SLAC Secure Linux Administration Conference 2018
08.-09 Mai 2018 | Berlin

LINUX HOST FORENSIC mit OSS LINUX TOOLS

Erstellt mit:

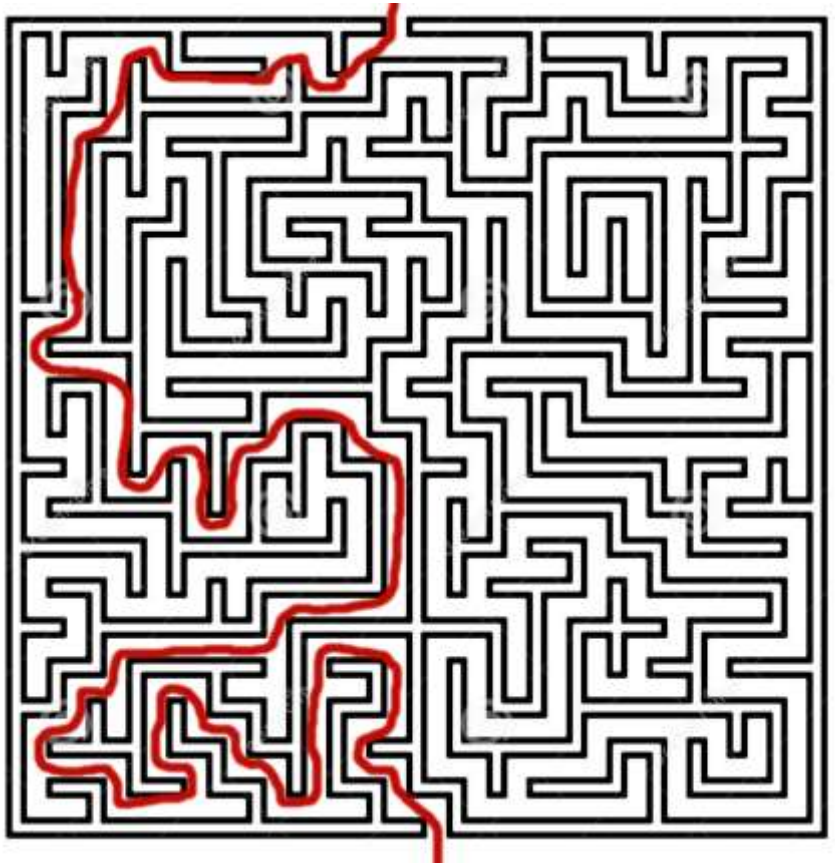
- LibreOffice
- GIMP
- Xmind
- Wikipedia

Erstellt von:
Fabian Paganotto
Jean-Claude Kiener
Michael Semling

Faden – Rot auf rot

1) Einleitung

- Vorstellung
- Was ist Forensik
- Feinde der Forensik und Gegenmassnahmen
- Entrypoints
- Linux Tools



2) Theorie

- Administrative Arbeit
- Logische Planung
- Physische Vorbereitung

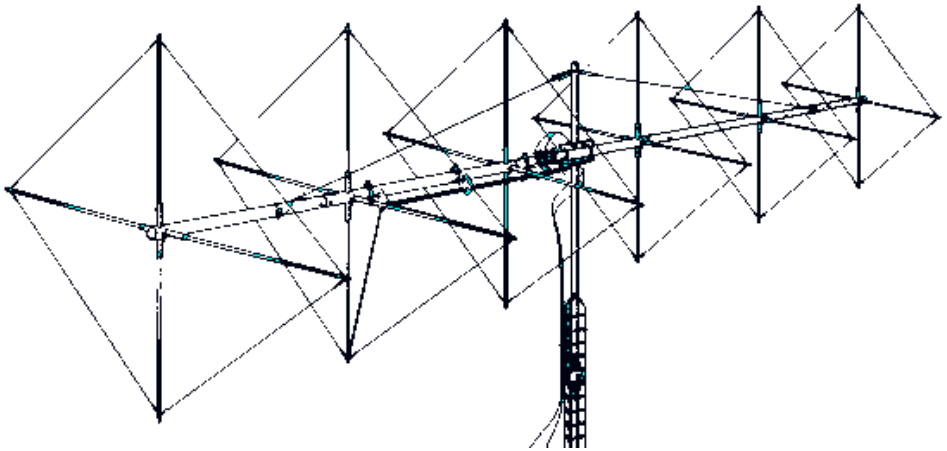
3) Praxis

- Übungsmaterial
- Üben, Beüben

Einleitung - Vorstellung Michael Semling

Dipl. El.-Ing. ETH, Spezialisierung in ADIT & HFMWE

Hobby: Segelfliegen, Funken, Makrophotos, TechDiving,……



Credo: Mache etwas falsch und lerne aus dieser Erfahrung. Mache es erneut falsch, lerne aus diesem Fehler.
Mache nie mehr als einen Fehler.

