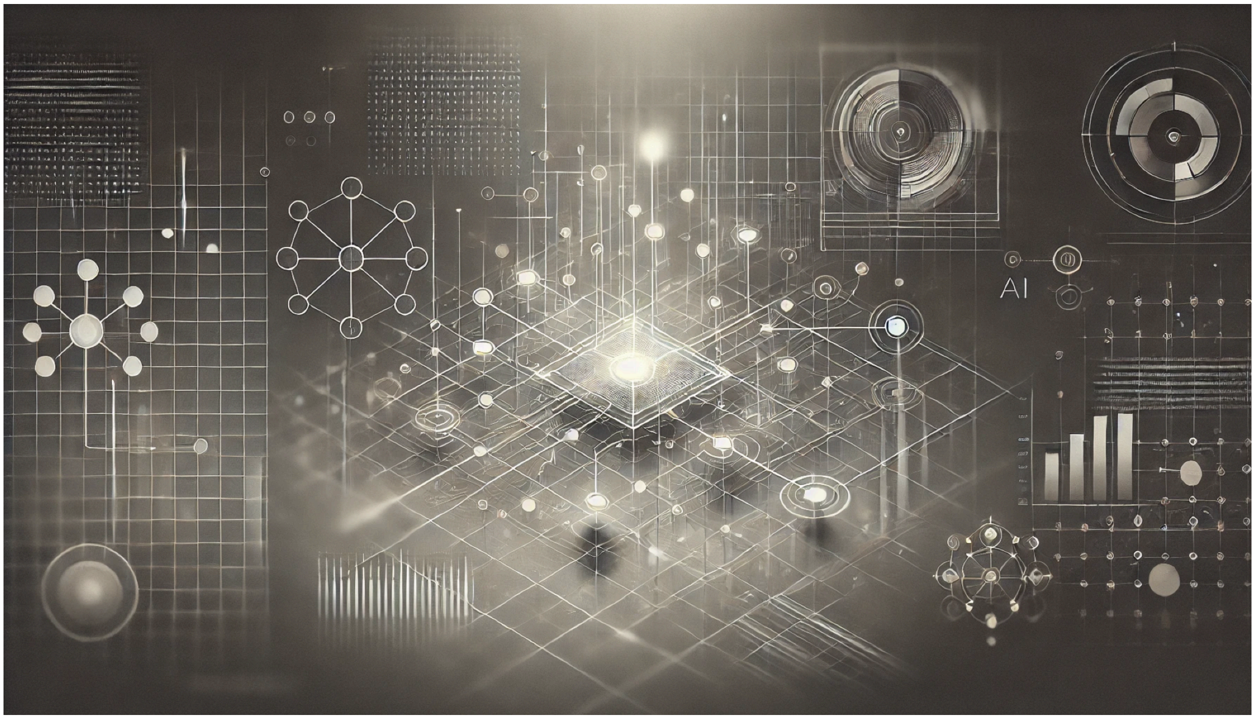
Fortifying AI: Hands-On Training in Adversarial Attacks and Defense of AI Systems (Full Day)

Workshop: AI Security: Foundations and Practical Attacks
Instructors: Vishal Thakur and John Lopes
Date & Time: Sunday, June 22nd, 08:30–17:30
Location: Bella Center Copenhagen
Format: Lecture + Hands-On Labs using Google Colab

Workshop Overview

This hands-on training will introduce AI security fundamentals, walk through real-world adversarial attacks, and provide practical lab exercises using pre-built Google Colab notebooks. **No local Python setup or installations are required.** Everything runs in the cloud using your browser.



System Requirements

To ensure a smooth experience, please bring a fully charged laptop that meets the following:

Hardware:

- Laptop with at least 8 GB RAM (16 GB recommended)
- Modern processor (Intel i5 or equivalent and above)
- At least 10 GB free disk space
- Charger and reliable power access

Software:

- Web Browser: Latest version of Chrome, Firefox, or Edge
- Google Account: Required to access Colab notebooks

Network:

- Stable internet connection (minimum 5 Mbps) – essential for Colab and dataset access
- The venue provides strong Wi-Fi

What to Bring

- A Google Account (make sure you can log in)
- A laptop that meets the system specs
- Enthusiasm and curiosity about AI and security

Prerequisites & Expectations

This course is beginner-friendly but fast-paced. You will get the most from it if you have:

Basic Knowledge:

- Familiarity with ML concepts (e.g., models, datasets, training)
- Basic understanding of Python (variables, loops, functions)

No Installation Needed:

- All labs will be provided via Google Colab
- No need to install Python, Jupyter, or any libraries locally

Optional Background (Helpful but not required):

- Exposure to libraries like TensorFlow, PyTorch, or scikit-learn
- Interest in cybersecurity and AI model behavior

During the Workshop

You will be provided with:

- A shared folder of Colab notebooks
- Live demos and real-time guidance
- Preloaded datasets (automatically downloaded inside Colab)

Important Reminders

- Check your Google login beforehand to ensure Colab access
- Save your work to your own Google Drive during the session
- Do not rely on tablet-only setups – full laptops are required
- Bring a backup battery or charger