

Department of Physics and Astronomy

Heidelberg University

Master thesis

in Computer Science

submitted by

Stefan Machmeier

born in Heidelberg

2022

# Honeypot Implementation

## in a

# Cloud Environment

This Master thesis has been carried out by Stefan Machmeier

at the

EMCL

under the supervision of

Herrn Prof. Dr. Vincent Heuveline

**(Titel der Masterarbeit - deutsch):**

**(Title of Master thesis - english):**

# Contents

<b>1</b>	<b>Introduction</b>	<b>5</b>
1.1	Problem description . . . . .	5
1.2	Justification, motivation and benefits . . . . .	5
1.3	Research questions . . . . .	5
1.4	Limitations . . . . .	5
<b>2</b>	<b>Background</b>	<b>6</b>
2.1	Cloud Computing . . . . .	6
2.2	Honeypots . . . . .	6
2.2.1	Definition of a Honeypot . . . . .	6
2.2.2	Honeyd . . . . .	6
2.2.3	Configuration Honeyd . . . . .	6
2.2.4	Honeynets . . . . .	6
2.2.5	Legal Issues . . . . .	6
2.3	Intrusion Detection System . . . . .	6
2.4	HoneyTrap . . . . .	6
2.5	T-Pot . . . . .	6
<b>3</b>	<b>Related Work</b>	<b>7</b>
3.1	The Bait and Switch Honeypot . . . . .	7
3.2	Intrusion Trap System . . . . .	7
3.3	Honeycomb . . . . .	7
<b>4</b>	<b>Practical Work</b>	<b>8</b>
4.1	Attack vectors . . . . .	8
4.2	Concept . . . . .	8
<b>5</b>	<b>Experimental Work</b>	<b>9</b>
5.1	SNORT . . . . .	9
<b>6</b>	<b>Conclusion</b>	<b>10</b>
6.1	Future work . . . . .	10

# 1 Introduction

## 1.1 Problem description

## 1.2 Justification, motivation and benefits

## 1.3 Research questions

## 1.4 Limitations

## 2 Background

### 2.1 Cloud Computing

### 2.2 Honeypots

#### 2.2.1 Definition of a Honeypot

#### 2.2.2 Honeyd

#### 2.2.3 Configuration Honeyd

#### 2.2.4 Honeynets

#### 2.2.5 Legal Issues

Honeypots Tracking Hackers

### 2.3 Intrusion Detection System

### 2.4 HoneyTrap

### 2.5 T-Pot

## 3 Related Work

### 3.1 The Bait and Switch Honeytrap

### 3.2 Intrusion Trap System

### 3.3 Honeycomb

## 4 Practical Work

### 4.1 Attack vectors

### 4.2 Concept



## 5 Experimental Work

Connect results of Honeypots with NIDS/IDS to update rules.

### 5.1 SNORT

## 6 Conclusion

### 6.1 Future work