Einleitung - Vorstellung Fabian Paganotto

Dipl. Ing. Inf FH, Spezialisierung Forensik und Audit

Hobby: ja

Credo: Mache die Welt jeden Tag etwas sicherer.

Einleitung - Vorstellung JC Kiener

Dipl. Ing. Inf FH, Spezialisierung IT Forensic, Incident Response

Hobby: Motorrad, Kochen, Longboard, ...

Credo: Auch mit den Steinen, die Dir in den Weg gelegt werden, kann man was schönes bauen.

Einleitung – Was ist FORENSIK?

IT-Forensik ist das methodische, Identifizieren, Extrahieren, Sicherstellen, Analysieren, Dokumentieren, Interpretieren der Hauptursache eines Computervorfalles.

Computer als Tatmittel. (Hacker)

Computer als Tatopfer. (Incident)

Hinweise suchen, wiederherstellen, Veränderungen vermeiden oder exakt protokollieren.

Einleitung – Was ist Forensik

Reaktion auf einen Vorfall (POST

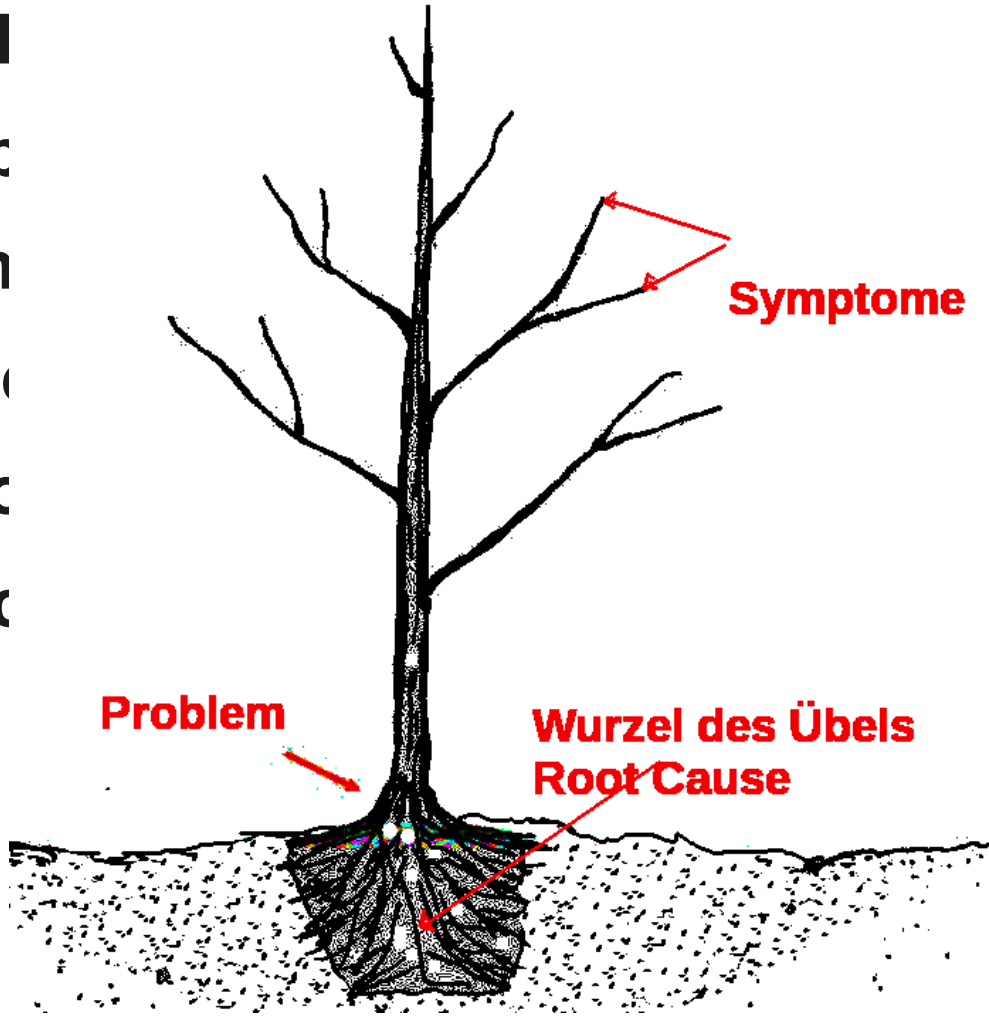
Der Versuch eine Erklärung herb

Beweise für eine Unschuld / Sch

Feststellen was geschehen ist / (

(Noch immer) vorhandene Bedrc

Entlastung eigener Verantwortlic



Einleitung – Was ist Host Forensik

Nachvollzug Ablaufs anhand der Spuren (auf einem Computer)

