



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







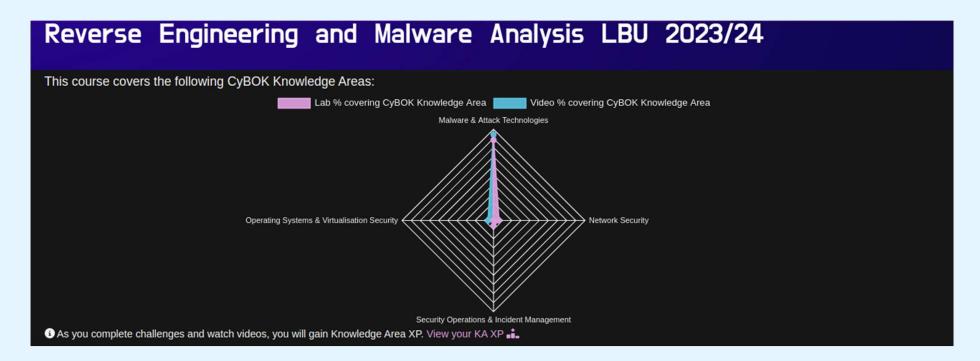
A huge open source library of content mapped to CyBOK

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

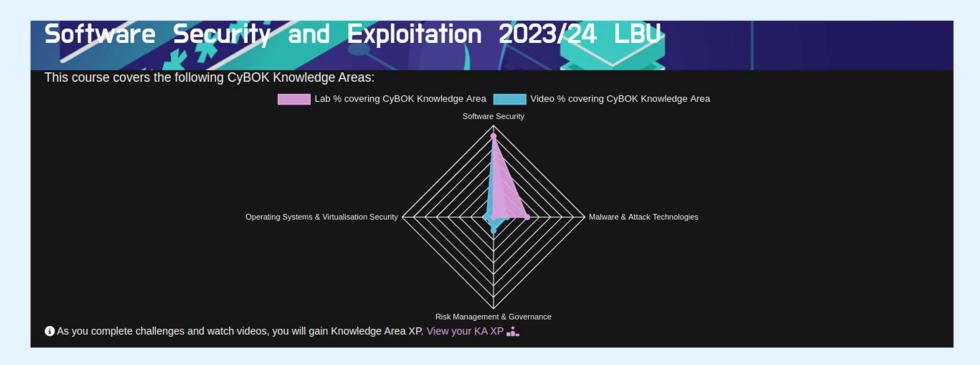
CyBOK enables us to understand what areas of knowledge are covered by modules

```
<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>
</CVBOK>
```

