TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

# Training:

# ML for Security and Security for ML

## Date of the online training: **March 24-26, 2021**

## Overview

Machine learning / Deep learning is under exponential growth these days. Businesses, Academia and tech enthusiasts are really hyped about trying out Deep learning to solve their problems. A lot of students, professionals and researchers are driven to learn this new cool tech. Just like every other technology, ML comes with awesome applications topped with some serious implications.

So, join this online expedition specially designed for security professionals to understand, build and hack Machine Learning applications. The course is divided into two parts, ML4SEC & SEC4ML. ML4SEC will focus on nitty-gritties of building ML applications. Then learn to hack them in SEC4ML part.

**ML4SEC**

Considering no prior knowledge of mathematics and ML, we will try to build the intuition behind algorithms. Attendees will go through hands-on experience in building ML powered defensive and offensive security tools. In-depth understanding of the entire ML pipeline is provided. Which consists of pre-processing data, building ML models, training and evaluating them and using trained models for prediction. Well known machine learning libraries like Tensorflow, Keras, Pytorch, sklearn, etc. will be used. At the end you will be ready with end-to-end and ready to apply ML Gyan for security professionals.

**SEC4ML**

This part will address the vulnerabilities (like Adversarial learning, Model stealing, Data poisoning, Model Inference, etc.) in state-of-the-art machine learning methodologies. Lab material will consist of Vulnerable Machine Learning applications that can be exploited to provide a thorough understanding of discussed vulnerabilities. Possible mitigation to these vulnerabilities will also be discussed.

## Who should attend this training?

- Machine learning enthusiasts and professionals
- Security researchers and pentesters looking forward to implementing ML/DL in their research
- Pentesters willing to explore new ways to pentest Machine learning applications
- Students with computer science background and a taste for ML and infosec

## Prerequisites

- Basic knowledge of python is good to have but not required
- Basic of Linux and VirtualBox

## Requirements

- Laptop with 8GB+ RAM
- 20 GB space
- Virtual box (latest version)
- Any flavor of Linux is preferred over windows
- Open mind made up for some intense mathemagic

## About the Trainers

**Nikhil Joshi** is a Security Researcher at Payatu. He has been the Machine Learning guy for more than 4 years and currently working on implementations of ML in offensive and defensive security products. At Payatu, He has orchestrated methodologies to pen-test Machine Learning application against ML specific vulnerabilities and loves to explore new ways to hack ML powered applications. Parallelly Nikhil's research is focused on security implications in Deep Learning applications such as Adversarial Learning, Model stealing attacks, Data poisoning, etc.

Nikhil is an active member of local Data Science and Security groups and has delivered multiple talks and workshops. Also has spoken at HITB Amsterdam, PhDays Russia and presented his research at IEEE conference. He is a trainer at NullCon. Being an Applied Mathematics enthusiast, recent advances in Machine Learning and its applications in security, behavioural science and telecom are of major interest to Nikhil.

## Booking

Recommended online booking of trainings through:

https://troopers.de/tickets/

## Contact

**Need assistance?** Don't hesitate to call us. We are fluent in English and German. +49 6221 480390 or info@troopers.de

**Booking is also possible offline through your trusted partner:**

**HM Training Solutions**, Falkenstrasse 6, 63820 Elsenfeld, Germany

+49 6022 508200 / info@hmtrainingsolutions.com

+49 6022 5089999 / www.hmtrainingsolutions.com