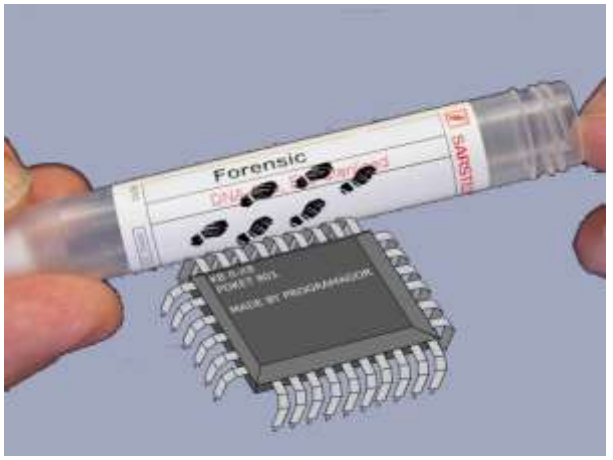
Indizien sammeln und Auswerten

Verknüpfen von relevanten Informationen

Verwerfen der irrelevanten Informationen

Eine Möglichkeit als plausibelste festlegen

Verteidigen der Theorie



Einleitung – FORENSIK!

Forensiker sind beharrliche Spürhunde auf der Jagd. Voller Adrenalin, immer wieder auf der Fährte. Auf der Suche nach

.Wer	war fähig, anwesend, beteiligt, involviert, informiert
.Wann	wurde der Vorfall verursacht (Datum/Zeit(Zeitzone))
.Was	ist geschehen, gegen welche Massnahmen
.Wie	wurde vorgegangen und welche Tools verwendet
.Warum	war es möglich, wurde es gemacht
.Welche	Absicht wurde verfolgt
.Wo	ist es passiert (Land, Ort, Gebäude, Raum, Rechner, Pfad, Datei)
.Womit	wurde operiert (APT / 0Day / CVE / Insider Know-How?)
.Wem	hat es gedient und wem geschadet
.Weshalb	wurde Alarmiert und wer wurde Informiert.

CHECKLISTE

Einleitung – Dokumentieren

Beweismittelglaubwürdigkeit

- Integrität
- Unveränderlichkeit
- Nachprüfbarkeit / Wiederholbarkeit
- Woher kommen die Informationen
- Wie und wer hat sie gesammelt
- Wer war der Eigentümer
- Wie waren die Informationen geschützt
- Wer hatte Zugriff und wie, wann……

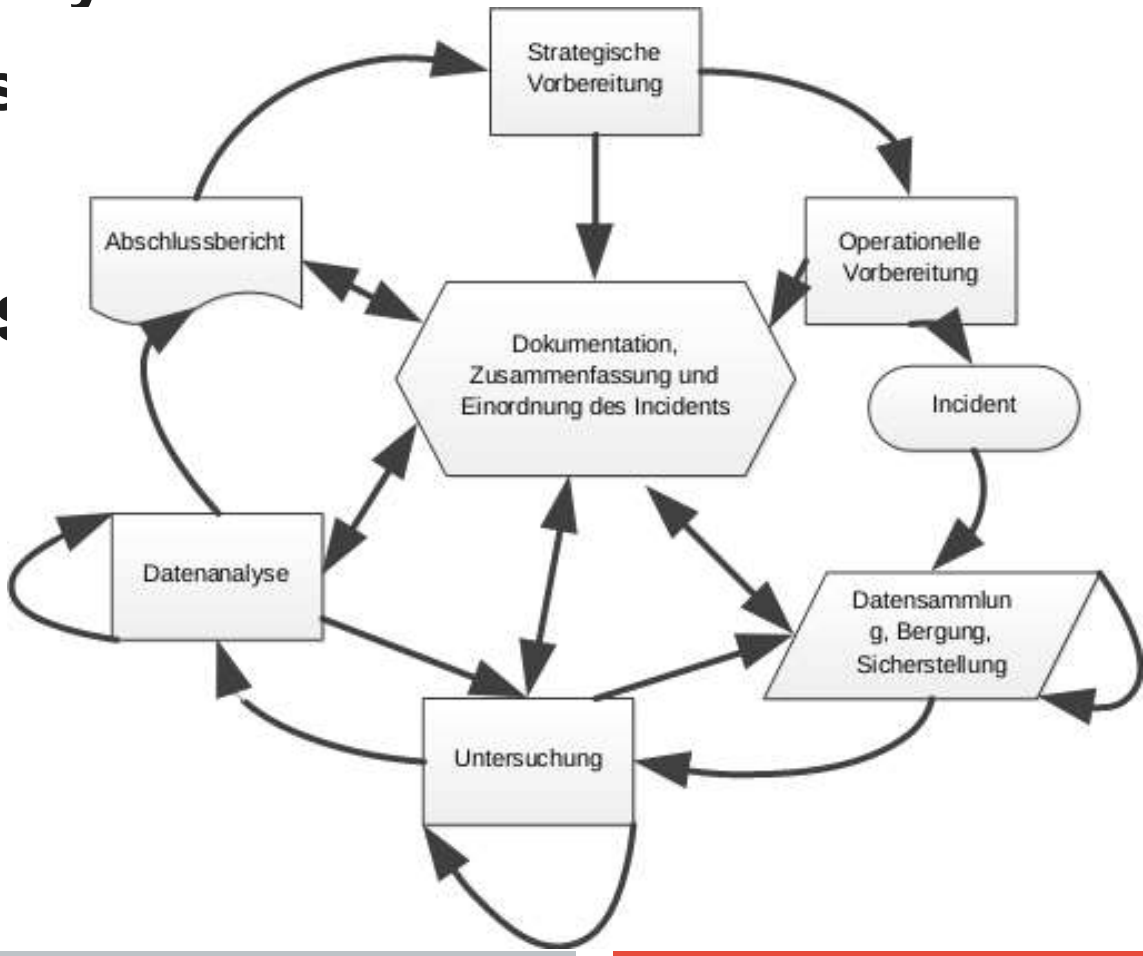
CFReDS
„Standard“ (Encase)
Protokollieren
Glaubwürdig Dokumentieren