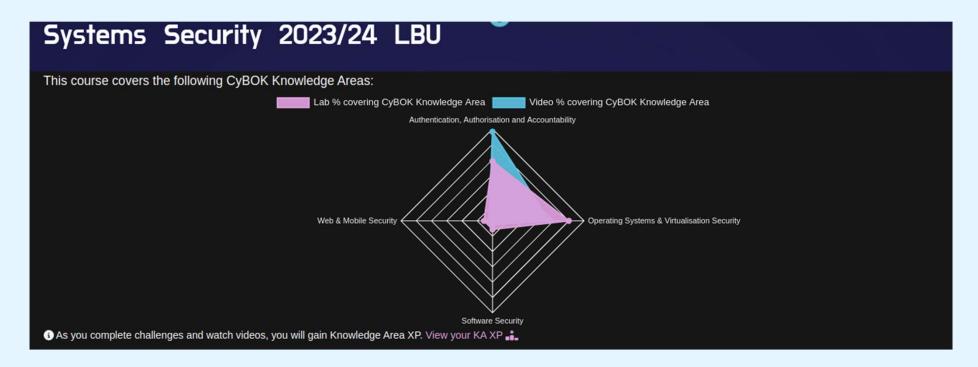








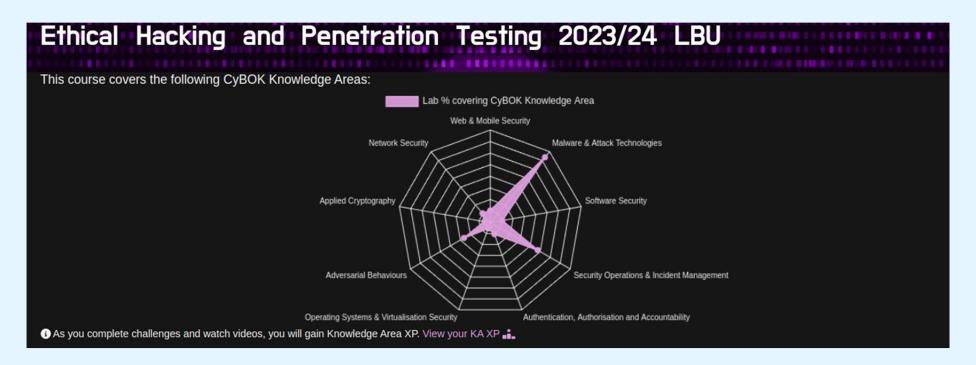
















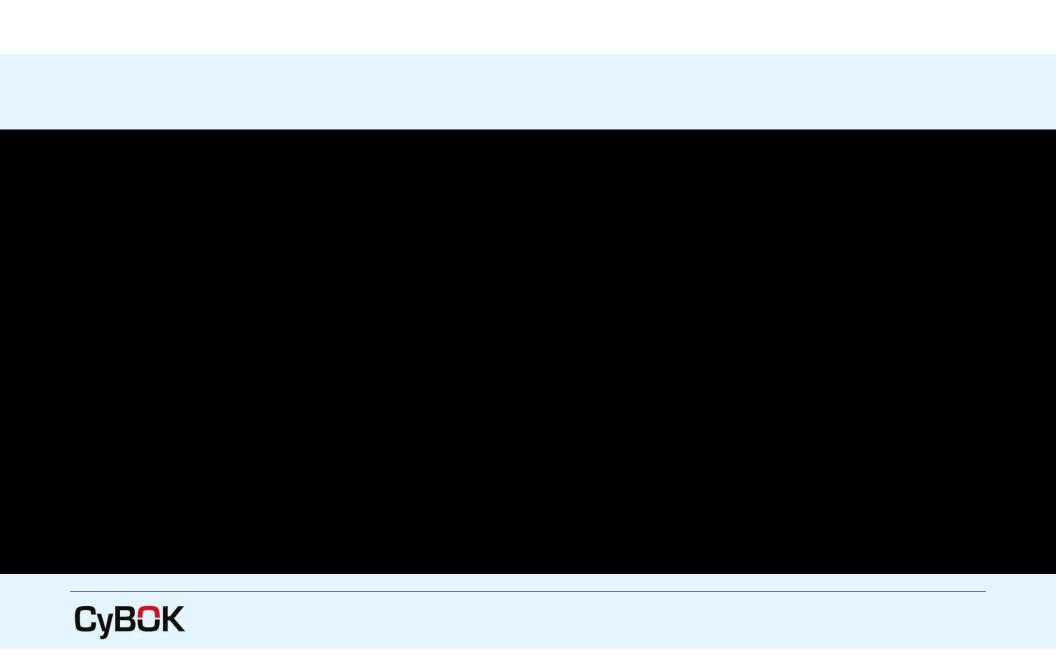


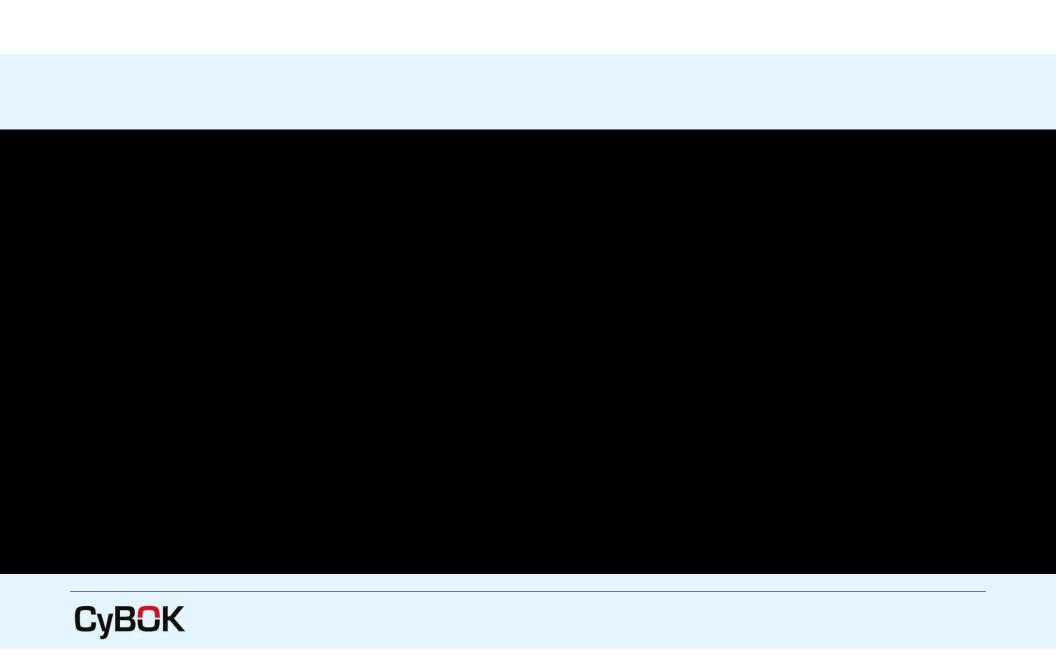
Demo time

