

DOKUMENTATION

zur Vorlesung Systemadministration
im Bachelor Studiengang Angewandte Informatik

Wintersemester 2016 / 2017
bei Herr Prof. Dr. Eggendorfer

Umsetzung von einem Honeypot auf Basis eines Raspberry Pi

Michael Stroh
Matrikelnr. 24972

Daniel Schwenk
Matrikelnr. 24961

12. Oktober 2016

Inhaltsverzeichnis

1	Einleitung	1
1.1	Motivation	1
1.2	Ziele	1
1.3	Eigene Leistung	2
2	Anforderungen	3
2.1	Muss-Kriterien	3
2.2	Soll-Kriterien	4
2.3	Kann-Kriterien	4
3	Gantt-Diagramm	5

1 Einleitung

Das Internet und die Digitalisierung, die in alle Lebensbereiche Einzug erhält, verändern Gesellschaft, Wirtschaft und Kultur. Egal ob im privaten oder beruflichen Umfeld, ständig sind wir von Computern in Form von Arbeitsgeräten, Smartphones oder anderen Geräten umgeben. Diese Vernetzung wird in den nächsten Jahren im Zuge der „Internet-der-Dinge-Evolution“ weiter drastisch zunehmen.

Ein oft vernachlässigter Aspekt hierbei ist das Thema „IT-Sicherheit“. Keine Software ist frei von Fehlern und Sicherheitslücken. Es bedarf einen großen Aufwand, um eine Infrastruktur vor möglichen Angriffen zu schützen.

1.1 Motivation

Durch unsere privaten wie auch beruflichen Tätigkeiten im Systemadministratorenumfeld werden auch wir mit dem Thema der Absicherung von Infrastrukturen konfrontiert.

sind beide als Systemadministratoren tätig betreuen eigene Netzwerkumgebungen, wollen wissen über mögliche Angriffe sammeln, wollen kleines kostengünstiges, einfach zu konfigurierendes honeypot system haben, wollen erfahrungen sammeln, ...?

1.2 Ziele

Ziel dieser Arbeit ist es, ein System zu entwickeln, dass als Honeypot dient. Dieser Honeypot soll eingesetzt werden, um Informationen über Angriffsmuster und Angreiferverhalten zu erhalten. Dazu stellt das System ein vermeintlich leicht angreifbares Ziel dar.

Jegliche Zugriffe und Aktivitäten die ein Angriff hinterlässt werden protokolliert und ausgewertet. Mit Hilfe von diesem Wissen kann eine reale Netzwerkumgebung gegen Angriffe abgesichert werden.

- Primärziel: einsatzfähige(r) Honeypot(s) - sicher, authentisch und lehrreich
- Sekundärziel: von Angreifern lernen

1.3 Eigene Leistung

Die Bereitstellung einer für einen potentiellen Angreifer authentische Umgebung, sowie die Einbettung des Honeypots in selbige.

- Bereitstellung einer authentischen Umgebung für den Honeypot
- Gewährleistung der Sicherheit für das eigene und das globale Netz
- Inbetriebnahme des Honeypots
- Auswertung von Log-Files et cetera

2 Anforderungen

Die Anforderungen an das Honeypot-System werden in Muss-, Kann- und Soll-Kriterien unterteilt.

2.1 Muss-Kriterien

- Honeypot simuliert eine Auswahl an Diensten (http, ssh, ftp)
- Honeypot simuliert offenes WLAN-Netz / Fake-Access-Point
- Angreifer hat keine Möglichkeit zur Interaktion mit dem Host-Betriebssystem
- Angreifer bekommt keine bzw. nur gefälschte Antworten auf seine Anfragen
- Überwachung des ein- und ausgehenden Netzwerkverkehrs
- Protokollierung darf für Angreifer nicht sichtbar sein
- Protokollierte Daten dürfen durch Angreifer nicht verändert werden können
- Honeypot muss jederzeit deaktivierbar sein
- Honeypot muss für Zeit X online / aktiv sein, um ein realistisches Angriffsziel zu sein
- Honeypot ist im Internet erreichbar
- Produktivsysteme dürfen keiner Gefahr ausgesetzt werden
- Honeypot muss in DMZ sein und darf keine Gefahr für unbeteiligte Dritte darstellen
















































2.2 Soll-Kriterien

- automatisierte Auswertung von Logdaten
- automatische Benachrichtigung, wenn System angegriffen wird
- Honeypot kann einfach zurückgesetzt / neu aufgesetzt werden (beispielsweise durch Skript zur automatischen Einrichtung / Konfiguration)
- Logdateien / ausgewertete Dateien werden automatisch separat gespeichert (extra System, Cloud-Speicher)

2.3 Kann-Kriterien

- geringer Stromverbrauch von Honeypot-System
- kostengünstiger Versuchsaufbau
- Reverse DNS-Lookup von Angreifer-IP-Adresse(n)
- Simulation weiterer Geräte (Router, Firewall, PC)

3 Gantt-Diagramm

		Name	Duration	Start	Finish	Predecessors	Resources
1	  	Bestimmung der Rahmenbedingungen	2d	14/10/2016	17/10/2016		Daniel, Michael
2	  	Erreichbarkeits-Test der Einsatzumgebung	3d	14/10/2016	18/10/2016		Daniel, Michael
3	  	Einsatz einer Firewall	2d	19/10/2016	20/10/2016	1,2	Daniel, Michael
4	  	Honeypot: Aufsetzen/Grundinstallation	4d	21/10/2016	26/10/2016	3	Daniel, Michael
5	  	Honeypot: Umsetzung Anforderungen der Rubrik "Must"	7d	27/10/2016	04/11/2016	3,4	Daniel, Michael
6	  	Honeypot: Umsetzung Anforderungen der Rubrik "Should"	6d	28/10/2016	04/11/2016	3,4	Daniel, Michael
7	  	Honeypot: Umsetzung Anforderungen der Rubrik "Could"	5d	31/10/2016	04/11/2016	3,4	Daniel, Michael
8	 	Honeypot: Zwischentest (Lokal)	1d	07/11/2016	07/11/2016	5,6	Daniel, Michael
9	 	Honeypot: Zwischentest (Externer Zugriff)	1d	08/11/2016	08/11/2016	5,6,8	Daniel, Michael
10	 	Dokumentation der bestehenden Umgebung	4d	09/11/2016	14/11/2016	8,9	Daniel, Michael
11	 	Honeypot-Phase 1	4d	09/11/2016	14/11/2016	9	Daniel, Michael
12	  	Analyse, Auswertung und Dokumentation der ersten Angriffsphase	4d	11/11/2016	16/11/2016		Daniel, Michael
13	  	Vornehmen von mögl. Anpassungen / Optimierungen	4d	17/11/2016	22/11/2016	12	Daniel, Michael
14	 	Honeypot-Phase 2	4d	23/11/2016	28/11/2016	13	Daniel, Michael
15	  	Analyse und Auswertung der zweiten Angriffsphase	4d	24/11/2016	29/11/2016	13	Daniel, Michael
16	  	Dokumentation der Ergebnisse	6d	25/11/2016	02/12/2016		Daniel, Michael
17	  	Überarbeitung Dokumentation	10d	05/12/2016	16/12/2016	16	Daniel, Michael

