Hacking and Securing Docker Containers v2.0

Duration: 1 days (8hrs/day)

Prerequisite: -- This course starts from very basics and thus no Docker experience is required

Course Objective:
This course introduces students to the security concepts associated with Docker. Docker is a popular software and it is widely used in Information Technology Industry. It's popularity also brings a larger attack surface and thus it is important to understand it's security aspects to be able to protect Docker containers.

Lab Requirement: -- Koenig DC

- **Module 1: Introduction**

- **Module 2: Fundamentals of Docker**
  - What is Docker?
  - Virtual Machines vs Containers
  - Virtual Machine Download
  - Lab setup
  - Building your first Docker Image
  - Running your first Docker container
  - Images vs Containers
  - How Docker Images are stored locally
  - Control Groups
  - Namespaces

- **Module 3: Hacking Docker Containers**
  - Introduction
  - Docker Attack Surface
  - Exploiting Vulnerable Images
  - Backdooring Docker Images
  - Privilege Escalation
  - Introduction to Container Breakout
  - Introduction to docker.sock
  - Container escape using docker.sock
  - Introduction to –privileged flag
  - Writing to Kernel Space from a container
  - Writing a Kernel Space to get a reverse shell
  - Accessing Docker Secrets

- **Module 4: Automated Assessments**
  - Introduction
  - Scanning Docker Images
  - Auditing the Environment using Docker Bench Security

- **Module 5: Defenses**
  - Introduction

- Apprarmor Profiles
- Seccomp Profiles
- Capabilities
- Docker Content Trust