Die Herausforderungen in der Logfileanalyse zur Angriffserkennung

Patrick Sauer, M.Sc.

29.01.2014
V1.0

Agenda

- Zielstellung
- Vorstellung: Wer bin ich, was mache ich?
- Angriffe und die Auswirkungen in den Logs
- Herausforderungen in der Auswertung
- Beispiel-Logfiles
  - sshd (real)
  - apache2 (real)
  - vsftpd (konstruiert)
- Fazit
- Im Anschluss: Live-Logs, „Live-Hacking“, <Wunsch xyz>

Zielstellung

- Verdeutlichung der Schwierigkeiten in der Logfileanalyse
- Durch Praxisbeispiele mehr Verständnis schaffen
- Diskussion; kein monotoner Vortrag!
- 20 Folien max. dafür Interaktion!
- Fragen beantworten, und zwar sofort!

Vorstellung Patrick Sauer

- Studium:
  - Diplom Wirtschaftsinformatiker (FH)
    Technische Hochschule Mittelhessen
  - Master of Science in Security Management
    Fachhochschule Brandenburg
    - Security Management / IT-Security
    - WPF: IT-Forensik
    - Master-Thesis: „Messung von Informationssicherheit“
- Zertifizierungen: CISSP, TISP, ...

- Security Blog:

http://blog.patricksauer.net

Vorstellung Patrick Sauer

Euro Payment Group

Chief Information Security Officer

- Seit 09 / 2010 (3,5 Jahre)
- Internet Payment Service Provider (Kreditkarten, Lastschrift)
- Fachliche Schwerpunkte
  - Security Management / PCI DSS
  - IT-Security & mehr

binary security binsec business true. risk false.

Information Security Consultant

- Seit 07 / 2013 (½ Jahr)
- Leistungen
  - Security Consulting
  - Secure Application Hosting
  - Ext. Datenschutzbeauftragter
  - (Penetration Testing)

SAUERSECURITY

Profil & mehr:
http://www.sauer-security.de

Unterschiedliche Angriffsvektoren

- Information Gathering
  - Google Hacking, DNS Enumeration, Port Scanning
- Client Side Attacks
  - Viren, Würmer, Trojaner
- Web Application Attacks
  - XSS, File Inclusion, SQL Injection
- Password Attacks
  - Brute Force, Dictionary Attack, Hash Attack
- (Distributed) Denial of Service / (D)DOS
- ……

Unterschiedliche Auswirkungen in den Logs!

(oder auch gar keine)

Typische Angriffserkennung!

- Es bemerkt der Falsche:

Von Hetzner Online AG <abuse@hetzner.de>
Betreff **[SysEng] [AbuseID:0E8086:18] Information about vulnerable systems for NTP reflection - an**
Antwort an [redacted] Hetzner Online AG <abuse@hetzner.de>
An [redacted]

[English version below]

Sehr geehrte Damen und Herren,

wir haben einen Spam- bzw. Abuse-Hinweis von certbund@bsi.bund.de erhalten.
Bitte treffen Sie alle nötigen Maßnahmen um dies künftig zu vermeiden.

Außerdem bitten wir Sie um die Abgabe einer kurzen Stellungnahme innerhalb
von 24h an uns und an die Person, die diese Beschwerde eingereicht hat.
Diese Stellungnahme soll Angaben enthalten, wie es zu dem Vorfall kommen
konnte, bzw. was Sie dagegen unternehmen werden.

Wie werden erfolgreiche Angriffe erkannt?

1. Gar nicht
2. Durch Dritte: Provider, Kunden, …
3. Durch andere Probleme (z.B. Fehler im System)
4. Meldung durch den Angreifer
5. Durch Zufall / Glück
6. Durch Logfileanalyse
7. Durch das IDS (Intrusion Detection System) oder SIEM (Security Incident and Event Monitoring)

Herausforderungen bei der Logfileanalyse

- Unterschiedliche IT-Infrastruktur (Anwendungen, Hardware).
- Anwendungen loggen unterschiedlich oder auch gar nicht.
- Gigantische Datenmenge, manuelle Sichtung unmöglich.
- Zentrales Logmanagement notwendig.
- Schwierige Entscheidung: Erfolgreich oder nicht?
- Probleme aktueller Analyseprodukte
  - False Positives
  - Ohne gezielte und sehr aufwendige (Personalkosten!) Konfiguration weitgehend sinnlos.

