CyBOK

Cybersecurity courseware – pentesting, incident response and forensics

This document outlines courseware for the three topic areas penetration testing, incident management and response, and cybercrime and digital forensics. The courseware is developed with CyBOK knowledge areas as main literature. Eash area includes lecture material and suggested practical exercises for students.

The material for each area has been developed as standalone modules which can be combined into a course or given as individual modules or courses. They intend to give the students an introduction to the respective topic area including fundamental theory and research directions. The theoretical foundation is augmented by practical assignments.

This document describes the available content for each topic area. Most material is available through GitHub using the link below. Some material is only available upon request to the author for practical reasons. Some material from other sources is used and those are referenced in this document.

GitHub repository: https://github.com/kavrestad/CybSec_Courseware

Developed by Joakim Kävrestad at the Jönköping School of engineering - Joakim.kavrestad@ju.se

Topic area: Penetration testing

The penetration testing topic area intends to introduce the student to the art of penetration testing by, in turn, addressing the topic as such, high level methods, common tools, and research and development directions. The lecture material is based on the following CyBOK knowledge areas:

- Malware and Attack Technologies
- Adversarial Behaviours

For practical assignments, the resources developed in the CyBOK project "Open source CyBOK practical challenges and learning resources[1]" (Hereafter called SecGen) by Dr. Cliffe Schreuders, or material provided by the service TryHackMe[2] and be used as outlined below. Note that some TryHackMe assignments require subscription.

Lecture Materials

The lecture material is delivered as three editable PowerPoint slide deck. Eash slide deck is estimated to include material for about 90 minutes of effective lecture time. The tiles for the respective slide decks are:

- Penetration testing – Introduction and methods
- Penetration testing - Tools and tricks
- Penetration testing – Research and state of the art

Practical exercises

The following practical exercises are suggested for this topic area:

Using SecGen:

- Introduction to Linux and Security
- Introducing Web Security
- Authentication lab

Using TryHackMe:

- CompTIA Pentest+
- Jr Penetration tester

[1] https://github.com/cliffe/SecGen/blob/master/README-CyBOK-Scenarios-Indexed.md#security-operations--incident-management-soim

[2] https://tryhackme.com/

Topic area: Incident Management and Response

This topic area begins with a discussion on the nature of security operations and incident response, with a focus on handling incidents when they occur. Methods and fundamental tools are then described before the material ends with a discussion on research and state of the art. The lecture material is based on the following CyBOK knowledge area:

- Security Operations and Incident Management

For practical exercises, the resources developed in the CyBOK project "Open source CyBOK practical challenges and learning resources[3]" (Hereafter called SecGen) by Dr. Cliffe Schreuders, or material provided by the service TryHackMe[4] and be used as outlined below. A tabletop incident response exercise has been developed within this project.

Lecture Materials

The lecture material is delivered as three editable PowerPoint slide deck. Eash slide deck is estimated to include material for about 90 minutes of effective lecture time. The tiles for the respective slide decks are:

- Incident management and response – Introduction and methods
- Incident management and response - Tools and tricks
- Incident management and response – Research and state of the art

Practical exercises

The following practical exercises are suggested for this topic area:

Using SecGen:

- Backups lab
- Live Analysis lab
- Security information and event management (SIEM) and Elastic (ELK) Stack lab

Using TryHackMe:

- SOC Level 1

The project also includes a tabletop exercise which is intended to be played in a classroom. The exercise assumes familiarity with the "Security Operations and Incident Management" knowledge area and intends to make the students reason and discuss various actions to take during a response process. The exercise is available at https://github.com/kavrestad/CybSec_Courseware

[3] https://github.com/cliffe/SecGen/blob/master/README-CyBOK-Scenarios-Indexed.md#security-operations--incident-management-soim

[4] https://tryhackme.com/

Topic area: Cybercrime and digital forensics

This topic area first elaborates on the terms cybercrime and digital forensics before addressing how digital forensics are used in law enforcement and for incident response. The topic area introduces the student to analysis of both secondary storage and memory. The topic area ends with an outline of research directions and state of the art which is mainly focused on password cracking. The lecture material is based on the following CyBOK knowledge area:

- Forensics

The following book is used as supporting literature for this topic area:

- Kävrestad, J., Birath, M., & Clarke, N. (2024). *Fundamentals of Digital Forensics: A Guide to Theory, Research and Applications*. Springer International Publishing. https://doi.org/10.1007/978-3-031-53649-6

Practical exercises for this topic area have been developed partly in this CyBOK project and partly in the previous project "Developing and testing a memory analysis workshop" and they are outlined below.

Lecture Materials

The lecture material is delivered as three editable PowerPoint slide deck. Eash slide deck is estimated to include material for about 90 minutes of effective lecture time. The tiles for the respective slide decks are:

- Digital forensics
- Memory analysis
- Forensics and Cybercrime - Research and state of the art

Practical exercises

This topic area includes the following two practical exercises:

- Digital forensics in law enforcement. This lab includes a forensic disk image that the students will investigate using Autopsy Forensics. It begins with questions inviting the students to find specific artifacts and continues with a simulated crime investigation in a phishing scenario. Full description and materials are available at: https://github.com/kavrestad/CybSec_Courseware
- Memory Analysis Lab. This lab invites the students to use Volatility to investigate a memory dump infected with the Cridex malware. It begins with a Volatility tutorial and continues with questions inviting students to find specific artifacts. The lab was developed in the CyBOK project "Developing and testing a memory analysis workshop" and full description and materials is available at that projects GitHub: https://github.com/kavrestad/MalwareAnalysis