0. Administrivia

055633 - COMPUTER SECURITY
Proff. Barenghi, Carminati, Zanero

Welcome

In this course, we will follow an **holistic approach** to **systems security**.

We will study what happens on **hosts**, **networks**, with an eye to the impact of **policies** and procedures...and the **PEBKAC**!

Instructors

Alessandro Barenghi

- Email: alessandro.barenghi@polimi.it
- Office: 1st floor, building 20, DEIB
  - Office hours: just e-mail me and we'll find a timeslot
- Phone: 9039

Tutors/Assistants

Lorenzo Binosi

- Email: lorenzo.binosi@polimi.it

Instructors

Michele Carminati

- Email: michele.carminati@polimi.it
- Office: 1st floor, building 20 or NECSTlab, DEIB
- Office hours: just e-mail me and we'll find a timeslot
- Phone: 4041

Tutors/Assistants
- **Marco D'Amico**
  - Email: marco.damico@polimi.it
- **Gabriele Digregorio**
  - Email: gabriele.digregorio@polimi.it

Instructors

Stefano Zanero

- Email: stefano.zanero@polimi.it
- Office hours: just e-mail me and we'll find a timeslot
- Phone: 4017
- http://zanero.org

Tutors/Assistants
- **Juri Sacchetta**
  - Email: juri.sacchetta@polimi.it
- **Daniele Mammone**
  - Email: daniele.mammone@polimi.it

What we do as Research Scientists

- AI for Security and Security of AI
- Cyber-physical security (automotive, robotics, medical, space)
- HW and SW security
- Secure HW design
- Malicious software (malware) analysis
- Novel attacks on bleeding-edge technology
- Post quantum cryptography
- Side channel attacks and countermeasures

Course Topics

Summary

1. Framing what a secure system is
2. Fundamentals of cryptography
3. Techniques for user authentication
4. Authorization and access control policies
5. Application and Web security
6. Network security
7. Malware

Exam Structure

Written test (up to 33 points)

- Theory and practical exercises
  - Since 2021–2022 we changed the structure, so previous exams are not representative

- Closed books & No Remote & No Oral Exam

(Bonus) Homeworks Challenges (up to 3 points)

- **Duration:** Last for two weeks (usually in May)

  - HW1 (1 week)
    - memory errors vulnerabilities (buffer overflow and format string)
  - HW2 (1 week)
    - web vulnerabilities (client + server)

Clarifications on the Challenges

- **Score computation**   *...Since 2024...*
  - Each challenge score is determined by the number of successful solutions:
    - *the more people solve a challenge, the lower the score assigned to it*

- The challenges are **not mandatory**
  - **Bonus** points + The written exam alone reaches 34 points

- **Challenges prerequisites:**
  - They may contain <u>advanced concepts</u> that require
    - <u>Individual effort and study</u>

- **We won't allow any cheating attempts**
  - If we are able to single out cheaters:
    - We will void their grades
  - otherwise
    - We will void the challenges to anyone...ask your colleagues what happened in 2022-2023...

Prerequisites

- C Programming and its execution model

  ○ Essentially "Fondamenti di informatica" / CS101

- A little of bash scripting and Python
- IA32 (aka i386) assembly

  ○ There's a prep class to bring you up to speed

- Network protocol fundamentals
- Be able to work in a GNU/Linux environment with a CLI
- If you are missing something, **just ask** us for the material

Materials

Option 1: Slides + Attend class + [Optional material]
Option 2: Slides + Books + [Optional material]
~~Option 3: Slides only~~ (best way to fail the exam)

Textbooks
- *D. Gollman*, "Computer Security", Wiley (3rd ed.)
- *R. Anderson*, "Security Engineering", Wiley (2nd ed.) `FREE`
- William Stallings, Lawrie Brown, Computer Security Principles and Practice
- Mike Rosulek "The joy of cryptography" `FREE`

Slides, **Recordings** (and all other material) on WeBeep

[Optional Material]

Books

- *C. Anley, J. Heasman, F. Linder, G. Richarte*, "The Shellcoder's Handbook", Wiley, 2007
- *Howard, LeBlanc*, "Writing Secure Code", Microsoft
- Advanced Linux Programming - Chapter 10

Papers

- The slides include links to in-depth material on select subjects

Hacking Group and CTFs

- about 21 years ago, we started playing CTFs
- now we have a local hacking group
- Tower of Hanoi

    https://towerofhanoi.it/

    https://twitter.com/towerofhanoi

- we hack at the NECSTLab
- we have a Discord channel
- just ask if you're curious!