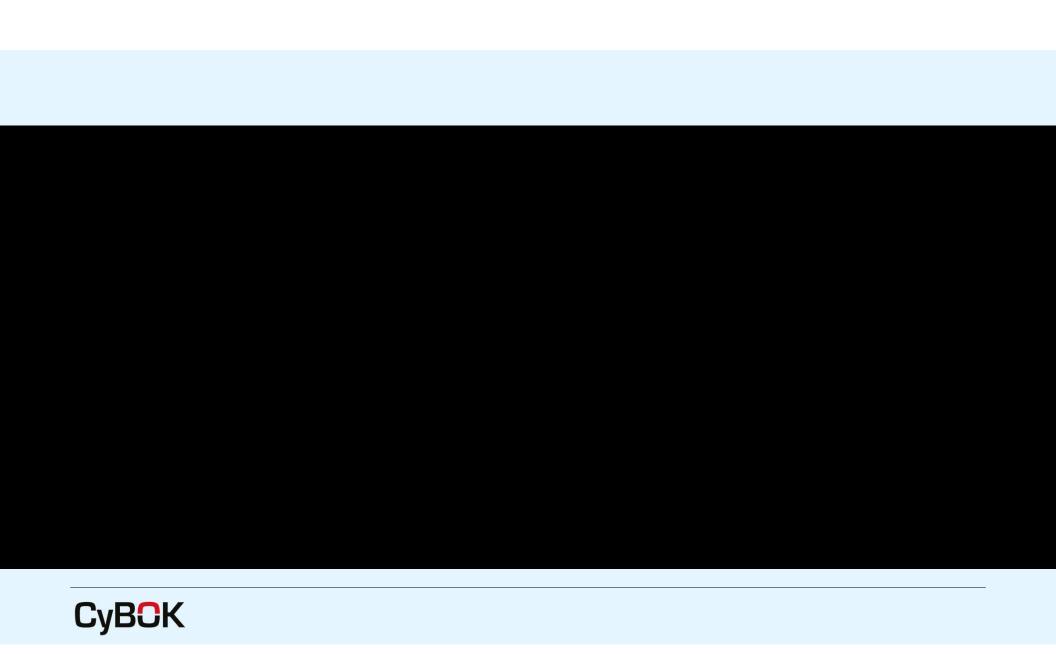












How we use **CyBCK**

CyBOK is central to the student/user experience.

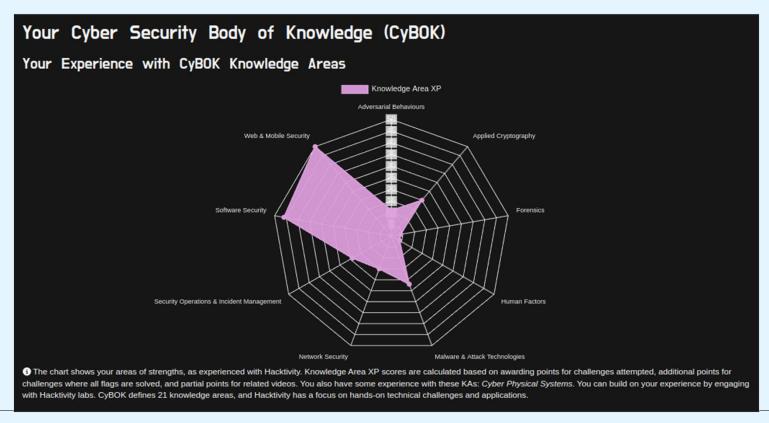
CyBOK is used:

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.

