Intrusion Detection Laboratory

Course guide

Course Overview 1
Learning goals 1
Content 2
Classes and coursework 2
Assessment criteria 3
Frequently asked questions 3

Study year:	2022-2023; quarter 3
Contact hours:	During class
Responsible lecturer:	Emmanuele Zambon
Co-lecturers:	Luca Allodi
Information:	e.zambon.n.mazzocato@tue.nl, l.allodi@tue.nl
Teaching schedule:	Lectures: 2+2 hours/week
Examination:	Lab projects in reverse classroom setup

Course Overview

What this course is. This course is a heavily hands-on course where students are required to go the extra mile by means of self-study and exploring possible solutions to the assigned challenges (see "Content" below). All students will join a group and are required to develop a fully-fledged laboratory for the other students to take. The labs are challenge-based and require the identification and analysis of threats in real-world data, and the development of appropriate detection techniques.

What this course is not. This course is not a manual and it is not **principles** of intrusion detection. It is a laboratory course through which to apply those principles to real data and challenges. The theoretical principles presented at the beginning of the course are meant as giving students the pointers to technologies, techniques, and methods of use in this domain. The students are expected to come up with original, and therefore creative, solutions to the posed challenges by understanding, combining, and expanding on the material presented in class.

Learning goals

- Learn theoretical and practical principles of cyber security monitoring.
- Learn how to derive a threat model from complex attack scenarios.

- Learn how to build detection procedures fitting a given threat model.
- Master practical and technical aspects of state-of-the-art network, host, and log-based intrusion detection systems.

Meta-objectives:

- Learn to structure the acquired knowledge into practical activities for training.
- Develop a capacity to manage and organise the work of small groups.

Content

The goal of this course is to provide students with a platform to get in-depth, hands-on experience on all three of the building blocks of cyber security monitoring: network-based, host-based and log-based intrusion detection.

To do so, the course is not focused on front classes but rather adopts a reverse classroom setup: the course will start by providing students with material covering practical and theoretical elements of security monitoring and additional material and pointers covering all three pillars, and their relationship. The students will then form groups and will be able to choose one of the building blocks to explore in depth by developing a fully-fledged laboratory activity for the other students of the course to attend. These laboratory activities will be run and coordinated, in class, by the very students developing them. The development and delivery of these lab sessions in class is also the final examination of the course for the group of students handling it, and it is therefore obligatory.

The outcome of this setup is that all students will have developed, by the end of the course, a profound understanding of a technology of their choice, and at the same time get hands-on experience on a multitude of aspects of intrusion detection, through the lab activities developed by the fellow students.

Classes and coursework

The first four classes are dedicated to covering the theoretical material needed for the course.

Classes five and six are dedicated to bootstrapping the lab activities; Class five will provide an example of lab activity serving as a blueprint for the lab delivered by the students at the end of the course. Class six is for project assignments and Q&A.

Note on the course material. The slides are meant to serve as the course study material. This material is meant to provide all the pointers needed for the course challenges to be addressed originally by the students during the devised labs. Consider them a starting point to investigate and explore possible solutions for the challenges. Do not consider yourself limited by them: the solution space you can explore for the challenges only starts – and does not end -- there.

Laboratories. At the end of the course all students (groups) will deliver the developed laboratories to the rest of the classroom. Delivering this activity is mandatory and constitutes the final examination. All students are expected to attend all activities delivered by their colleagues.

Assessment criteria

Criteria	Weak	Developing	Accomplished
Attack Scenario is well analyzed	Attack scenario is not or incorrectly identified. TTPs are not or incorrectly identified. TTPs are non-coherently combined.	Attack scenario is correctly identified. Relevant TTPs are identified.	**Attack scenario** is correctly identified. **Relevant TTPs** are correctly identified, contextualized, and combined. **Impact of the attack** scenario and **affected assets** are thoroughly discussed.
Attack Mechanics are well understood	Imprecise understanding of some features characterizing the attack; identified characterizing features are not observable in the data.	Understanding of some characterizing features of the attack; features can be observed in the data.	Understanding of the **core characterizing features** of the attack observable in the data; hard for the attacker to change these features.
Technical implementation is fit to attack scenario	The proposed detection signatures/strategies are incompatible with attack mechanics and observable data. No discussion of advantages and disadvantages of the proposed detection method.	The proposed detection signatures/strategies are trivial or with insufficient accuracy/completeness w.r.t. what the available data allows to do. Basic evaluation, metrics and discussion of advantages and disadvantages of the proposed detection methods.	The proposed detection signatures/strategies and their accuracy/completeness are **adequate to what the available data allows to do**. Thorough evaluation, with **metrics**, **investigation of FPs and FNs**, **discussion of advantages and disadvantages** of the proposed detection methods, with proposed **alternatives**.
The lab activities are well structured and coordinated	Presentation is difficult to follow; activity steps are not well organized or too large/difficult; activity goes overtime.	Minor presentation issues; activity steps could be better explained/documented; activity would benefit from more time.	**Appropriate** and concise **presentation**; activity **steps** are clearly **described** and **achievable by the audience**; activity is correctly **sized for available time**.

Frequently asked questions

I have an M1/arm/non-x86 chip on my laptop, how do I do the virtualization?

You do not. The lab work will be done in groups, so you can always work on the VM with some of your colleagues. We do however provide alternatives to the VM for you to deploy them in your own setup locally, or on a custom VM you can run on your system (some tooling may need to be recompiled for this work).

Where do we form the groups?

On canvas. Students without a group by the deadline announced on canvas will be assigned to a group.

<more questions will be added as/if we receive them>