Einleitung - IT Forensik

FNA – Forensic Network Analysis

FDA – Forensic Data Analys

FHA – Forensic Host Analysis



Einleitung - Gegner der Forensik und Gegenmassnahmen

Zeit und Ressourcenmangel

- Eingabefristen
- Termine
- Ferien
- Andere Projekte (Priorisierungen)
- >1 Forensische Analyse
- ...

Vorschriften → Vorher mit Anwalt abklären

- Bundesdatenschutzgesetz (DE)
- Landesdatenschutzgesetz (DE)
- Datenschutzgesetz des Bundes (CH)
- Datenschutzgesetz 2000 (A)
- Data Protection Act (GB)
- General Data Protection Regulation GDPR (EU)
- Strafrecht
- Policies / Guidelines / Freigaben
- Ethische und moralische Richtlinien
- Verhaltensrichtlinien
- ...

Einleitung - Gegner der Forensik und Gegenmassnahmen

Datenmengen → GByte→TByte→PByte

Filesysteme → Extx, BTRFS, ZFS, XFS, FFS, LVM, DM

Technik → Hardware-Raid, TPM

Fileformate → Komprimiert, Binär, BLOBs, Proprietär

Verschlüsselung → BIOS, TrueCrypt, LUKS, Steganografie

Kompression → ZIP, XZ, LZMA, 7Z, LHA, ARJ, ARC, COMP, Brotli, Deflate, Zopfli, BZIP2,……

Antiforensische Techniken: Timestomp, Decoy, encoding

Einleitung - Gegner der Forensik und Gegenmassnahmen

Bullshit und Mythen beeinflusst die Beteiligten

- Bullshit: H. G. Frankfurt→ Weitergabe von unreflektiertem und nicht überprüften Informationen zusammen mit dem Glauben der absoluten Wahrheit.
- Mythos: Absoluter Wahrheitsanspruch ohne logische korrekte Nachvollziehbarkeit oder Widerlegbarkeit.
- Dogmen: Unfehlbare und einzig richtige Aussage einer göttlichen Instanz.

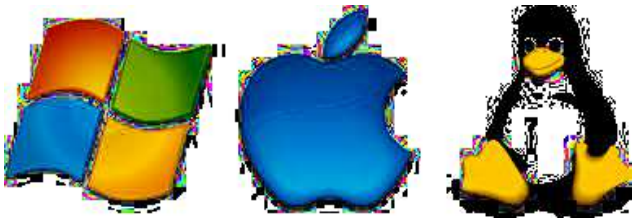
Nachvollziehbar verifizieren. Informationsquellen nennen.

>=4 Augen Prinzip.