Logfileanalyse: Post Mortem

- Angriff bereits bemerkt
- Relativ „einfach“, weil man weiß wonach man suchen muss.
- Ausreichend Zeit vorhanden, da ohnehin zu spät.
- Dennoch wichtig: Lessons Learned

Logfileanalyse: Incident Response

- Herausforderungen:
  - Den Angriff bemerken.
  - Die Erfolgschancen korrekt einschätzen.
  - Die Auswirkungen korrekt einschätzen.
  - Eine sinnvolle Gegenmaßnahme treffen.
- Problem: Zeit ist knapp und 24/7-Überwachung kostenintensiv.

Typisches Logfile: sshd

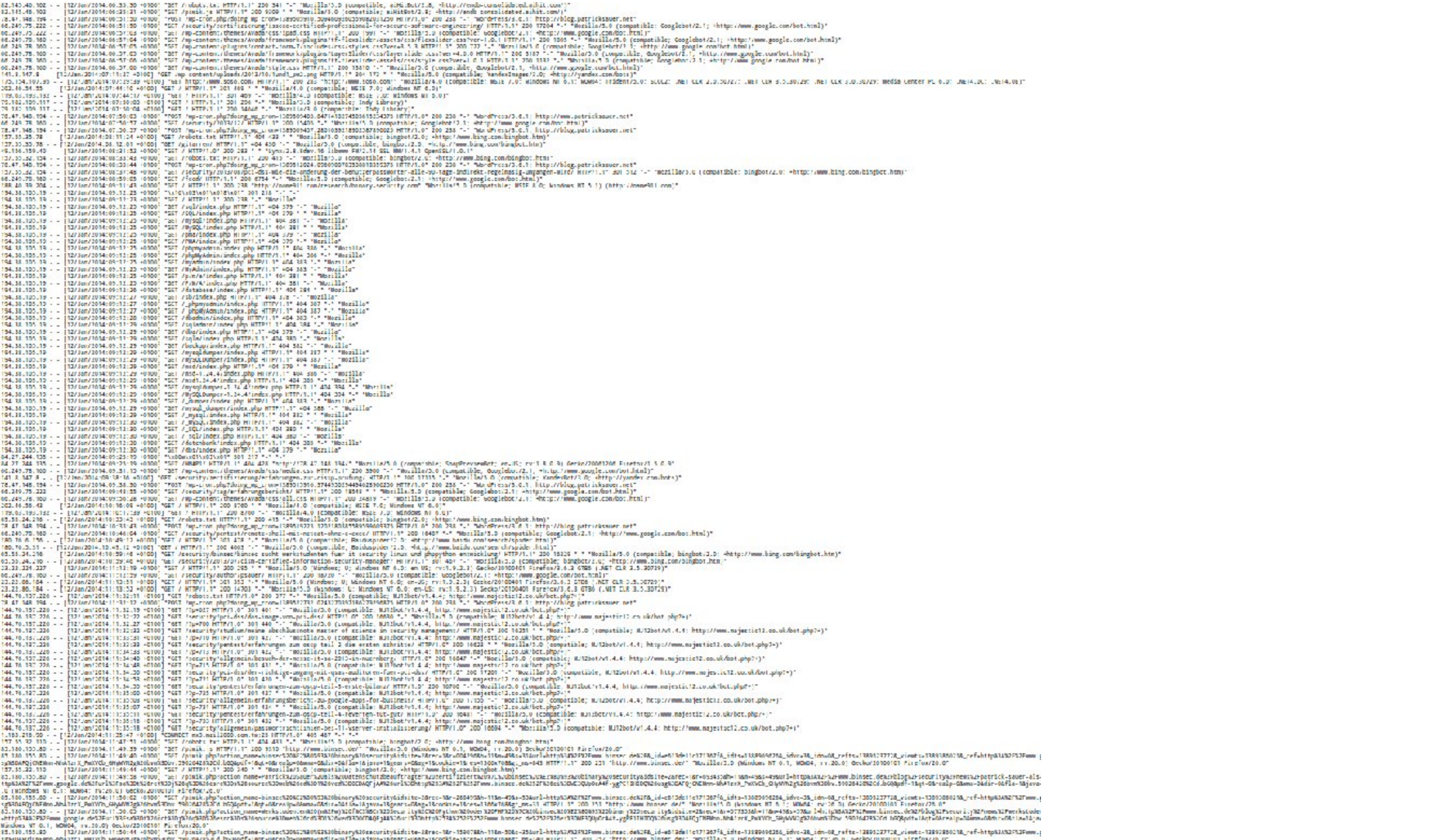
```
sshd[29021]: reverse mapping checking getaddrinfo for ip197.hichina.com [121.197.8.22] failed - POSSIBLE BREAK-IN ATTEMPT
sshd[29021]: Invalid user user from 121.197.8.22
sshd[29021]: pam_unix(sshd:auth): check pass; user unknown
sshd[29021]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=121.197.8.22
sshd[29021]: Failed password for invalid user user from 121.197.8.22 port 58415 ssh2
sshd[29023]: reverse mapping checking getaddrinfo for ip197.hichina.com [121.197.8.22] failed - POSSIBLE BREAK-IN ATTEMPT
sshd[29023]: Invalid user user from 121.197.8.22
sshd[29023]: pam_unix(sshd:auth): check pass; user unknown
sshd[29023]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=121.197.8.22
sshd[29023]: Failed password for invalid user user from 121.197.8.22 port 58576 ssh2
sshd[29025]: reverse mapping checking getaddrinfo for ip197.hichina.com [121.197.8.22] failed - POSSIBLE BREAK-IN ATTEMPT
sshd[29025]: Invalid user user from 121.197.8.22
sshd[29025]: pam_unix(sshd:auth): check pass; user unknown
sshd[29025]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=121.197.8.22
sshd[29025]: Failed password for invalid user user from 121.197.8.22 port 58726 ssh2
```

