# Honeypots

## Course 71556 – 40 Hours

### Overview

The class would mainly include hands-on demonstrations and labs on selected honeypots that form a wide array of capabilities against hackers. From low-interaction honeypots that stall hackers, to medium and high interaction honeypots that aim to provide hackers a false sense of safety that would make them reveal their tools and techniques. This wide variety of demonstrations and labs would be tested through a final project in which students would have to demonstrate independent thinking, based on the knowledge gained, to protect their own assets.

### On Completion, Delegates will be able to

- Students will understand the security concepts behind honeypots' usage and get familiar with the deployment, operation, advantages, and pitfalls of selected open-source and commercial products in order to build a comprehensive deception security framework for their organizations.
- Students will understand the concepts and purposes of using honeypots as part of a computer security suite in an organization.
- Students will get familiar with the main open source and commercial products in the field.
- Students will deploy and operate selected low, medium, and high interaction honeypots to acknowledge their up and down sides.
- Students will consolidate the data gathered from sensors during the class and come with security research observations.
- Students will demonstrate the utilization of honeypots as research tools to protect their own digital assets while trying to capture the assets of others.

### Prerequisites

- Security analysts who are familiar with defense mechanisms and attacking patterns
- Linux, Windows, Python, and Networking knowledge

### Course Contents

**Module 1: Introduction to Deception-based Security**

- What is a Honeypot?
- What is its added value to the organization?
- What should we pay attention to when deploying deception security
- Overview of the type of deceptions (low-medium-high interactions) deployed today.

**Module 2: Low-Interaction Honeypots**

- Demonstration and hands-on labs on selected low-interaction honeypots: Artiellery, BearTrap, PortSpoof, SpiderTrap, Weblabryinth, and WordPot [All under the ADHD distribution]

- The purpose: Stalling the hacker
- Up and Down sides of each implementation
- What can we take from low-interaction honeypots to our organizations?

**Module 3: Medium-Interaction Honeypots**

- Demonstration and hands-on labs on selected medium-interaction honeypots: Glastopf Web App and Windows KFSensor
- The purpose: Making the hacker feel safe to expose hacking tools
- Lesson 1&2: Glastopf Web-App – template-based vs. vulnrability emulator based web honeypot. We will unpack the mechanisms, PHP SandBox usage, and four types of vulnrability emulation: RFI, LFI, Index, and Unknown type of attacks.
- Lesson 3: Windows KFSensor – Emulation of a variety of Windows Services under a heavily monitored Windows Machine
- What can we take from medium-interaction honeypots to our organizations?

**Module 4: High-Interaction Honeypots**

- Demonstration and hands-on labs on selected high-interaction honeypots: HonSSH, MazeRunner [Cymmetria]
- The purpose: Making the hacker feel safe and analyzing the exposed hacking tools.
- Lesson 1 & 2: HonSSH – An advanced Terminal-based honeypot of SSH tunneling – will be studied in conjuction with OpenVZ decoys to build a full data center and capture the behaivor of hackers as they are trying to log into system servers and turn them into Bots.
- Lesson 3: MazeRunner [Cymmteria] – Emulation of a variety of Data Center services, applied with agentless breadcumbs (Cookies, Credentials, Shared Folder Connections, and etc.) to give a full deception scenerio to the hacker.

**Module 5: Honeytokens**

- Demonstration of the concept of Honeytokens – how is it used? What is the added value?
- The purpose: Revealing and locating stoled sensitive informaiton
- 0.5 lesson: Overview of the Honeybadger server to trace geo-location and Docz.py generator of inserting webbugs into *.Docx documents. Molehunt tool can also attach documents to suspect list from within the organizaiton.

**Module 6: Final Project**

- Students would demonstrate the gained knowledge by defending their own assets based solely on honeypots technologies.
- They will be divided into teams – each team will design its own infrastructure to protect its flag.
- Each team would have one Kali-Linux machine to capture the flag of the other team.
- Score Criteria: 80% - Accuracy of defense report based on the attacking strategy of the other team. 20% - The ability to capture the other team's flag.