What is this CTF thing, anyway?

Information security-oriented "game"

Try to break into (toy) applications "for fun"

... get flags: **flag{this_is_a_flag}**

WHICH SKILLS?

cryptography
reverse engineering
binary exploitation
web application security
stego / forensics
mobile security
... and others

Good teams generally have strong skills and experience in all these areas

Jeopardy

CRYPTO

BETTER ZIP	231pt
	38 solves
DM COLLISION	176pt
	63 solves
DOGESTORE	267pt
	27 solves
MITM	243pt
	34 solves
PERFECT SECRECY	158pt
	74 solves

MISC

BOOKSHELF	363pt
	10 solves
FEEL IT	208pt
	47 solves
PHRACK	420pt
	5 solves
TAPE	355pt
	11 solves
WIRED CSV	220pt
	42 solves

PWN

DRIVE	500pt
	0 solves
EXECVE SANDBOX	283pt
	23 solves
APT42 - PART 2	420pt
	5 solves
SANDBOX COMPAT	420pt
	5 solves
SFTP	181pt
	60 solves

RE

SHALL WE PLAY A GAME?	113pt
	11 solves
BACK TO THE BASICS	293pt

WEB

BBS	453pt
	3 solves
CAT CHAT	210pt

Attack/Defense
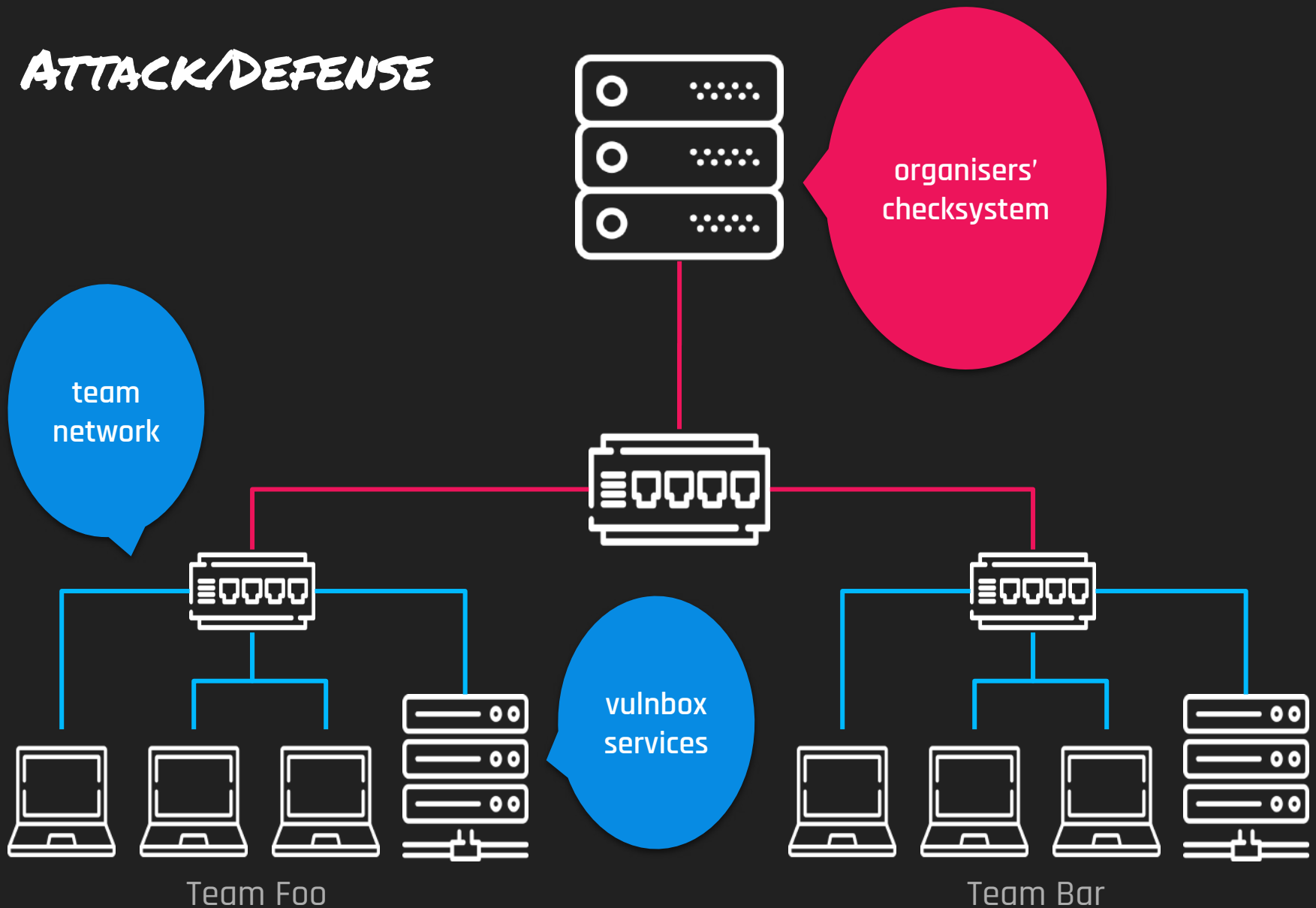
organisers' checksystem

team network

vulnbox services

Team Foo

Team Bar

Slide credit: Marco Squarcina, TU Wien

