TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

Machine Learning for Security & Security for Machine Learning

Date of the training: **March 16-17, 2020** in Heidelberg, Germany

Book now using the voucher code: **TR20_HMTS** and save an additional 5% of the current valid rate of any package!

Overview

Machine learning / Deep learning is under exponential growth these days. Businesses, Academia and tech enthusiast 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.

This course is aimed for security researchers/ penetration testers/ InfoSec enthusiasts to bridge their gap between Infosec and Machine learning. Considering no prior knowledge of mathematics and ML, we will try to build the intuition behind of Machine Learning methodologies. Attendees will go through the hands-on experience with building application like Firewalls, IDS/IPS, Malware Detection engines, etc. In-depth understanding of the entire ML pipeline is provided. Which consists of preprocessing data, building ML models, training and evaluating them and using trained models for prediction. Well known machine learning libraries like Tensorflow, Keras, Pytorch, Scikit learn, etc. will be used, providing an end-to-end and ready to apply ML Gyan for security professionals.

Along with the applications, this course will address the vulnerabilities in the 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 observed vulnerabilities. Reasons behind the existence of these vulns and the defensive strategies will also be discussed.

Training Outline

This training is divided into two parts i.e. “ML for Security” and “Security for ML”. Considering no prior knowledge of mathematics and ML, we will try to build the intuition behind algorithms.

ML4SEC

Attendees will go through the hands-on experience in building ML powered defensive and offensive security. 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.

In this session, we will build up our understanding of basic yet state of the art machine learning algorithms. Discuss mathemagic behind why these models work the way they do. Build some smart Machine Learning applications and evaluate them. By the end, we will get an idea of how to solve a real-world problem using machine learning.

SEC4ML

This part will address the vulnerabilities (like Adversarial learning, Model stealing, Data poisoning, Model Inference, etc.) in the 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.

In this session we will have a deeper look on different flaws in how ML/DL algorithms are implemented. Hands on examples explaining and attacking such vulnerable implementations. Also, discussion on possible mitigation.

What to expect

- Thorough understanding of basic machine learning methodologies;
- Hands on practice on Specially crafted labs for ML and Infosec enthusiasts;
- End-to-end and ready to apply ML knowledge for security professionals;
- Good understanding of Machine learning vulnerabilities;
- Hands on experience with well-known machine learning libraries;
- Lab material for post-course practice.

Prerequisites

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

Requirements

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

About the Trainer

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, behavioral science and telecom are of major interest to Nikhil.

TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Booking

Recommended online booking of trainings through:
https://troopers.de/tickets/

Voucher code: TR20_HMTS
Using this voucher code automatically gives you an additional 5% off the current valid price! You can register with this code until seats have run out.

Contact

Need assistance? Don't hesitate to call us. We are fluent in English and German. +49 151 16228365 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