=

Cyber Security Labor (cysL)

Martin Gwerder

..

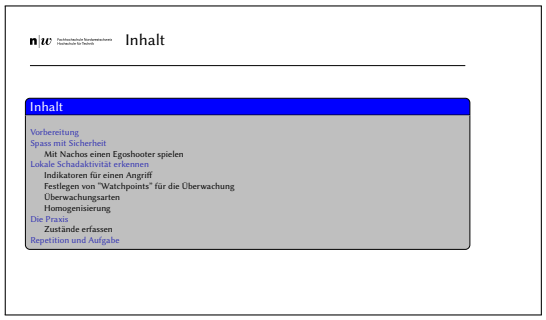


Abbildung 1: Inhaltsverzeichnis

Inhaltsverzeichnis

1 Vorbereitung

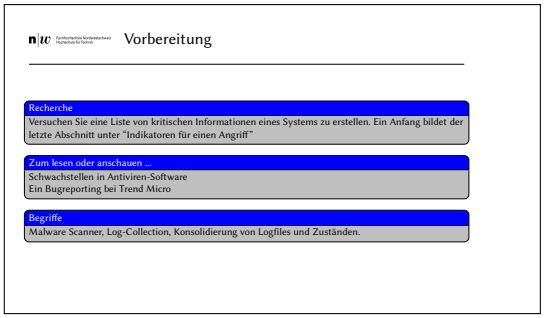


Abbildung 2: “Vorbereitung”/“”

Bitte arbeiten sie jeweils die Vorbereitungs-Slide vor(!) einer Lektion durch. Sie erlauben es damit, dass alle mit einem bestimmten Vorwissen in die Lektion kommen. Dies führt zu interessanteren, abwechslungsreicheren Diskussionen.

2 Spass mit Sicherheit

2.1 Mit Nachos einen Egoshooter spielen

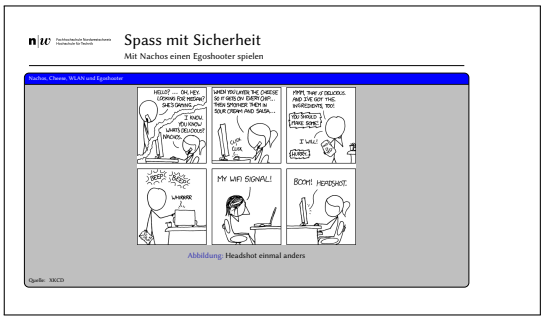


Abbildung 4: “Spass mit Sicherheit”/“Mit Nachos einen Egoshooter spielen”

Gewisse Dinge gehören nicht offensichtlich zusammen. In diesem Fall waren es Nachos, eine Mikrowelle ein WLAN-Router und ein Egoshooter. Das Problem bei der Abwehr ist, dass Hacker Dinge “unkonventionell” verwenden. Sie müssen also auch unkonventionell denken, wollen sie diese abwehren.

3 Lokale Schadaktivität erkennen

3.1 Indikatoren für einen Angriff

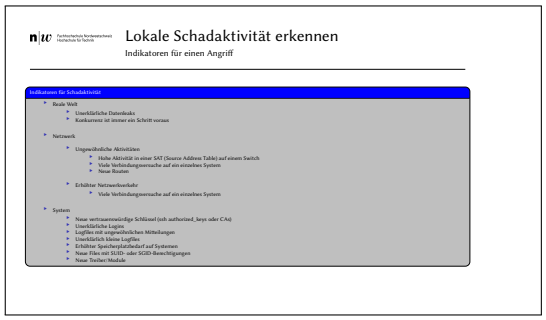


Abbildung 5: “Lokale Schadaktivität erkennen”/“Indikatoren für einen Angriff”

- 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)
    Dies gilt speziell für höher privilegierte Accounts wie root.
  - Unerklärliche Logins
    Es ist sicher erschreckend zu sehen, dass ein System $\approx 13'000$ Loginversuche innerhalb von 24h hinter sich hat. Viel schlimmer ist es aber zu sehen, das root zu unerklärlichen Zeiten eingeloggt hat.
  - Logfiles mit ungewöhnlichen Mitteilungen
    Wenn neue Log-Mitteilungen auftreten, dann hängt das häufig mit neuen Programmen zusammen (oder mit Updates) aber auch hier lohnt sich das kritische Hinterfragen.
  - Unerklärlich kleine Logfiles
    Wenn jemand sich Zutritt zu einem System verschafft hat, wird er versuchen (falls er wieder kommen möchte) seine Spuren zu verwischen.
  - Erhöhter Speicherplatzbedarf auf Systemen
  - Neue Files mit SUID- oder SGID-Berechtigungen
  - Neue Treiber/Module

3.2 Festlegen von “Watchpoints” für die Überwachung

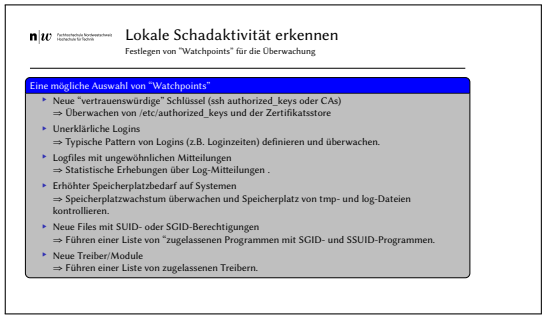


Abbildung 6: “Lokale Schadaktivität erkennen”/“Festlegen von “Watchpoints” für die Überwachung”

- 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.