Defcon CTF

DEF CON 33 will be August 7-10, 2025 at the Las Vegas Convention Center!

Internet connection!

Internet connection!

- Hotel LAN
- LTE Sim Cards
- Radio Bridge to another hotel
  - …er, which one?
  - Bellagio was in sight

It is not a game

- CTFs are played by Professionals
  - Used as recruitment tool
- Very little fair play
  - Physical attacks
  - Attacking the infrastructure
- 0-days:
  - Kernel exploits: https://t.co/6OnnGK363y
  - XSS Auditor Fail
  - ExpressionEngine
- It is NOT Real Application
- Good Challenges
  - Let you explore Ideas
  - Guide you through something new

Niklas B
@_niklasb

Cool, that means all 5 0day challenges from #35C3CTF got solved eventually :)

> Ronen Shustin @ronenshh · Jan 7
> Here is my writeup on how I solved the express-yourself challenge from the #35C3 CTF.
> github.com/r0nen/ctf/tree...

8:24 PM · Jan 7, 2019 · Twitter Web Client

17 Retweets   82 Likes

Tools: TULIP and The META Game

- Traffic Analyzer
- Reply Capabilities
- Developed By Team Europe
- github.com/OpenAttackDefenseTools/tulip
- Attacks on Tulip at ECSC 2022

