TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

Pentesting the Modern Application Stack

Date of the training: **March 18–19, 2019** in Heidelberg, Germany

Book Now using the voucher code: **TR19_HMTS** and save an additional 5% of the current valid rate of any package!

Overview

This is a unique course that covers red team tactics for pentesting modern day application stack. Attendees will learn to identify, exploit and exfiltrate data from Database Servers, Software Collaboration tools, CI tools, Distributed Configuration & Resource management tools, Containers, Big Data Environments, Search Technologies and Message Brokers. The 2 days course is a fast paced and completely hands on program that aims to impart the technical know-how methodology and tools of trade for testing these systems. Real world corporate stacks are emulated in the form of containerized challenges to prepare students for real world scenarios.

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 2-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.

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.

Course Outline - Day 1

Pentesting some of the widely used systems in the modern stack

Module 0: Modern Application Stack

- Evolution of Application Stack
- Components of Stack
- Threat Modelling
- Attack Surface

Module 1: Pentesting Databases

- MySQL, Postgres and OracleDB
- Basic Enumeration
- Laying out the attack surface
- Pentesting third party plugins.
- Attacking Database Servers.
- Case Study of CVE-2016-6663
- Security testing using tools of trade.

Pentesting NoSQL Databases & Caches: MongoDB,
Cassandra, Redis & Memcache:

- Fingerprinting NoSQL databases,
- Injection attacks on NoSQL Databases.
- Attacking and identifying vulnerabilities in NoSQL databases through NoSQL exploitation framework.
- Case study on Mongo Ransomware and hands on vulnerable applications.
- Securing databases.

Module 2: Public Cloud Environments

- Introduction to Cloud Environments.
- AWS Configurations & AWS Security Checks.
- Pentesting AWS lambda servers & Fuzzing Lambda functions and identifying vulnerabilities.
- Secure Best practices for Cloud environments and Securing AWS instances

Module 3: CI Tools

- Introduction to Jenkins, TeamCity and Go.
- Basic misconfigurations and attack surface for these tools.
- Security testing of CI Tools and outlook on vulnerabilities in Jenkins,
- TeamCity and Go.
- Case Study: Red-team assessment from Jenkins to Production.

Module 4: Software Collaboration Tools

- Leveraging Version Control Systems like Git, SVN and Perforce.
- Attacking Code collaboration tools - Phabricator, Gitlab and Github Enterprise.

Module 5: Message Brokers

- Introduction to RabbitMQ and Kafka.
- Common misconfigurations.
- Attacking and extracting juicy information from Message brokers.
- Using message brokers for data exfiltration.

Course Outline - Day 2

Module 6: Containers

- Hacking Docker environments (Lateral Movements in docker, Docker breakouts, Docker Monitoring in CI/CD pipeline).
- Setting up vulnerability static analysis for Docker containers (Clair and other tools).
- Hacking Vagrant instances.
- Securing Docker and Vagrant instances.

Module 7: Distributed Configuration Management Systems (DCMS)

- Attacking Apache Zookeeper, HashiCorp Consul & Serf, CoreOS Etcd.
- Owning the entire application thorough DCMS, pivoted attacks.
- Attacking and Scanning using Garfield.

Module 8: Distributed File System

- Basic misconfigurations for Hadoop.
- Analyzing the threat model for Hadoop.
- Attacks and remote code executions on Hadoop.
- Securing Hadoop Instances.

Module 9: Kubernetes, Mesos and Marathon (Distributed Deployment & Resource Management)

- Introduction to Kubernetes, Mesos and Marathon
- Fingerprinting Kubernetes, Mesos and Marathon
- Common Misconfigurations & Abusing them to gain access to system pods.
- Pentesting Kubernetes and pivoting through Kubernetes containers.
- Hacking entire application stack through Mesos and Marathon.
- Securing Mesos instances.

Module 10: Search Technologies

- Introduction to ElasticSearch and Apache Solr (Lucene)
- Laying out the attack surface and common misconfigurations.
- Pentesting ElasticSearch and Solr.
- Case Study: Elasticsearch CVE-2015-1427 RCE Exploit.

Requirements

- Knowledge of basic pentesting, web application working and Linux command line basics
- Ability to use basic set of tools like curl, NMAP, Metasploit, Burp Suite, ZAP
- Ability to write basic scripts in any interpreted language is an added advantage.
- A laptop with administrative and USB access and minimum configuration of 8GB RAM and 100GB hard-disk space
- Full virtualization support, Virtual Box and Docker should be installed. Unix box is preferred

About the Speaker: Francis Alexander

Francis Alexander, Lead Security Engineer for Envestnet/Yodlee, has over 4+ 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.

About the Speaker: Bharadwaj Machiraju

Bharadwaj Machiraju is a security engineer by profession who does some research and writes some tools both during day and night alike. All tools are available at github.com/tunnelshade and all ramblings at tunnelshade.in. Spoke at few conferences notably Nullcon, Troopers, Brucon, Pycon India etc. Apart from information security, he is interested in sleeping, mnemonic techniques & machine learning.

TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Booking

Recommended Online Booking of Trainings Through:

Sign-Up Form https://troopers.de/tickets/

Voucher code: **TR19_HMTS**

Using this voucher code automatically gives you an additional 5% off the current valid price! You can register with this code up until March 11th, 2019 or until seats have run out.

Contact

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

Zögern Sie nicht uns zu kontaktieren. Wir sprechen fließend Englisch und Deutsch.

Troopers Organization Team

+49 151 16228365 or info@troopers.de

Booking is also possible offline through your trusted partner from:

HMTS HM Training Solutions

HM Training Solutions, Falkenstrasse 6, 63820 Elsenfeld, Germany

+49 6022 508200 / info@hmtrainingsolutions.com

+49 6022 5089999 / www.hmtrainingsolutions.com