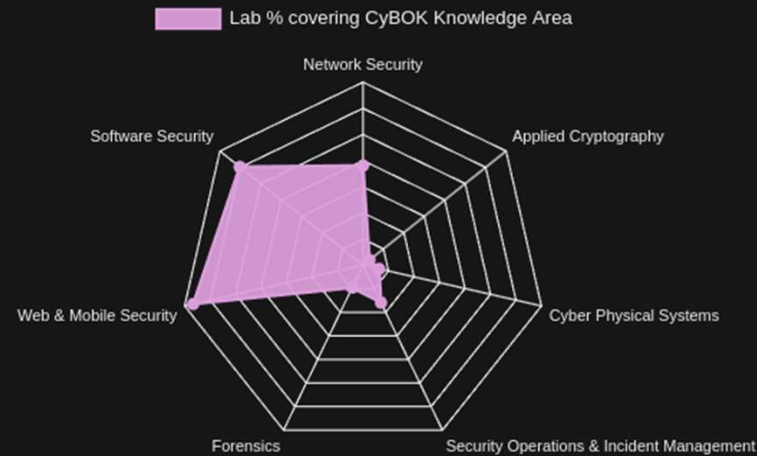


📘 As you complete challenges and watch videos, you will gain Knowledge Area XP. [View your KA XP](#) 📊

Modules mapped to CyBOK

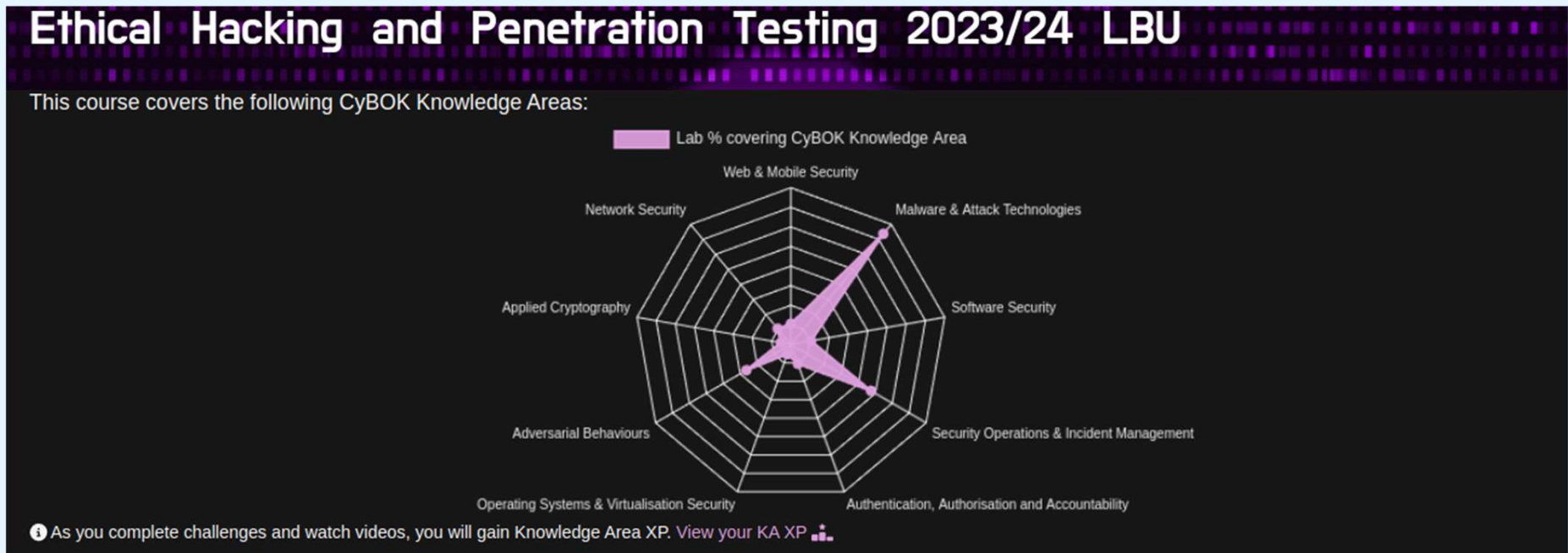
Web and Network Security 2023/24 LBU

This course covers the following CyBOK Knowledge Areas:



As you complete challenges and watch videos, you will gain Knowledge Area XP. [View your KA XP](#)

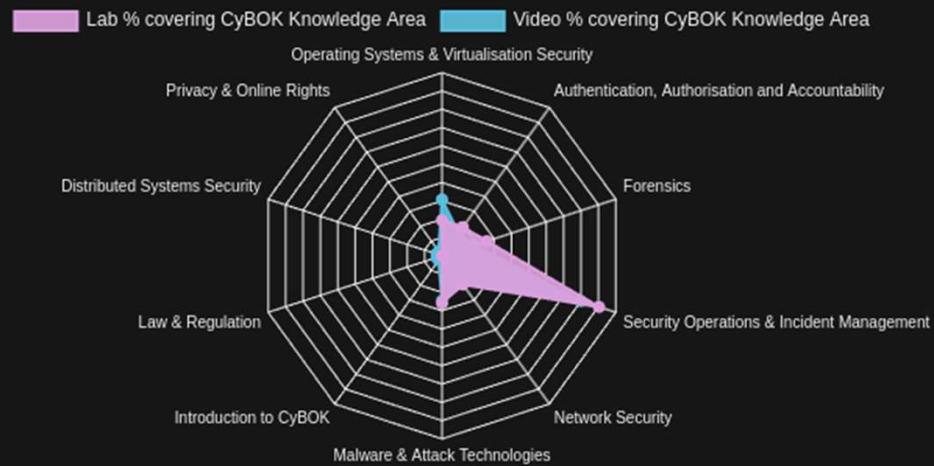
Modules mapped to CyBOK



Modules mapped to CyBOK

Incident Response and Investigation LBU 2023/24

This course covers the following CyBOK Knowledge Areas:



As you complete challenges and watch videos, you will gain Knowledge Area XP. [View your KA XP](#)

Demo time

How we use **CyBOK**

CyBOK is central to the student/user experience.

CyBOK is used:

- To describe knowledge associated with modules

- To describe knowledge associated with labs and CTFs

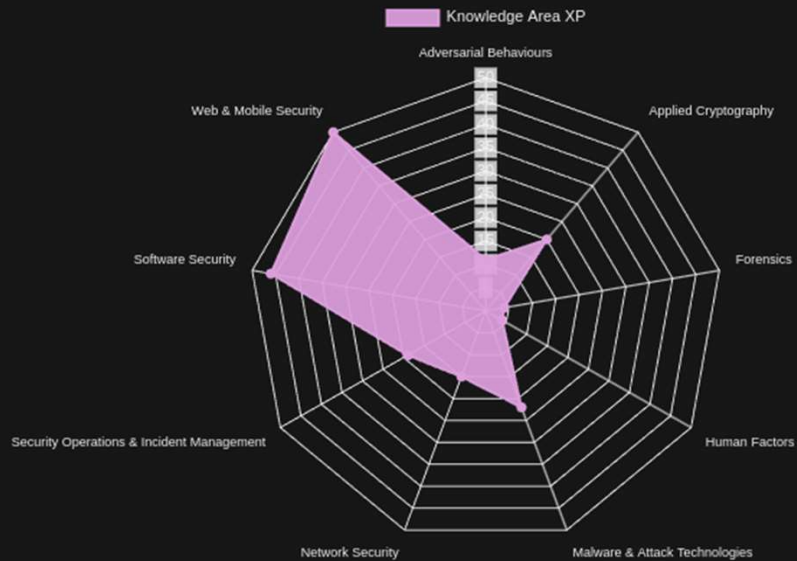
CyBOK is also used to track individual learning and progress

- To help students reflect on what they have learned.