Einleitung - Gegner der Forensik und Gegenmassnahmen

Diversifizierung Betriebssysteme

- Linux
- Windows(7,8,8.1,10)
- Mac
- Solaris
- HP Unix
- Open/Free/…. BSD
- Android
- IOS
- IoT



Vorbereitung pro Betriebssystem
Toolbox pro Betriebssystem
Spezialist pro Betriebssystem

Einleitung - Gegner der Forensik und Gegenmassnahmen

Vielfalt

- Little Endian/Big Endian
- UTF8/16/32
- Matroschkas
- Doc(x), Od[t|p|s|d], XML-Styles
- Herstellerformate/Tools
- Bios / Uefi / ilo / Firmware
- Virtualisierung
- Clouds

Ausbildung
Üben
Trainieren
Verifizieren

Einleitung - Gegner der Forensik und Gegenmassnahmen

Mensch

- Angst (Fehler gemacht zu haben)
- Verärgert
- Unfall
- Gleichgültigkeit
- Angestiftet
- Überlistet

Technik

- Shares
- Clouds
- P2P
- VPN
- TOR
- Updates
- Smart devices
- Apps/Programme

Übliche Tools
Spezialsoftware
Experten

Entrypoints - Administrative Einstiegspunkte

Welche System → Host Admin

- Gesetze, Verordnungen
- Wer hatte Zugriff auf Daten
- Wann wurde durch wen Zugriff genehmigt
- Policies
- Requirements
- Spezifikationen
- Owner (HW, System, DB, Prozess,….)
- Service MAP, Network Map, Physical Map, Port Matrix etc.

Entrypoints - Physikalische Einstiegspunkte

- HW
  - Kreditkarte
  - Ausweise
- Kameras
- GPS info
- Spuren von Gewaltanwendung
- Fingerabdrücke
- Genetische Abdrücke
- Fussabdrücke

- NAS / DISKS / USB-wasauchimmer
- Ethernet / MAC layer
- Router, Switches
- NAC
- Zutritt
  - Schlüssel
  - PINs
  - Batches
  - X-Faktor Auth

Entrypoints - Logische Einstiegspunkte

Welche System → Host Admin

- Device
  - Mobile/Laptop/Desktop
  - Server
  - VM
  - Cloud
- OS
- MRU
- User(s)
- Erster Zeitpunkt
- Backups/Archive / Baselines???

Welche Zone → Netzwerk Admin

- Proxies
- AD/LDAP
- Zentrale AV
- Zentrale HIDS
- Zentrale LOG / SIEM
- WLAN, NAC, Cert. Server
- NIDS
- Moloch

Vor- und Nachteile Linux Tools

PRO

- Meist Gebührenfrei
- Meist Open Source
- Flexibel
- Adaptierbar
- Bei richtiger Anwendung sogar Gerichtsverwertbar

CONTRA

- Kein (tech) Support
- Weiterentwicklung?
- „as-is“ buggy
- Featureitis
- Toolvielfalt - welches wofür?
- Abhängigkeiten zu anderen Werkzeugen.
- Verschiedene Look & Feel
- Gefahr einer Fehlmanipulation

Unterstützen der Entwickler Feedback und Monetär, Testen, Trainieren, Gegenüberstellen, Programmieren

Tools – Linux Tools

Vorschlag Einsatz Linux Tools für Workshop

Jeder sein Werkzeugkasten, seine Tools

Scalpel, testdisk&photorec

bash, perl, c/c++

find, awk, sed, cut, ls, host, dd ,……..

! Image benötigt ca. 5-10 fach Platz für alles!

Linux Tools Download

Linux Forensic Tools

autopsy	SUITE	http://www.sleuthkit.org/autopsy/
Encrypted Disk Detector	Detect Encrypted Containe	https://www.magnetforensics.com/free-tool-encrypted-disk-detector/
ExifTool	Perl Lib	http://www.sno.phy.queensu.ca/~phil/exiftool/
SANS Cheatsheets	Lazy Memory	https://digital-forensics.sans.org/community/downloads/#overview
SIFT	SUITE	http://computer-forensics.sans.org/community/downloads
Dumpzilla	Firefox Data Extractor	http://www.dumpzilla.org/
PALADIN	SUITE	https://sumuri.com/software/paladin/
The Sleuth Kit	SUITE	http://www.sleuthkit.org/sleuthkit/
CAINE	SUITE	https://www.caine-live.net/
Volatility	Framework	https://www.volatilesystems.com/default/volatility
FTK Imager		http://www.accessdata.com/support/product-downloads
DEFT		http://www.deftlinux.net/download/
Xplico	NFAT	http://www.xplico.org/download
Foremost	Grabber	http://foremost.sourceforge.net/
KALI	SUITE	https://www.kali.org/downloads/
MARTIUX	SUITE	http://www.matriux.com/index.php?page=download
TCT	Collection	http://www.porcupine.org/forensics/tct.html
Trapkit	Collection	http://www.trapkit.de/tools/index.html
ExifTool	Tool	https://www.sno.phy.queensu.ca/~phil/exiftool/
plaso	Tool	https://github.com/log2timeline/plaso
systemrescuecd	BootMedia	http://www.system-rescue-cd.org/
photorec	Tool	https://www.cgsecurity.org/wiki/TestDisk_Download
testdisk	Tool	https://www.cgsecurity.org/wiki/TestDisk_Download
TriD	Tool	http://mark0.net/soft-trid-e.html
BulkExtractor	Tool	https://github.com/simsong/bulk_extractor
CFReDS	NIST-Collection	https://www.cfreds.nist.gov/

