TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

Pentesting the Modern Application Stack

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

Continuous Build & Deployment tools, Message brokers, Configuration Management systems, Resource Management systems and Distributed file systems are some of the most common systems deployed in modern cloud infrastructures thanks to the increase in the distributed nature of software. Modern day pentesting is no more limited to remote command execution from an exposed web application. In present day scenario, all these applications open up multiple doors into a company's infrastructure. One must be able to effectively find and compromise these systems for a better foothold on the infrastructure which is evident through the recent attacks on the application stack through platforms like Shodan paving way for a full compromise on corporate infrastructures.

In this two-day course we start by looking into red team tactics for pentesting modern application stack consisting of Databases, CI tools, Distributed Configuration & Resource management tools, Containers, Big Data Environments, Search technologies and Message Brokers.

ERNW Insight GmbH
Carl-Bosch-Str. 4
69115 Heidelberg
BIC: GENODE61HD3

Tel. +49 – 6221 – 48 03 90
Fax +49 – 6221 – 41 90 08
Ust-ID DE 304 445 827
IBAN: DE84 6729 0100 0067 1236 03

Managing Director:
Kerstin Schröter

Along with the training knowledge, the course also aims to impart the technical know-how methodology of testing these systems. This course is meant for anyone who would like to know, attack or secure the modern day stack. The students are bound to have some real fun and entirely new experience through this unique course, as we go through multiple challenging scenarios one might not have come across.

During the entire duration of the course, the students are expected to learn the following:

- Look for vulnerabilities within the application stack.
- Gain in depth knowledge on how to pentest the modern stack consisting of Continuous Build & Deployment tools, Message broker's, Configuration Management systems, Resource Management systems and Distributed file systems.
- Security testing of an entire application stack from an end-to-end perspective.

Prerequisites

- Knowledge of basic pentesting, web application working and linux command line basics;
- Ability to use a web proxy like Burp Suite, ZAP;
- Ability to write basic scripts in any interpreted language is an added advantage.

Requirements

- A laptop with administrative and USB access;
- Minimum configuration of 8GB RAM and 100GB hard-disk space;
- Full virtualisation support, Virtual Box and Docker should be installed. Unix box is preferred.

About the Trainer

Francis Alexander , Lead Security Engineer for Nash.io has over 3+ Years of Experience in the Application Security industry, the author of NoSQL Exploitation framework and NoSQL Honeypot. His areas of interest include NoSQL Databases, Machine Learning and Cloud Security. He has spoken and trained at conferences such as Troopers, Hack in the Box, Hack in Paris, PhDays,44Con,Nullcon, C0c0n.

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