Student #1: L5 CyBOK KAs

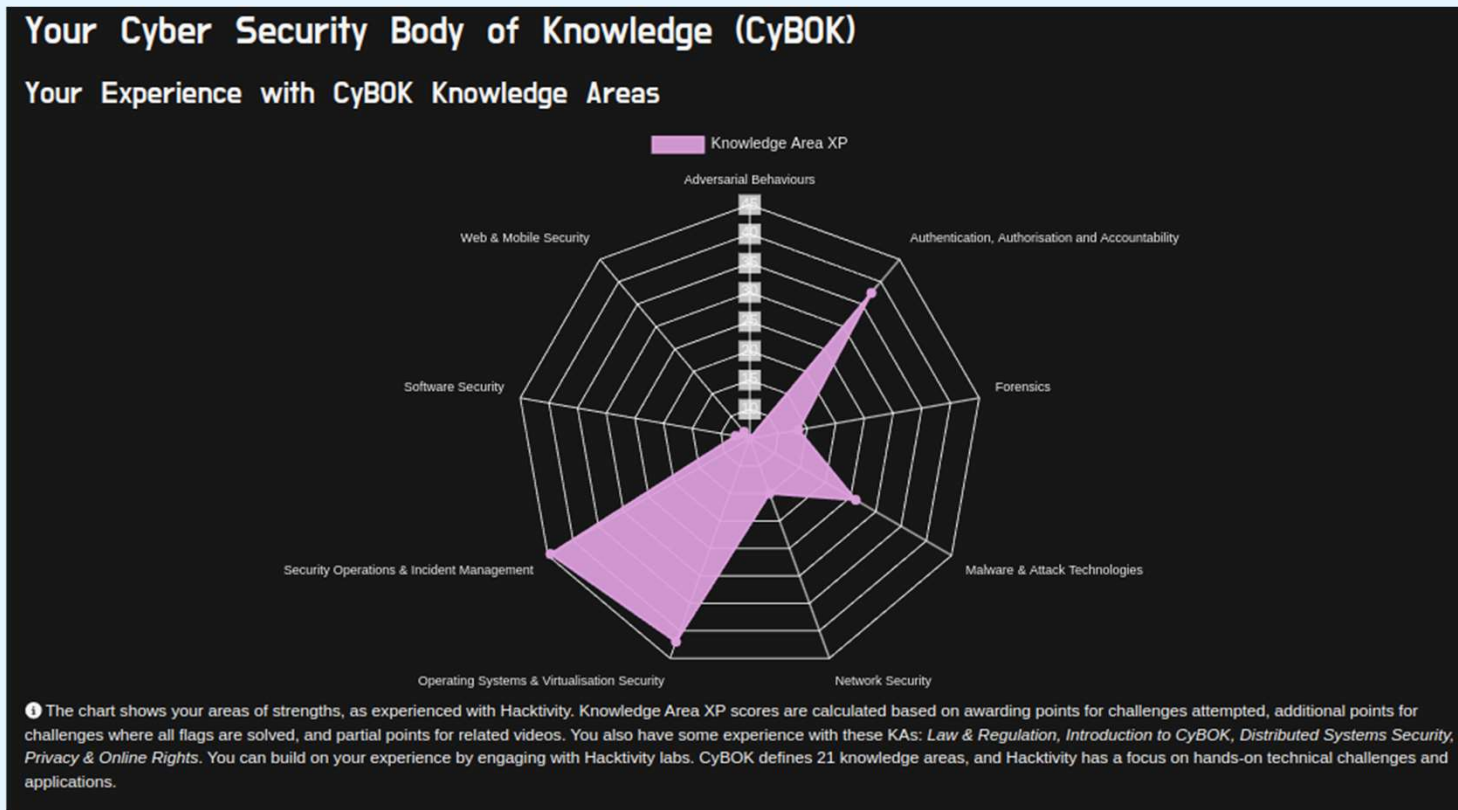
Your Cyber Security Body of Knowledge (CyBOK)

