Faculty of Mathematics and Computer Science

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

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

2.1 Cloud Computing

2.1.1 Cloud Provider

2.1.2 HeiCloud

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

3 Related Work

3.1 The Bait and Switch Honeypot

3.2 Intrusion Trap System

3.3 Honeycomb

4 Practical Work

4.1 Attack vectors

4.2 Concept

4.3 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

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., and Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, 53(4):50–58.

Borisaniya, B., Patel, A., Patel, D. R., and Patel, H. (2012). Incorporating honeypot for intrusion detection in cloud infrastructure. In Dimitrakos, T., Moona, R., Patel, D., and McKnight, D. H., editors, *Trust Management VI*, pages 84–96, Berlin, Heidelberg. Springer Berlin Heidelberg.

Hayes, B. (2008). Cloud computing.

Jiang, X., Xu, D., and Wang, Y.-M. (2006). 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.

Kelly, C., Pitropakis, N., Mylonas, A., McKeown, S., and Buchanan, W. J. (2021). A comparative analysis of honeypots on different cloud platforms. *Sensors*, 21(7):2433.

Kuwatly, I., Sraj, M., Al Masri, Z., and Artail, H. (2004). A dynamic honeypot design for intrusion detection. In *The IEEE/ACS International Conference on-Pervasive Services, 2004. ICPS 2004. Proceedings.*, pages 95–104.

Mahajan, V. and Peddoju, S. K. (2017). 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.

Nawrocki, M., Wählisch, M., Schmidt, T. C., Keil, C., and Schönfelder, J. (2016). A survey on honeypot software and data analysis. *CoRR*, abs/1608.06249.

P. Diebold, A. Hess, G. S. (2005). A honeypot architecture for detecting and analyzing unknown network attacks.

Provos, N. (2003). Honeyd: A virtual honeypot daemon (extended abstract).

Song, J., Takakura, H., Okabe, Y., Eto, M., Inoue, D., and Nakao, K. (2011). 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. Association for Computing Machinery.

Spitzner, L. (2003). *Honeypots - Tracking Hackers*. Addison-Wesley, Amsterdam.

Wang, L., von Laszewski, G., Younge, A., He, X., Kunze, M., Tao, J., and Fu, C. (2010). Cloud computing: a perspective study. *New Generation Computing*, 28(2):137–146.

Wendzel, S. (2021). *IT-Sicherheit für TCP/IP- und IoT-Netzwerke*. Springer Fachmedien Wiesbaden.

Zhang, Y., Peng, L., and Youn, C.-H., editors (2016). *Cloud Computing*. Springer International Publishing.