Hochschule
Ravensburg-Weingarten
Technik | Wirtschaft | Sozialwesen

Projektskizze

zur Vorlesung Systemadministration
im Bachelor Studiengang Angewandte Informatik

Wintersemester 2016 / 2017
bei Herr Prof. Dr. Eggendorfer

Umsetzung von einem Honeypot

Michael Stroh
Matrikelnr. 24972

Daniel Schwenk
Matrikelnr. 24961

13. Oktober 2016

Inhaltsverzeichnis

1 Einleitung

Das Internet und die Digitalisierung, die in alle Lebensbereiche Einzug hält, 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 Verbreitung sowie die Vernetzung von Geräten untereinander wird in den nächsten Jahren im Zuge der „Internet-der-Dinge-Evolution“ weiter drastisch zunehmen.

Ein oft vernachlässigter Aspekt ist hierbei das Thema „IT-Sicherheit“. Keine Software ist frei von Fehlern und Sicherheitslücken. Falsch konfigurierte Dienste und Software, die nicht regelmäßig aktualisiert wird, sind ein leichtes Ziel für Angreifer. Durch die zunehmende Vernetzung wird das Thema IT-Sicherheit in Zukunft weiter an Bedeutung gewinnen.

Um eine Infrastruktur, egal ob im privaten oder geschäftlichen Bereich, vor möglichen Angriffen zu schützen bedarf es einen immer größeren Aufwand.

1.1 Motivation

Durch unsere beruflichen wie auch privaten Tätigkeiten im Bereich der Systemadministration sehen auch wir uns mehr und mehr mit dem Thema „IT-Sicherheit“, insbesondere im Bereich der Absicherung von Infrastrukturen, konfrontiert.

Die Gewährleistung dieser Sicherheit ist mittlerweile eine immens wichtige, wenn nicht sogar die wichtigste Anforderung an eine intakte IT-Infrastruktur. Jegliche Bemühungen dieser Anforderung gerecht zu werden sind Teil des täglichen Brots eines Systemadministrators.

Das Konzept eines Honeypots, also einen potentiellen Angreifer nicht nur vor eigentlich wichtigen System fernzuhalten, sondern auch noch von seinem Wissen zu profitieren, stellt dabei einen hochspannenden Ansatz dar. Unsere Hoffnung ist es, dass dieser Ansatz dazu in der Lage ist, uns dabei zu helfen, die Sicherheit unserer Systeme hochzuhalten und uns unser tägliches Brot etwas zu „versüßen“.

1.2 Ziele

Ziel dieser Arbeit ist es, ein System zu entwickeln, das als Honeypot dient. Dieser Honeypot soll eingesetzt werden, um Einblicke in die Vorgehensweise eines Angreifers zu bekommen. Das System stellt dazu ein vermeintlich leicht angreifbares Ziel dar.

Jegliche Zugriffe und Aktivitäten die ein Angriff hinterlässt werden protokolliert und ausgewertet. Das hierbei gewonnene Wissen soll in Form von IT-Sicherheitsmaßnahmen in bestehende und künftige IT-Infrastrukturen einfließen.

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

1.3 Eigene Leistung

Der Hauptbestandteil dieses Projekts liegt in der Inbetriebnahme und Bereitstellung eines Honeypots, sowie die Integration desselben in eine für einen potentiellen Angreifer authentisch erscheinenden Umgebung. Dabei liegt das Hauptaugenmerk auf der Gewährleistung von absoluter Sicherheit sowohl für das eigene als auch für das globale Netz. Selbstverständlich werden aber auch Auswertung und Dokumentation stattgefundener Angriffe nicht zu kurz kommen.

- Bereitstellung einer authentischen Umgebung für den Honeypot
- Gewährleistung der Sicherheit für das eigene und das globale Netz
- Inbetriebnahme des Honeypots selbst
- Auswertung von Log-Files et cetera
- Dokumentation von Honeypot inkl. Umgebung, Angriffsphase und Ergebnisse