Your Experience with CyBOK Knowledge Areas

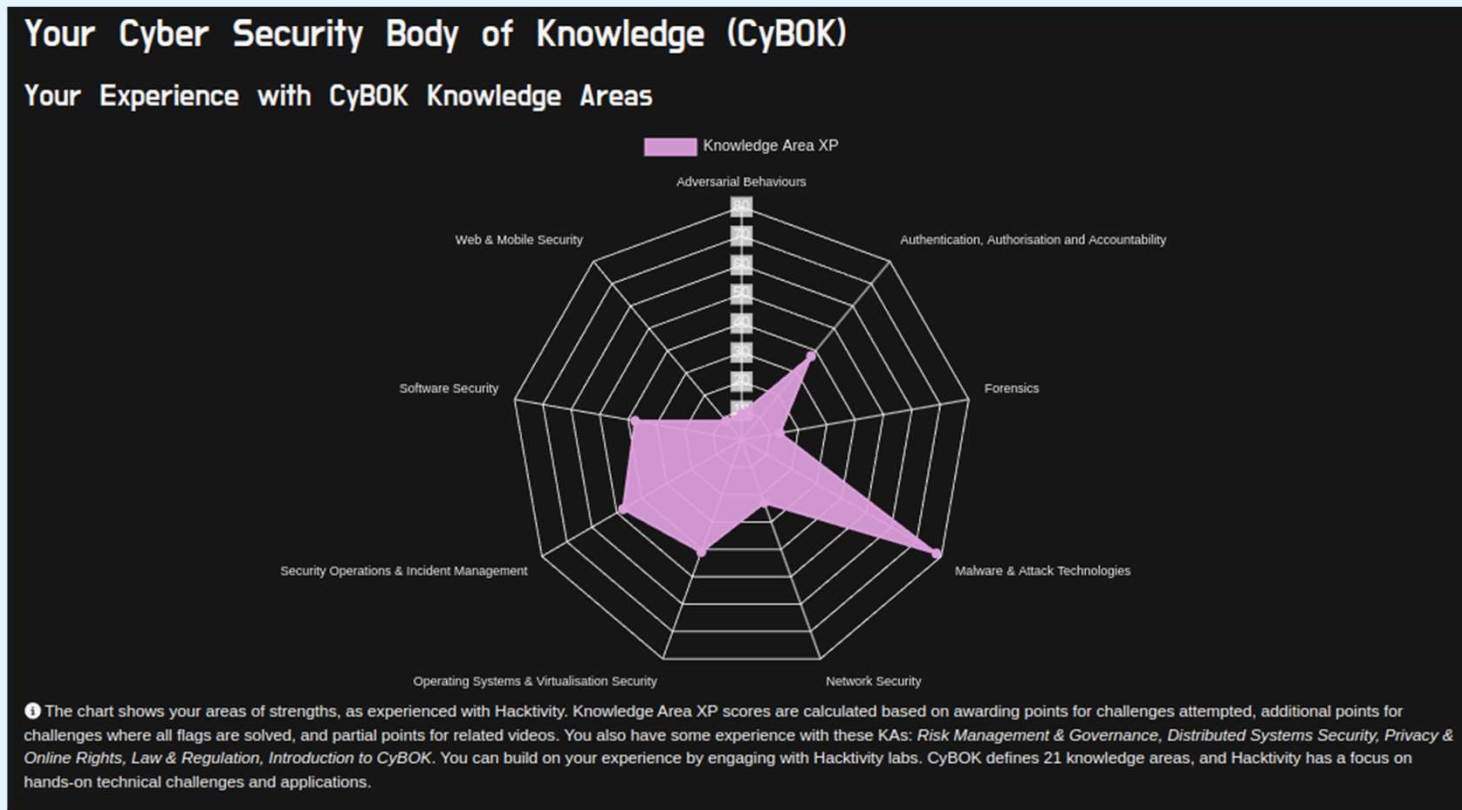


i The chart shows your areas of strengths, as experienced with Hacktivity. Knowledge Area XP scores are calculated based on awarding points for challenges attempted, additional points for challenges where all flags are solved, and partial points for related videos. You also have some experience with these KAs: *Cyber Physical Systems*. You can build on your experience by engaging with Hacktivity labs. CyBOK defines 21 knowledge areas, and Hacktivity has a focus on hands-on technical challenges and applications.

Student #2: L6 CyBOK KAs



Student #3: L7 CyBOK KAs





Conclusion

We publish extensive open source learning resources, SecGen:

<https://github.com/cliffe/SecGen>

Hacktivity provides a fully hosted user experience

with CyBOK at the forefront of the user experience

<https://hacktivity.co.uk>

CyBOK is helpful for course design and communicating where education places focus. From entire degrees through to individual training modules.

CyBOK can be used in practical situations, such as training, to help learners understand what they are learning and what concepts they are putting into practice.