Theorie

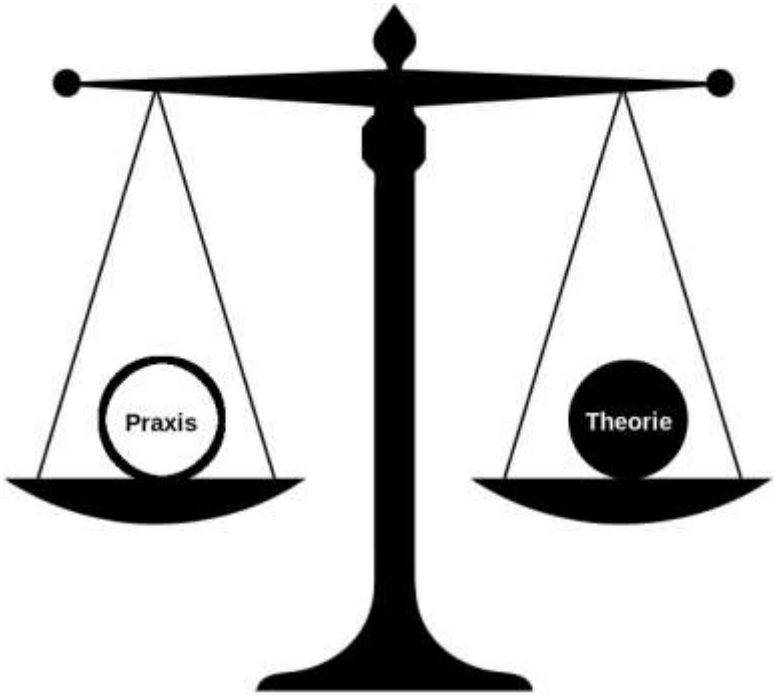
THEORIE

.Trocken

.Langweilig

.Weiss man schon lange

.Kann man besser

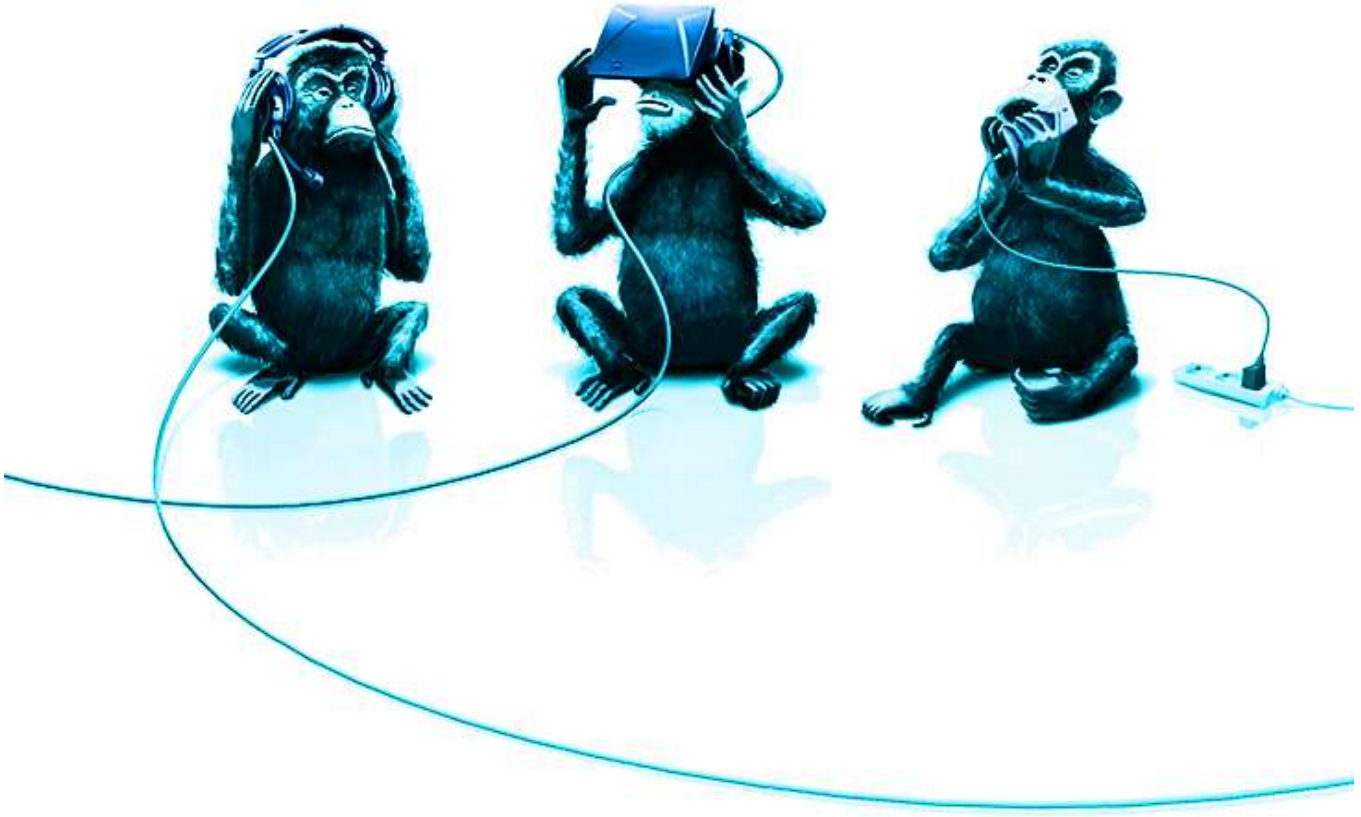