Bewertung:

- Angriff erfolgreich: ja/nein
- Falls nicht, kann er erfolgreich werden: ja/nein
- Ist der Angriff relevant: ja/nein
- Gegenmaßnahmen ergreifen: ja/nein

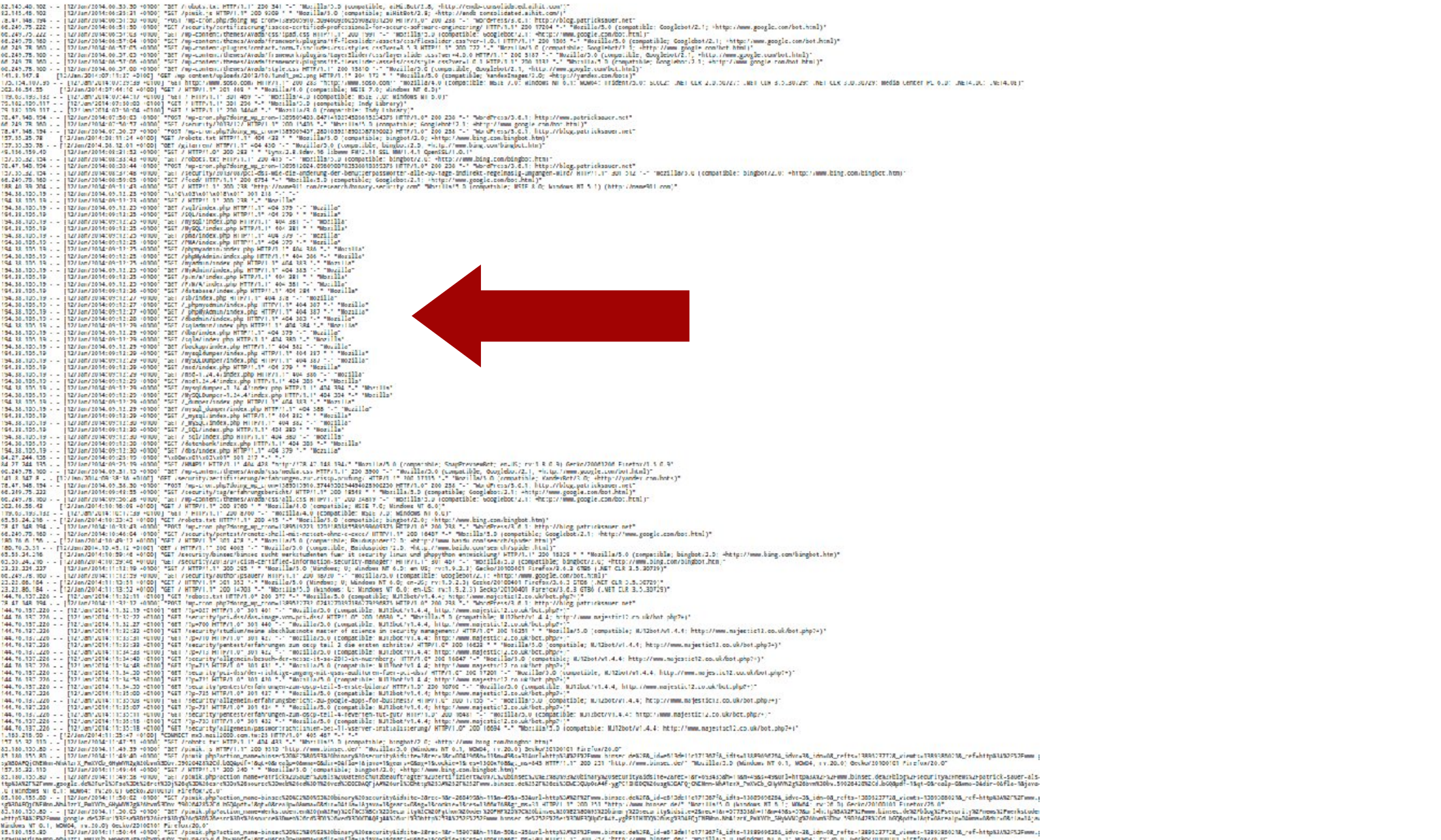
Typisches Logfile: apache2

- Was fällt auf?



Typisches Logfile: apache2

- Was fällt auf?



Typisches Logfile: apache2 (Vergrößerung)

```
194.38.105.19 - - [12/Jan/2014:09:12:23 +0100] "\x16\x03\x01\x018\x01" 501 218 "-" "-"
194.38.105.19 - - [12/Jan/2014:09:12:23 +0100] "GET / HTTP/1.1" 200 238 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:25 +0100] "GET /sql/index.php HTTP/1.1" 404 379 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:25 +0100] "GET /SQL/index.php HTTP/1.1" 404 379 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:25 +0100] "GET /mysql/index.php HTTP/1.1" 404 381 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:25 +0100] "GET /MySQL/index.php HTTP/1.1" 404 381 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:25 +0100] "GET /pma/index.php HTTP/1.1" 404 379 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:25 +0100] "GET /PMA/index.php HTTP/1.1" 404 379 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:25 +0100] "GET /phpmyadmin/index.php HTTP/1.1" 404 386 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:25 +0100] "GET /phpMyAdmin/index.php HTTP/1.1" 404 386 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:25 +0100] "GET /myadmin/index.php HTTP/1.1" 404 383 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:25 +0100] "GET /MyAdmin/index.php HTTP/1.1" 404 383 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:25 +0100] "GET /p/m/a/index.php HTTP/1.1" 404 381 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:25 +0100] "GET /P/M/A/index.php HTTP/1.1" 404 381 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:26 +0100] "GET /database/index.php HTTP/1.1" 404 384 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:27 +0100] "GET /sb/index.php HTTP/1.1" 404 378 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:27 +0100] "GET /_phpmyadmin/index.php HTTP/1.1" 404 387 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:27 +0100] "GET /_phpMyAdmin/index.php HTTP/1.1" 404 387 