Faculty of Mathematics and Computer Science

Heidelberg University

Master thesis

in Computer Science

submitted by

Stefan Machmeier

born in Heidelberg

1996

Honeypot Implementation

in a

Cloud Environment

This Master thesis has been carried out by Stefan Machmeier

at the

Engineering Mathematics and Computing Lab

under the supervision of

Herrn Prof. Dr. Vincent Heuveline

(Titel der Masterarbeit - deutsch):

(Title of Master thesis - english):

Contents

List of Figures

List of Tables

1 Introduction

1.1 Problem description

1.2 Justification, motivation and benefits

1.3 Research questions

1.4 Limitations

2 Background

This chapter concludes the fundamental knowledge that is needed to comprehend the upcoming practical work. Firstly, an introduction to cloud computing will be held. Next, a throrough understanding of honeypots is given. Lastly, we introduce some concepts of intrusion detection systens.

2.1 Cloud Computing

Nowadays it is one of the well-known keywords and has been used by vary large companies such as Google, or Amazon, however, the term ”cloud computing” dates back to the late 1996, when a small group of technology executives of Compaq Computer framed new business ideas around the Internet.[Reg20] In this section, we want to give basic unterstandings of cloud computing, and give a short introduction to HeiCloud.

2.1.1 Definition of Cloud Computing

Considering the definition of Brian Hayes, cloud computing is ”a shift in the geography of computation” [Hay08]. Thus,

2.1.2 Service models

Software-as-a-Service

Platform-as-a-Service

Infrastructure-as-a-Service

2.1.3 Deployment models

Public Cloud

Private Cloud

Hybrid Cloud

2.1.4 Cloud Security

[NCM12]

2.1.5 HeiCloud

2.2 Honeypots

The first public honeypot [Spi03]

2.2.1 Definition of a Honeypot

[Spi03]

High-interaction honeypots

Low-interaction honeypots

Pure honeypots

2.2.2 Honeynets

[Spi03]

2.2.3 Legal Issues

[Spi03]

2.3 Intrusion Detection System

3 Previous Work

3.1 The Bait'n'Switch Honeypot

[PD05]

3.2 Intrusion Trap System

[PD05]

3.3 Honeycomb

[PD05]

3.4 Honeypots in a cloud environment

[KPM+21]

4 Practical Work

4.1 Attack vectors

4.2 Proposed Honeypots

4.3 Concept

4.4 HoneyTrap

5 Experimental Work

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

5.1 SNORT

6 Evaluation

6.1 T-Pot

7 Conclusion

7.1 Future work

Bibliography

[AFG+10] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. A view of cloud computing. *Communications of the ACM*, 53(4):50–58, April 2010.

[BPPP12] Bhavesh Borisaniya, Avi Patel, Dhiren R. Patel, and Hiren Patel. Incorporating honeypot for intrusion detection in cloud infrastructure. In Theo Dimitrakos, Rajat Moona, Dhiren Patel, and D. Harrison McKnight, editors, *Trust Management VI*, pages 84–96, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[Hay08] Brian Hayes. Cloud computing, 2008.

[JXW06] Xuxian Jiang, Dongyan Xu, and Yi-Min Wang. Collapsar: A VM-based honeyfarm and reverse honeyfarm architecture for network attack capture and detention. *Journal of Parallel and Distributed Computing*, 66(9):1165–1180, September 2006.

[KPM+21] Christopher Kelly, Nikolaos Pitropakis, Alexios Mylonas, Sean McKeown, and William J. Buchanan. A comparative analysis of honeypots on different cloud platforms. *Sensors*, 21(7):2433, April 2021.

[KSAMA04] I. Kuwatly, M. Sraj, Z. Al Masri, and H. Artail. A dynamic honeypot design for intrusion detection. In *The IEEE/ACS International Conference onPervasive Services, 2004. ICPS 2004. Proceedings.*, pages 95–104, 2004.

[MP17] Varan Mahajan and Sateesh K Peddoju. Integration of network intrusion detection systems and honeypot networks for cloud security. In *2017 International Conference on Computing, Communication and Automation (ICCCA)*, pages 829–834, 2017.

[NCM12] SR Nithin Chandra and TM Madhuri. Cloud security using honeypot systems. *International Journal of Scientific & Engineering Research*, 3(3):1, 2012.

[NWS+16] Marcin Nawrocki, Matthias Wählisch, Thomas C. Schmidt, Christian Keil, and Jochen Schönfelder. A survey on honeypot software and data analysis. *CoRR*, abs/1608.06249, 2016.

[PD05] G. Schaefer P. Diebold, A. Hess. A honeypot architecture for detecting and analyzing unknown network attacks, Feburary 2005.

[Pro03] Niels Provos. Honeyd: A virtual honeypot daemon (extended abstract). 01 2003.

[Reg20] Antonio Regalado. Who coined 'cloud computing'?, Feb 2020.

[Spi03] Lance Spitzner. *Honeypots - Tracking Hackers*. Addison-Wesley, Amsterdam, 2003.

[STO+11] Jungsuk Song, Hiroki Takakura, Yasuo Okabe, Masashi Eto, Daisuke Inoue, and Koji Nakao. Statistical analysis of honeypot data and building of kyoto 2006+ dataset for nids evaluation. In *Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security*, BADGERS '11, page 29–36, New York, NY, USA, 2011. Association for Computing Machinery.

[Wen21] Steffen Wendzel. *IT-Sicherheit für TCP/IP- und IoT-Netzwerke*. Springer Fachmedien Wiesbaden, 2021.

[WvLY+10] Lizhe Wang, Gregor von Laszewski, Andrew Younge, Xi He, Marcel Kunze, Jie Tao, and Cheng Fu. Cloud computing: a perspective study. *New Generation Computing*, 28(2):137–146, April 2010.

[ZPY16] Yin Zhang, Limei Peng, and Chan-Hyun Youn, editors. *Cloud Computing*. Springer International Publishing, 2016.