Hochschule
Ravensburg-Weingarten
Technik | Wirtschaft | Sozialwesen

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

05. Oktober 2016

Inhaltsverzeichnis

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 kofigruerendes 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.

1.3 Eigene Leistung

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Aenean commodo ligula eget dolor. Aenean massa. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur

ridiculus mus. Donec quam felis, ultricies nec, pellentesque eu, pretium quis, sem. Nulla consequat massa quis enim. Donec pede justo, fringilla vel, aliquet nec, vulputate eget, arcu. In enim justo, rhoncus ut, imperdiet a, venenatis vitae, justo. Nullam dictum felis eu pede mollis pretium. Integer tincidunt. Cras dapibus.

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 Betriebssystem
- Angreifer bekommt keine bzw. nur gefälschte Antworten auf seine Anfragen
- ...
- Sammeln von Informationen z.B. über Verwundbarkeiten, Angreiferverhalten (Werkzeuge, Taktiken,Motive) ??
- 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 (x Stunden, x Wochen?) um ein realistisches Angriffsziel zu sein
- ..
- Positionnierung
- Honeypot ist im Internet erreichbar
- separater Honeypot ist im internen Netz erreichbar?
- Produktivsysteme dürfen keiner Gefahr ausgesetzt werden (?)

2.2 Soll-Kriterien

- das System soll einen möglichst geringer Stromverbrauch haben
- das System soll kostengünstig sein (Hardware)
- ...?

2.3 Kann-Kriterien

- automatische Benachrichtigung, wenn System angegriffen wird
- automatisierte Auswertung von Logdateien
- ...
- Honeypot kann einfach zurückgesetzt / neu aufgesetzt werden (Skript zur automatischen einrichtung / konfiguration schreiben)?
- Logdateien / ausgewertete Dateien werden automatisch separat gespeichert (extra System, Cloud-Speicher, . . . ?)