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:28 +0100] "GET /dbadmin/index.php HTTP/1.1" 404 383 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:29 +0100] "GET /sqladmin/index.php HTTP/1.1" 404 384 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:29 +0100] "GET /dba/index.php HTTP/1.1" 404 379 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:29 +0100] "GET /sqla/index.php HTTP/1.1" 404 380 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:29 +0100] "GET /backup/index.php HTTP/1.1" 404 382 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:29 +0100] "GET /mysqldumper/index.php HTTP/1.1" 404 387 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:29 +0100] "GET /MySQLDumper/index.php HTTP/1.1" 404 387 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:29 +0100] "GET /msd/index.php HTTP/1.1" 404 379 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:29 +0100] "GET /msd-1.24.4/index.php HTTP/1.1" 404 386 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:29 +0100] "GET /msd1.24.4/index.php HTTP/1.1" 404 385 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:29 +0100] "GET /mysqldumper-1.24.4/index.php HTTP/1.1" 404 394 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:29 +0100] "GET /MySQLDumper-1.24.4/index.php HTTP/1.1" 404 394 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:29 +0100] "GET /_dumper/index.php HTTP/1.1" 404 383 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:29 +0100] "GET /mysql_dumper/index.php HTTP/1.1" 404 388 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:29 +0100] "GET /_mysql/index.php HTTP/1.1" 404 382 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:30 +0100] "GET /_MySQL/index.php HTTP/1.1" 404 382 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:30 +0100] "GET /_SQL/index.php HTTP/1.1" 404 380 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:30 +0100] "GET /_sql/index.php HTTP/1.1" 404 380 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:30 +0100] "GET /datenbank/index.php HTTP/1.1" 404 385 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:30 +0100] "GET /dbs/index.php HTTP/1.1" 404 379 "-" "Mozilla"
84.27.244.135 - - [12/Jan/2014:09:25:19 +0100] "\x80w\x01\x03\x01" 501 217 "-" "-"
```

