Fachhochschule Nordwestschweiz
Hochschule für Technik

Cyber Security Labor (cysL)

Fachhochschule Nordwestschweiz
Hochschule für Technik

Cyber Security Labor (cysL)

u.ä. auslagern (modularisieren verbessern)

Inhalt

Inhalt

Vorbereitung
Spass mit Sicherheit
- Mit Nachos einen Egoshooter spielen

Lokale Schadaktivität erkennen
- Indikatoren für einen Angriff
- Festlegen von “Watchpoints” für die Überwachung
- Überwachungsarten
- Homogenisierung

Die Praxis
- Zustände erfassen

Repetition und Aufgabe

Vorbereitung

Recherche

Versuchen Sie eine Liste von kritischen Informationen eines Systems zu erstellen. Ein Anfang bildet der letzte Abschnitt unter “Indikatoren für einen Angriff”

Zum lesen oder anschauen ...

Schwachstellen in Antiviren-Software
Ein Bugreporting bei Trend Micro

Begriffe

Malware Scanner, Log-Collection, Konsolidierung von Logfiles und Zuständen.

Spass mit Sicherheit

Mit Nachos einen Egoshooter spielen

Nachos, Cheese, WLAN und Egoshooter

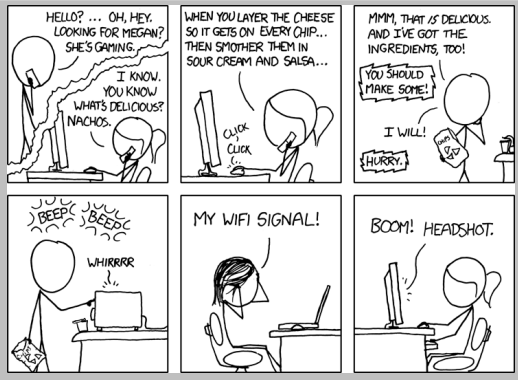

Abbildung: Headshot einmal anders

Quelle: XKCD

Lokale Schadaktivität erkennen

Indikatoren für einen Angriff

Indikatoren für Schadaktivität

- Reale Welt
  - Unerklärliche Datenleaks
  - Konkurrenz ist immer ein Schritt voraus
- Netzwerk
  - Ungewöhnliche Aktivitäten
    - Hohe Aktivität in einer SAT (Source Address Table) auf einem Switch
    - Viele Verbindungsversuche auf ein einzelnes System
    - Neue Routen
  - Erhöhter Netzwerkverkehr
    - Viele Verbindungsversuche auf ein einzelnes System
- System
  - Neue vertrauenswürdige Schlüssel (ssh authorized_keys oder CAs)
  - Unerklärliche Logins
  - Logfiles mit ungewöhnlichen Mitteilungen
  - Unerklärlich kleine Logfiles
  - Erhöhter Speicherplatzbedarf auf Systemen
  - Neue Files mit SUID- oder SGID-Berechtigungen
  - Neue Treiber/Module

Lokale Schadaktivität erkennen

Festlegen von “Watchpoints” für die Überwachung

Eine mögliche Auswahl von “Watchpoints”

- Neue “vertrauenswürdige” Schlüssel (ssh authorized_keys oder CAs)
  ⇒ Überwachen von /etc/authorized_keys und der Zertifikatsstore
- Unerklärliche Logins
  ⇒ Typische Pattern von Logins (z.B. Loginzeiten) definieren und überwachen.
- Logfiles mit ungewöhnlichen Mitteilungen
  ⇒ Statistische Erhebungen über Log-Mitteilungen .
- Erhöhter Speicherplatzbedarf auf Systemen
  ⇒ Speicherplatzwachstum überwachen und Speicherplatz von tmp- und log-Dateien kontrollieren.
- Neue Files mit SUID- oder SGID-Berechtigungen
  ⇒ Führen einer Liste von “zugelassenen Programmen mit SGID- und SSUID-Programmen.
- Neue Treiber/Module
  ⇒ Führen einer Liste von zugelassenen Treibern.

Lokale Schadaktivität erkennen

Überwachungsarten

Mögliche Überwachungsarten

- Push
  Die Informationen werden bei Erzeugung an ein zentrales System gesandt.
- Pull
  Die Informationen werden periodisch durch ein zentrales System abgegriffen.
- Hybrid
  Die Informationen werden schnellstmöglich propagiert aber auch periodisch abgegriffen.

Lokale Schadaktivität erkennen

Homogenisierung

Quellen

Grundsätzlich gibt es zwei verschiedene Arten von Informationen, die anfallen können

- Events
  Dies sind Meldungen, die aus einer Aktion heraus entstehen (z.B. Fehler beim Lesen eines Sektors).
- Zustände
  Dies sind Verkörperungen der gegenwärtigen Systemsituation (Liste der aktuell eingeloggten Benutzer).

Nicht alle Zustände können sinnvoll in Events und nicht alle Events sinnvoll in Zustände übersetzt werden.

Die Praxis

Zustände erfassen

Malware Scanner

Typischerweise erfassen Malware Scanner den Zustand. Im Idealfall aber versuchen sie den Zustand zeitnah zu erfassen.

Repetition und Aufgabe

Aufgabe

Versuchen sie einmal Logs “von Hand” zu analysieren, indem sie “grep” als Filter-Tool verwenden. Versuchen sie jetzt einmal das Selbe mit anderen Analysetools (Möglicher Startpunkt: http://www.findbestopensource.com/tagged/log-analysis). Machen sie jetzt einmal richtig Zoff. Verwenden Sie Beispielsweise einen SSH Brute-Force-Tester (Wie SSH Brute Force tester oder SSH FTP Brute Force). Was stellen sie fest? Wie einfach sind diese Attacken aufzuspüren? Was ist das Problem, wenn sie es auf andere Fälle übertragen.
Übrigens: Gute Wort-Listen finden Sie unter PacketstormSecurity oder können sie generieren mit hydra (Auf Kali installiert).
Versuchen sie sich doch einmal zu überlegen, was Ihnen ein Tool wie SSHguard bringt. In welchen Fällen hilft das Programm nicht oder nur wenig?

Repetition und Aufgabe

Nächster Block

Nächster Termin

Einreichen Übung 1 vor Beginn der Lektion 8 am 04.11.2025 (in 82235 Tagen)