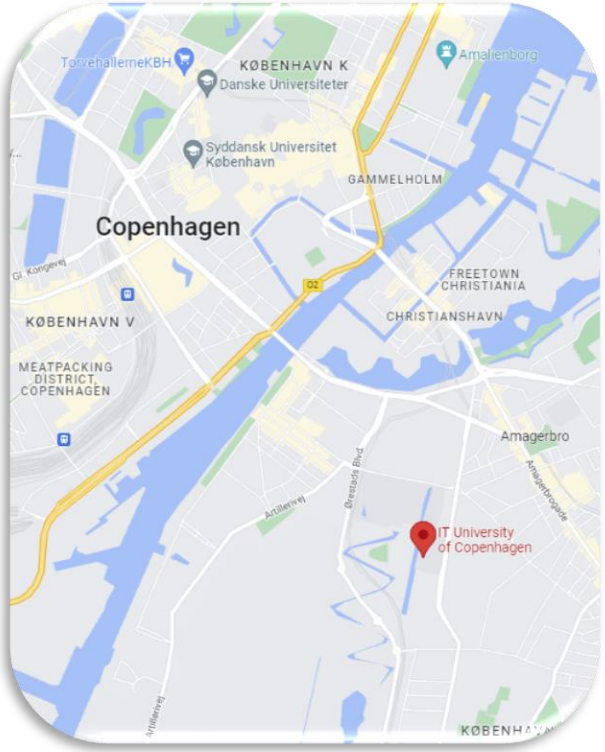
# BSIDES

KØBENHAVN

# IT University of Copenhagen



# CTFs and Workshops

- OT CTF
- OSINT CTF
- Defensive CTF
- Threat Hunting CTF
- Scavenger Hunt CTF

- Make the SOC hate you with this One Weird Trick
- CrowdSec for Absolute Beginners
- Career Village
- OT/ICS hacking stand

# Cool talks

(but not all slides are available yet)

# Getting started with Ransomware

David Af

Do you want to learn more about the technical side of malware, maybe earn some money along the way, then this is the talk for you.

We will cover different aspect of a ransomware including code snippets.

(This is a joke of course. You will learn some technical aspect, but please only use them for good)

# Breaking stuff in industrial networks

mikael vingaard

Presentation on ICS/OT and a on-site CTF with ICS devices

# Sandboxing Malware Safely

Lars Birch

Malware inspection 101 - build your own "free" sandbox and detonate/inspect malware safely.

# Why you should think about elephants while creating your IT disaster recovery plan

Sarah Aalborg

When you are in a crisis you think way differently than you do when you are preparing your plan in a nice and quiet mental state.
This speak is on what you should be aware of and how to mitigate on the risks your mental biases cause when preparing for and during a crisis situation.

The presentation is targeted anyone involved in Disaster recovery from IT security management to the technical response teams.

# Flying Under The Radar - Stealth Hacking Tactics

Magnus K. Stubman

As an attacker, you can't do your job if your activities are constantly detected. Certain attacks can be easily detected and prevented, and others are really hard to even notice. This talk aims to cover various hacking tactics that are significantly hard for defenders to detect. Topics will span from low-level technical attacks to high-level attack-in-depth strategies. The talk is based on the experience of professional Red Teamers that are conducting targeted attacks on a daily basis.

The talk aims to inspire both attackers and defenders to rethink their tradecraft, and hopefully improve in both disciplines.

# Active Directory trust attacks

Martin Sohn and Jonas Bülow Knudsen

What is interesting is that SID filtering can be enabled on intra-forest domain trust as well and in theory prevent the SID-History injection technique. This posed the question – could SID filtering make the domain a security boundary?

Our talk will take the audience through our research on this question. We will demonstrate typical trust attacks, how they can be mitigated, present SID filtering research and new techniques we discovered that make intra-forest SID filtering obsolete. Finally, we will explain and demonstrate a trust attack technique for moving from a TRUSTING domain to a TRUSTED domain (opposite direction of other trust attacks) which works even over one-way forest trusts (thereby breaking both Microsoft’s “forest is security boundary” statement and the “Red Forest”/ESAE design).

Knowledge of Kerberos authentication is not necessary as the attacks are of low complexity, but it is an advantage. Attacks will be demonstrated using Mimikatz, Rubeus, and living off the land tools.