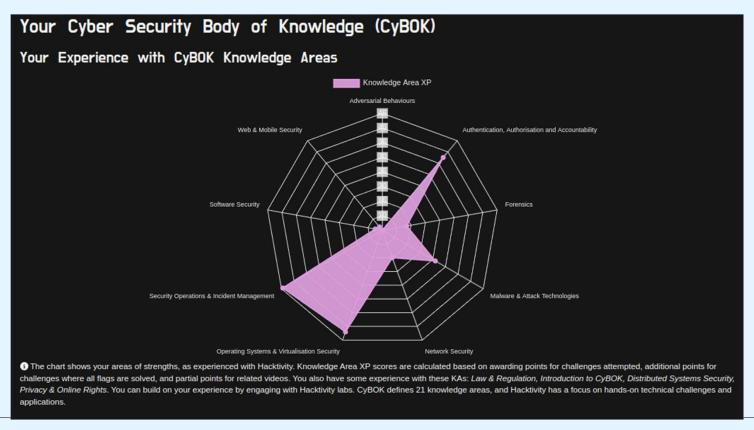


Student #1: L5 CyBOK KAs



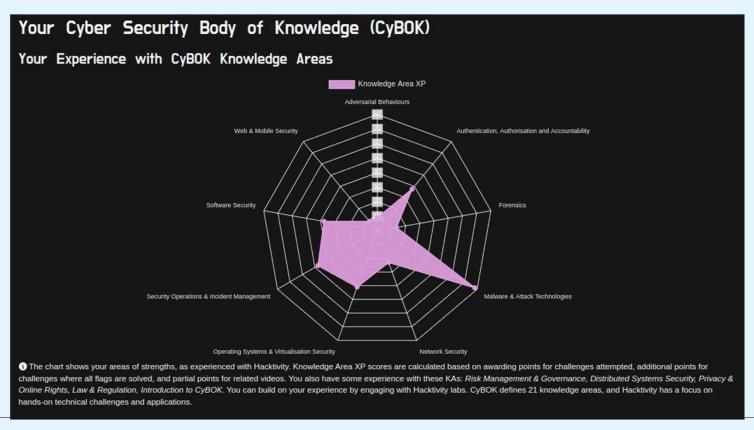


Student #2: L6 CyBOK KAs





Student #3: L7 CyBOK KAs





```
personal data breach notification contribution of siem to analysis and detection thentication - otp (one-time password)cloud computing - resource pooling
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 investigation and prevention of crime
                                                                                                                                                                                                                                                                                                                             technical underpinnings for memory management vulnerabilities; the stack
                                                                                                                                                                                            vulnerabilities can be exploited without being noticed

Client Side Vulnerabilities And Mitigations
Client Side Vulnerabilities
Client Side Vulner
                                                                                                                                                                                                                           enforcement and penalties client-server models network based-authentication with heterogeneous linux and windows network Cloud Computing Services container-based sandboxes: chroot active directory domain serv
                                                                                                                                                                                                                                                               session hijacking non-executable memory penetration testing - network mapping - fingerprinting open source secure development
                                                                                                                                                                                   architectural principles authentication - kerberos
                                                                                                                                                                                                                      Human Factors: Incident Management penetration testing - network mapping - reconnaissance
                                                                                                                                                                                                                                                                         tors: Incident Management

Network Protocols And Vulnerability the fallibility of digital evidence to tampering anti-analysis and evasion techniques
                                                                                                                                                                                                             data recovery and file content carving anti-analysis and evasion techniques cloud computing - deployment models access control - data (discretionary access control) linux security model linux extended access control lists (fac) threats to security for modern oss
                                                                        hypertext markup language (html) race condition miligations

Ilinux Security model linux extended access control lists (lact) threats to security for modern oss linux extended access control lists (lact) threats to security for modern oss linux extended access control lists (lact) threats to security for modern oss linux extended access control lists (lact) threats to security for modern oss linux extended access control lists (lact) threats to security for modern oss linux extended access control lists (lact) threats to security for modern oss linux extended access control lists (lact) threats to security for modern oss linux extended access control lists (lact) threats to security for modern oss linux extended access control lists (lact) threats to security for modern oss linux extended access control lists (lact) threats to security for modern oss linux extended access control lists (lact) threats to security for modern oss linux extended access control lists (lact) threats to security for modern oss linux extended access control lists (lact) threats to security for modern oss linux extended access control lists (lact) threats to security for modern oss linux extended access control lists (lact) threats to security for modern oss linux extended access control lists (lact) threats to security for modern oss linux extended access control lists (lact) threats to security for modern oss linux extended access control lists (lact) threats to security for modern oss linux extended access control lists (lact) threats to security for modern oss linux extended access control lists (lact) threats to security for modern oss linux extended access control lists (lact) threats to security extended access control lists (lact) threats threats (lact) threats (lact) threats (lact) threats (lact) threats
                                                                                                                                                                          linux read only protections: ro mounts memory management vulnerabilities csrf Network Defence Tools potentially unwanted programs
                                                                                                                                                                       Fundamental Concepts And Approaches anomaly detection Os Hardening Threat Analysis
                                                                                                                          system and kernel logs Main Memory Forensics Monitor: Data Sources penetration testing - software toolsfile attributes federated access control
                                authorization - Idago (lightweight directory access protocol integer overflow analysis techniques of local computing - service models - paas Frevention Of Vulnerabilities analysis environments incides/Models exploitation frameworks challenges of live forensics
             workflows and vocabulary antivirus software reference monitor reference monitor reference monitor and the control of the contr
                                                                                                                                   technical underpinnings for malware analysis: c penetration testing - network mapping - nmap Artifact Analysis linux authentication