2 Anforderungen

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

2.1 Muss-Kriterien

- Honeypot ist über das Internet erreichbar
- Honeypot darf keinerlei Gefahr für andere Systeme darstellen
- Honeypot muss jederzeit deaktivierbar sein
- Angreifer darf keinerlei Möglichkeit zur Interaktion mit dem Host-Betriebssystem haben
- Angreifer darf keine bzw. nur gefälschte Antworten auf Anfragen erhalten
- Honeypot muss mindestens einen, besser jedoch mehrere Dienste, wie beispielsweise HTTP, SSH oder FTP, simulieren/anbieten
- Honeypot muss ein realistisch wirkendes Angriffsziel darstellen
- Angriffe werden geloggt
- ein- und ausgehender Netzwerkverkehr muss (überwacht und) geloggt werden
- protokollierte Daten dürfen durch Angreifer nicht verändert werden können

2.2 Soll-Kriterien

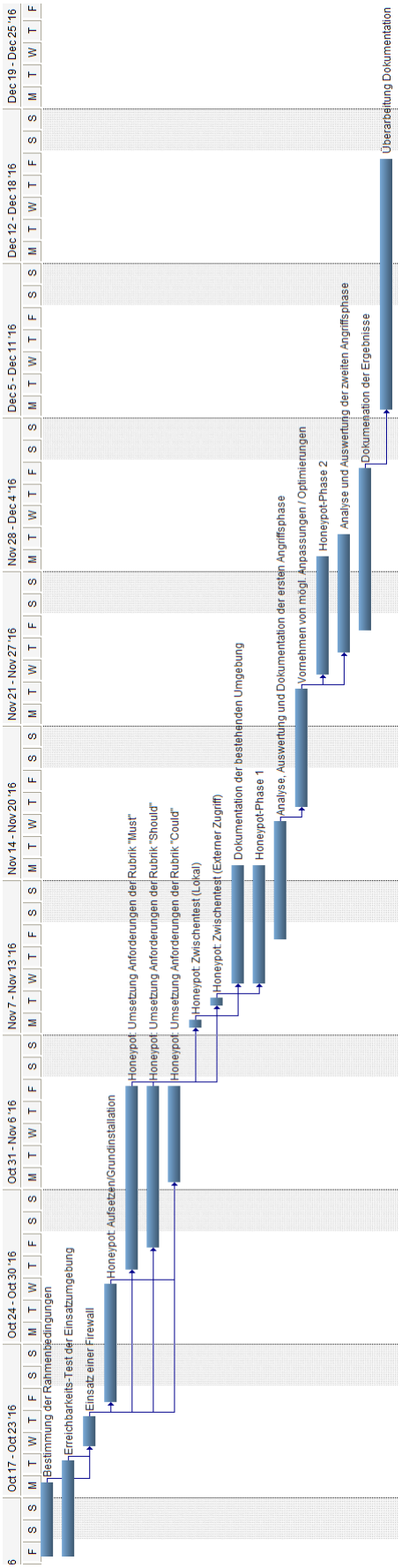
- automatische Benachrichtigung, wenn System angegriffen wird
- Protokollierung und ggf. Forwarding von Log-Files dürfen für den Angreifer nicht sichtbar sein
- automatisierte Auswertung von Logdaten
- Logdateien / ausgewertete Daten werden automatisch separat gespeichert (extra System, Cloud-Speicher)

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)
- Honeypot simuliert offenes WLAN-Netz / Fake-Access-Point

3 Gantt-Diagramm

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


Oct 17 - Oct 23 '16
Oct 24 - Oct 30 '16
Oct 31 - Nov 6 '16
Nov 7 - Nov 13 '16
Nov 14 - Nov 20 '16
Nov 21 - Nov 27 '16
Nov 28 - Dec 4 '16
Dec 5 - Dec 11 '16
Dec 12 - Dec 18 '16
Dec 19 - Dec 25 '16
Bestimmung der Rahmenbedingungen
Erreichbarkeits-Test der Einsatzumgebung
Einsatz einer Firewall
Honeypot Aufsetzen/Grundinstallation
Honeypot Umsetzung Anforderungen der Rubrik "Must"
Honeypot Umsetzung Anforderungen der Rubrik "Should"
Honeypot Umsetzung Anforderungen der Rubrik "Could"
Honeypot Zwischentest (Lokal)
Honeypot Zwischentest (Externer Zugriff)
Dokumentation der bestehenden Umgebung
Honeypot-Phase 1
Analyse, Auswertung und Dokumentation der ersten Angriffsphase
Vornehmen von mögl. Anpassungen / Optimierungen
Honeypot-Phase 2
Analyse und Auswertung der zweiten Angriffsphase
Dokumentation der Ergebnisse
Überarbeitung Dokumentation