3.3 Überwachungsarten

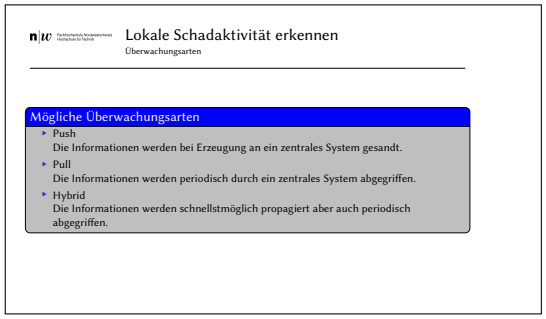


Abbildung 7: “Lokale Schadaktivität erkennen”/“Überwachungsarten”

- 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.

3.4 Homogenisierung

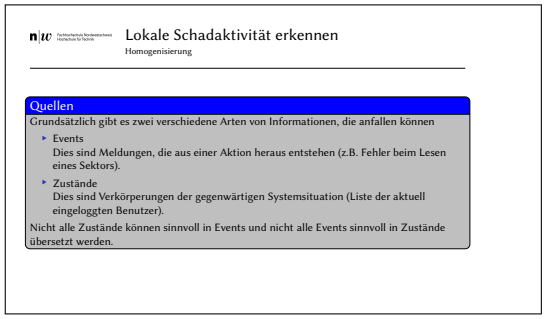


Abbildung 8: “Lokale Schadaktivität erkennen”/“Homogenisierung”

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

- Events
  Dies sind Meldungen, die aus einer Aktion heraus entstehen.
- Zustände
  Dies sind Verkörperungen der Gegenwärtigen Systemsituation.

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

Ein fehlgeschlagener Login hat beispielsweise keine Zustandsänderung zur Folge. Er kann aber wichtig sein. Auf der anderen Seite hat eine aktive Shell kein Gefahrenpotential. Dies kann sich ändern, wenn in Betracht gezogen wird, dass dieser Account vorgängig viele fehlgeschlagenen Logins hatte.

4 Die Praxis

4.1 Zustände erfassen

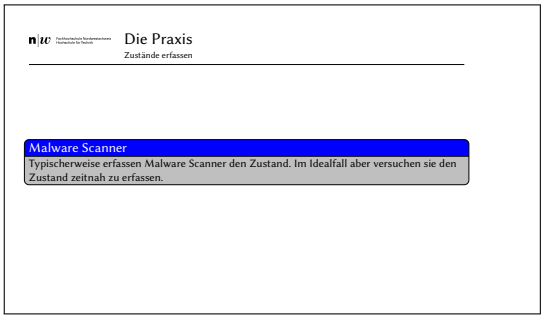
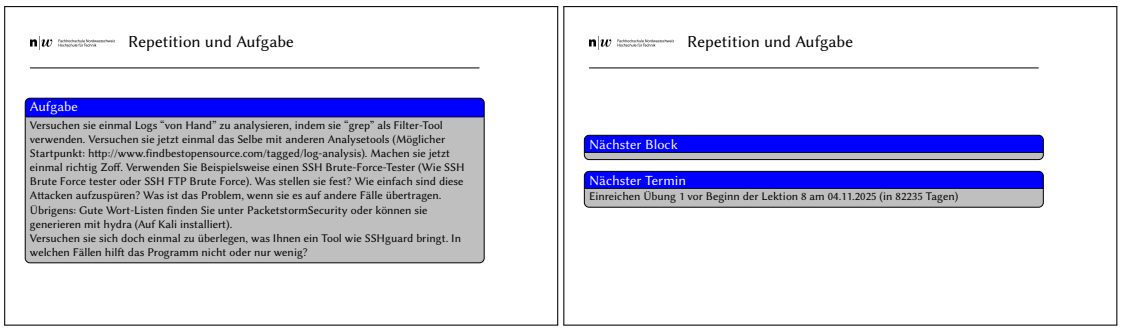


Abbildung 9: “Die Praxis”/“Zustände erfassen”

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

Um dies tun zu können Überwachen von sie Netzwerkverbindungen und Dateisysteme. Leider können diese Systeme nicht verschlüsselte Verbindungen überwachen (⇒ Schutz kann trivial umgangen werden). Auch ist die Transferleistung von und zur Disk viel zu hoch um sinnvoll der ganze Verkehr zu analysieren.

5 Repetition und Aufgabe



(a) "Repetition und Aufgabe"/"" (b) "Repetition und Aufgabe"/""

Abbildung 10

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/l 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?