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 process information certificates
                                                                                                       Code and data negarity checks

Operating Systems & Virtualisation Security kill chains

attack on confidentiality

Malware Taxonomy

Malware Taxonomy

Analysis asm
                        attack on confidentiality Malware Taxonomy
Foundational Concepts information gathering Malware Detection Software and Platform Security network traffic timeline analysis system call interposition
                         reundational concepts and parameters and parameters
 system-level sandboxes (complete os fleesystems web pix and parts format string attacks web pix and ptxps format string attacks and ptxps format string attacks.

Attacker Model Operating System Analysis

handle: actual incident response | metasploit framework development Osi (Open System Interconnect) Model sandbox

Network Security | System savivises by malavare | 
                                                                                                    nuthernication ipitables dentity management recover data and services after an incident os Security Operations & Incident Management umask threat model of Security Principles Technical Underpinning Accountability intrusion detection systems of security Principles of Vulnerabilities of Software Security Operations & Incident Management umask threat model umask threat model umask threat model umask threat model of Security Operations & Incident Management umask unmask threat model umask threat model of Security Operations of Security Operat
penetration testing - drus zone transfer Detection of Vulnerabilities exploitation Software Security Penetration Testing cross-site scripting (xss) Execute: Mitigation And Countermeasures Distributed dystems Security enforcing access control cloud computing - storage elevated privileges cover where kill chain securities are control covered and security penetration and Accountability integrity integrity integrity integrity penetration and Accountability integrity integrity integrity integrity penetration and security penetration and security penetration and security penetration and accountability integrity integrity integrity integrity penetration and security pen
                                                                                                                                                                            race condition vulnerabilities cyber kill chain dimensions docker malware Analysis arace condition vulnerabilities cyber kill chain dimensions docker malware Analysis integrity aractery when & Mobile Security permission dialog based access control facets of authentication at the translation and the security permission dialog based access control facets of authentication are presentational state translate (rest) types of user accounts technical introduction are presentational introduction.
                                                                                                                   vacy & Online Rights affack(s) - arp ' capabilities affack(s) - arp ' capabilities and pidesign common network attacks And Exploitation |

Attacks And Exploitation |

The Attacks And Exploit
                                                                                                  Privacy & Online Rights attack(s) - arp
                                                                                                                                                                api vulnerabilities real and effective identity vulnerabilities and attacks on access control misconfigurations address resolution protocol(arp)
                                                                                                                                                                                                 command injection cves and cwes Malicious Activities By Malware penetration testing - network mapping - ping man-in-the-middle attack (mitm)
                                                                                                                                 access control - role-based access control - matrix required projection roll-realistic protecting integrity penetration testing - active penetration backup - inferential cookies protecting integrity penetration testing - active penetration backup - inferential cookies protecting integrity penetration testing - active penetration backup - inferential cookies protecting integrity penetration testing - active penetration backup - inferential cookies protecting integrity penetration testing - active penetration backup - inferential cookies protecting integrity penetration testing - active penetration backup - inferential cookies protecting integrity penetration testing - active penetration backup - inferential cookies protecting integrity penetration testing - active penetration backup - inferential cookies protecting integrity penetration testing - active penetration backup - inferential cookies protecting integrity penetration testing - active penetration backup - inferential cookies protecting integrity penetration testing - active penetration backup - inferential penetration testing - active penetration backup - inferential penetration backup - inferential penetration testing - active penetration backup - inferential penetration testing - active penetration - active penetration testing - active penetration - active penetration -
                                                                                                                                                                                                                                                               litibes protecting integrity
pipes application-based access controls: user-based access controls insufficiently limit privileges back-end
same origin policy (sop) mitigation bypass: asir vulnerabilities and attacks on sandboxing misconfigurations
sql-injection
```



broken access control / insecure direct object references server-side misconfiguration and vulnerable components malcode/malware - third-party certifications

malcode/malware - countermeasures - code signing Human, Organisational & Regulatory Aspects Virtual - private network (vpn

hardware-emulation and paravirtualisation

hypertext transfer protocol (http) - proxying aslr (address space layout randomization) protecting against session management attacks

Access Control In Distributed Systems

cloud computing - service models - iaas

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.