Typisches Logfile: apache2 (Bewertung)

```
194.38.105.19 - - [12/Jan/2014:09:12:23 +0100] "\x16\x03\x01\x018\x01" 501 218 "-" "-"
194.38.105.19 - - [12/Jan/2014:09:12:23 +0100] "GET / HTTP/1.1" 200 238 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:25 +0100] "GET /sql/index.php HTTP/1.1" 404 379 "-" "Mozilla"
194.38.105.19 - - [12/Jan/2014:09:12:25 +0100] "GET /SQL/index.php HTTP/1.1" 404 379 "-" "Mozilla"
```

Bewertung:

- Angriff erfolgreich: ja/nein
- Falls nicht, kann er erfolgreich werden: ja/nein
- Ist der Angriff relevant: ja/nein
- Gegenmaßnahmen ergreifen: ja/nein

Typiches Logfile: vsftpd (konstruiert)

```
Fri Jan 10 04:56:58 2014 [pid 4698] CONNECT: Client "192.168.1.110"
Fri Jan 10 05:16:58 2014 [pid 4845] CONNECT: Client "192.168.1.110"
Fri Jan 10 05:17:02 2014 [pid 4844] [root] FAIL LOGIN: Client "192.168.1.110"
Fri Jan 10 05:17:09 2014 [pid 4860] CONNECT: Client "192.168.1.110"
Fri Jan 10 05:17:15 2014 [pid 4859] [ftp] OK LOGIN: Client "192.168.1.110", anon password "?"
Fri Jan 10 05:18:34 2014 [pid 4861] [ftp] FAIL UPLOAD: Client "192.168.1.110", "/test", 0.00Kbyte/sec
Fri Jan 10 05:18:46 2014 [pid 4866] CONNECT: Client "192.168.1.110"
Fri Jan 10 05:18:49 2014 [pid 4865] [ftp] OK LOGIN: Client "192.168.1.110", anon password "?"
Fri Jan 10 05:18:51 2014 [pid 4867] [ftp] FAIL UPLOAD: Client "192.168.1.110", "/test", 0.00Kbyte/sec
Fri Jan 10 07:32:09 2014 [pid 8791] CONNECT: Client "192.168.1.110"
Fri Jan 10 09:18:37 2014 [pid 9897] CONNECT: Client "192.168.1.110"
Fri Jan 10 09:18:40 2014 [pid 9896] [user] OK LOGIN: Client "192.168.1.110"
Fri Jan 10 09:19:53 2014 [pid 9904] CONNECT: Client "192.168.1.110"
Fri Jan 10 09:19:53 2014 [pid 9903] [ftp] OK LOGIN: Client "192.168.1.110", anon password "klog"
```

Bewertung:

- Angriff erfolgreich: ja/nein
- Falls nicht, kann er erfolgreich werden: ja/nein
- Ist der Angriff relevant: ja/nein
- Gegenmaßnahmen ergreifen: ja/nein

Wie erkennt man Angriffe in Logfiles:

- Optisch auffällig:
  - Kürzere Logeinträge, längere Logeinträge
  - Wiederholungen
  - Ungewöhnliche Muster
- Nach Fehlermeldungen suchen.
- Schlagwörter:
  - BREAK-IN
  - ERROR, FAILED und danach SUCCESS
- Wichtig:
  - Kontext
  - Die Infrastruktur kennen

Fazit

- Enorme Datenmenge erschwert manuelle Sichtung
- Die manuelle Analyse ist schwierig
- Keine IT-Infrastruktur gleicht der anderen, Logs auch nicht
- Manche Angriffe erscheinen optisch auffällig in den Logs

Danke,

Fragen.... ? ? ?