Systemadministration Projekt

Hier sind die Dateien für das Projekt "Systemadministration" enthalten. Sowohl das Projekt an sich, als auch die Dokumentation.

Projektteilnehmher:

- Benedikt Geiger
- Ruben Miller

Grundidee

Überwachung eines Systems durch IDS, die auf einem Raspberry Pi laufen.

Genauere Skizze

Auf dem Raspberry Pi sollen IDS laufen, die sowohl die Disc als auch das Netzwerk überwachen. Der Raspberry Pi soll dabei von dem überwachten System nicht kontrolliert werden können, da bei einem erfolgreichen Angriff dieser unmöglich verändert werden kann. Noch besser wäre, wenn dieser nicht entdeckbar ist.

Disc-Scan

Der Raspberry Pi soll in regelmäßigen Abstanden die Festplatte kontrollieren, bspw ein cronjob mit aide.

Dabei werden Hashwerte von relevanten Dateien (wie Configs oder binaries) erstellt, und beim ersten Einrichten des Servers in einer Referenzdatenbank gespeichert. So sind sie sicher noch nicht infiziert.

In regelmäßigen Abständen wird diese Referenzdatenbank dann mit neueren Ständen der Dateien verglichen, um Abweichungen zu finden. Hier kann noch untersucht werden, ob Technologien wie `inotify` oder `trusted timestamping` sinnvoll sind um dem Server Zeit und Rechenleistung zu ersparen, hinderlich sind, oder sogar ein Sicherheitsrisiko.

Network-Scan

Beim Network Scan, wird der Raspberry als Gateway und als DNS-Server zwischen den Server und das Internet geschaltet. Die auf ihm befindliche Software scannt alle Pakete die ein und aus gehen nach Auffälligkeiten. Hier gibt es zwei verschiedene Ansätze: Signaturbasierte IDS und anomaliebasierten IDS.

Bei einem signaturbasierten IDS, auch bekannt als wissensbasiertes IDS, wird nach Regeln oder Mustern für bekannten bösartigen Datenverkehr gesucht. Bei einem anomaliebasierten IDS, auch bekannt als verhaltensbasiertes IDS, ist die Aktivität, die den Datenverkehr generiert hat, weitaus wichtiger als die zugestellte Nutzlast.

Ein auf Anomalien basierendes IDS-Tool basiert auf Baselines und nicht auf Signaturen. Es wird nach ungewöhnlichen Aktivitäten gesucht, die vom statistischen Durchschnitt früherer Aktivitäten oder zuvor gesehener Aktivitäten abweichen. Wenn sich beispielsweise ein Benutzer immer von Kalifornien aus in das Netzwerk einloggt und auf technische Dateien zugreift, ist dies ein Warnsignal, wenn sich derselbe Benutzer von Peking aus anmeldet und sich HR-Dateien ansieht.

Zudem kann hier ein Pi-Hole integriert werden, welches mit enormen Blocklisten und schnellen RegEx-Filter basierten Regeln schon erste Angriffe verhindern kann.

Technologien

Wir verwenden zum Scannen die Technologie Advanced Intrusion Detection Environment kurz AIDE. Hier kann untersucht werden, ob zusätzlich noch Software wie inotify oder Trusted timestamping sinnvoll ist, um den Vorgang zu beschleunigen und Rechenleistung zu sparen. Zudem kann hier noch ein Standard Antivirenprogramm für einfache Angriffe wie ClamAV verwendet werden.

Für Network Scans verwenden wir entweder Zeek oder Suricata. Zudem kann hier noch ein Pi-hole eingerichtet werden, um erste Angriffe schon vor dem Geschehen abzublocken.

All diese Technologien sind Kostenfrei und Open-Source.

Roadmap

- [ ] Installation Skript
  - [ ] Skript für den Server, welches (wenn nicht vorhanden) ein Zertifikat erstellt, auf dem PI hinterlegt und dem PI alle nötigen Informationen über den Server gibt
- [ ] Netzwerk Traffic scannen
  - [ ] Pihole als erste Instanz (Nicht wirklich zum Scannen geeignet, aber zur Intrusion Protection)
  - [ ] Zum Scannen:
    - The Zeek Network Security Monitor
    - Home - Suricata
- [ ] Disc Scannen
  - [ ] wird mittels des SSH-Zertifikats vom PI aus gestartet
  - [ ] Server macht die Arbeit
  - [ ] Welche Directories brauchen wir?
  - [ ] Zusätzlich: Virenscann?
  - [ ] von welchen Dateien brauchen wir den Hash um ihn auf dem Pi zu speichern? Können wir eine Vorauswall mittels **zuverlässigem** Timestamp treffen?
  - [ ] Wie verarbeitet der PI die Daten?
    - [ ] Datenbank
    - [ ] Abgleichen mittels eigener Software

- [ ] Angriff gefunden, was dann?
  - [ ] Server runterfahren?
  - [ ] Internet blocken?
  - [ ] Prozess(e) beenden?
  - [ ] Admin benachrichtigen?
    - [ ] Wie?

Quellen zum Nachlesen

- Pi-hole as a simple IDS? : r/pihole (reddit.com)
- Raspberry Pi 4GB as IDS / IPS ? : r/AskNetsec (reddit.com)
- Pi-hole – Network-wide Ad Blocking
- Nicht alle Dateien Scannen mittels
  - inotify › Wiki › ubuntuusers.de
  - Trusted timestamping - Wikipedia