OTHER GAMES: King Of The Hill
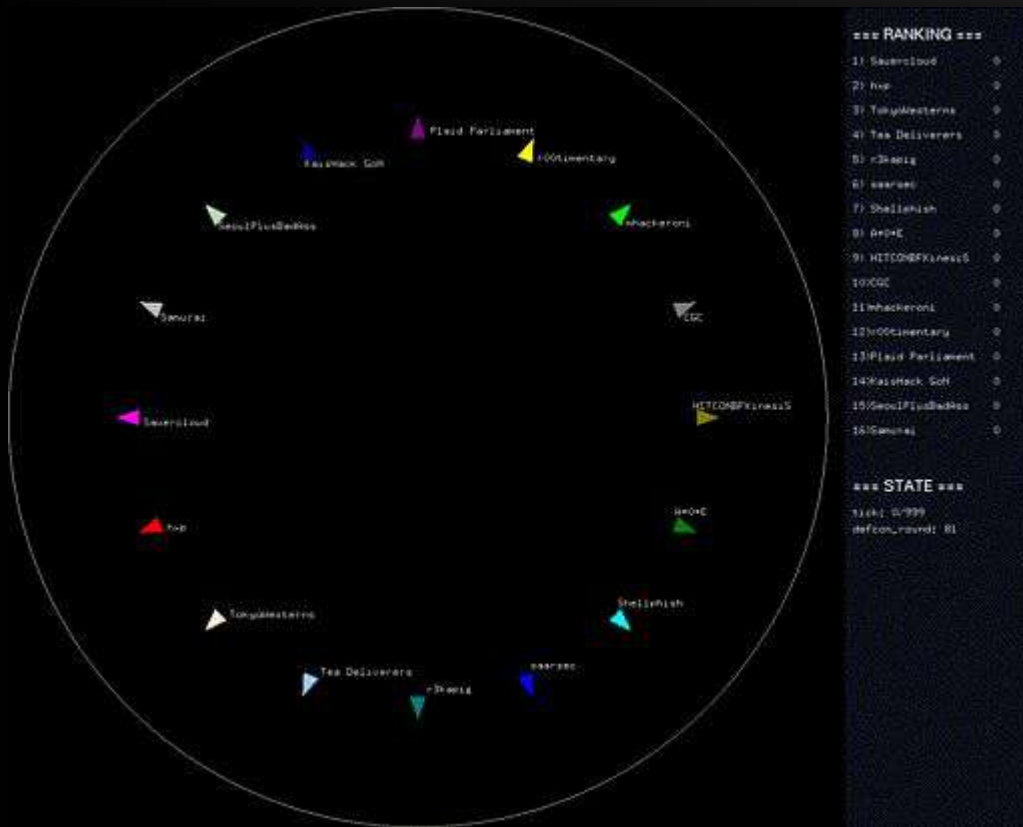
**Best Exploits WIN!**

- Ranking, bytes limit

ROPShip

- In a nuthsell… **Visual A/D!**
- Automatically generate **ROP chains** from random data to determine the next action of the spaceship

```
up, down, right,
left, shield,
attack, nop
```

- Many different strategies

Building an E-Sports ?

Hack-A-Sat

- **Space Themed CTF**
  - Orbiting Challenge
  - Landing
  - Communication
  - Apollo Code Reversing and Attack
  - etc.
- **2023 There was a Final on an orbiting Satellite**
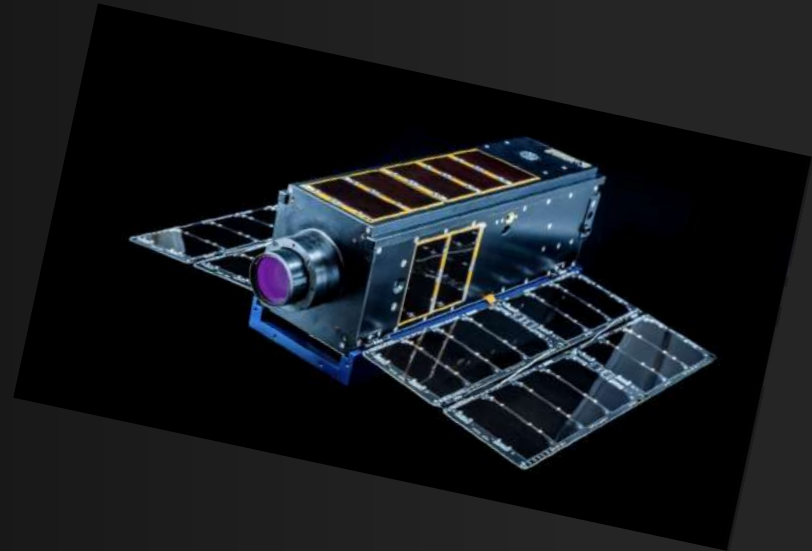
FINALS TEAMS

Krautsat   mHACKeroni   SpaceBitsRUs   Poland Can Into Space   jmp fs: [rcx]

mHackeroni Won!

mHackeroni Won!

How About Machines?

Conclusion

You just met your Professor :-)

Having a textbook is not mandatory, but is a good substitute for coming to class (or watching recordings).

"Slides only" is a no-no.

If you find yourself interested in security by the end of this course, a natural continuation would be to explore...

056896 - OFFENSIVE AND DEFENSIVE CYBERSECURITY