Theorie - Arbeiten

TEAM

Kommunikation

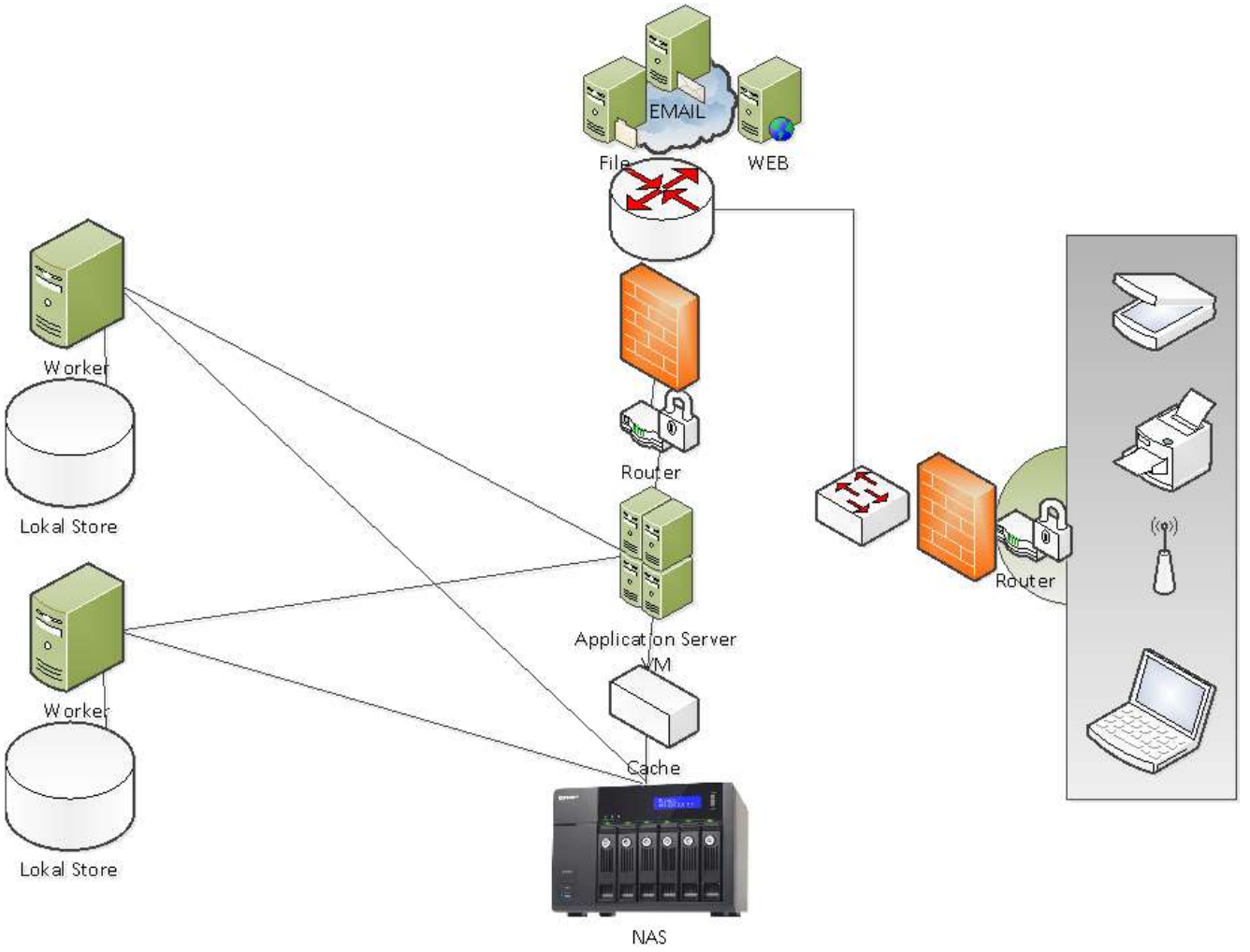
Infrastruktur



Theorie – Arbeiten Verteilte Forensik

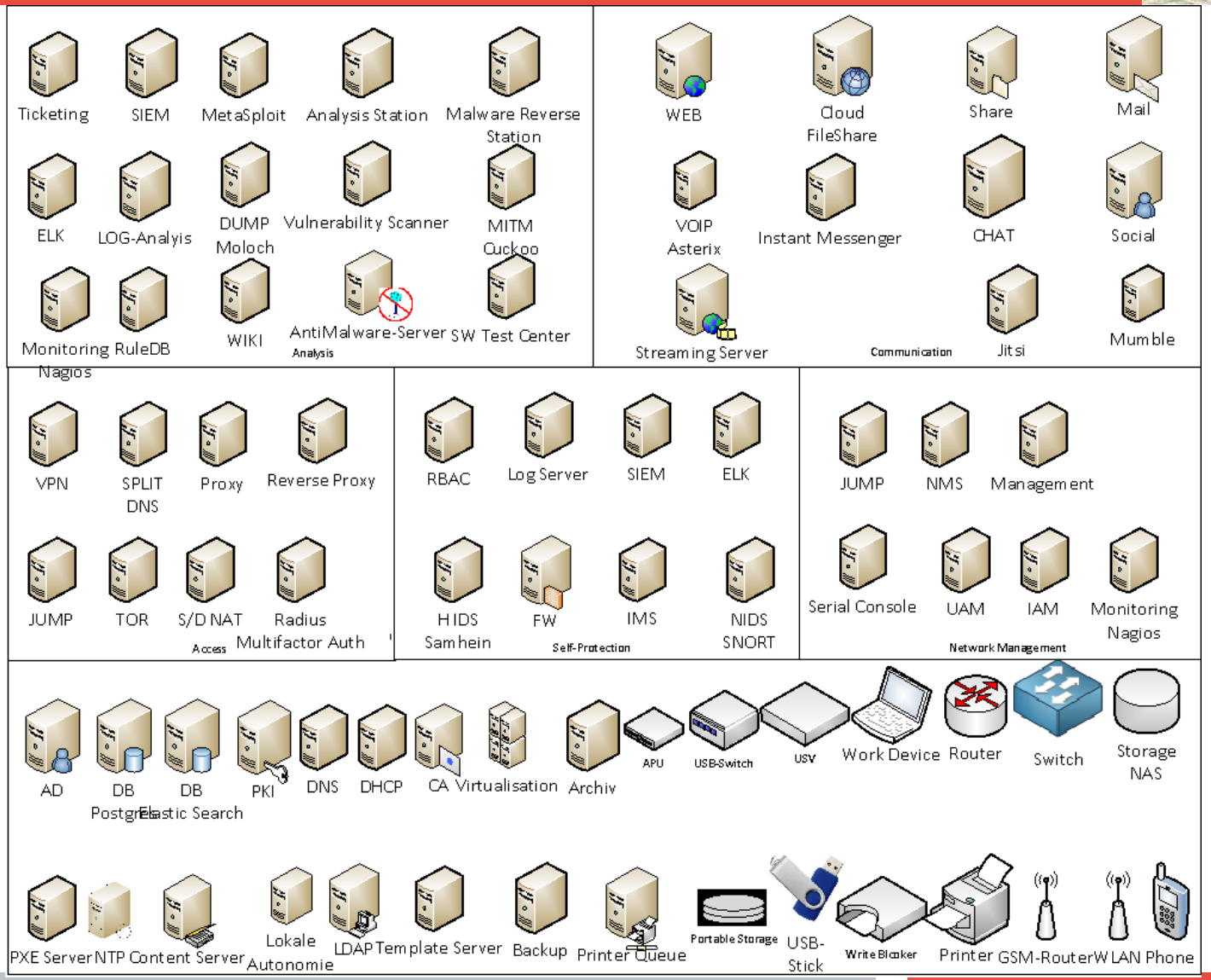
Infrastruktur

- 4-Augen-Prinzip
- Diversifikation (andere Programme)
- Parallele Prozesse (unabhängig)



Theorie – Arbeiten Verteilte Forensik VMs

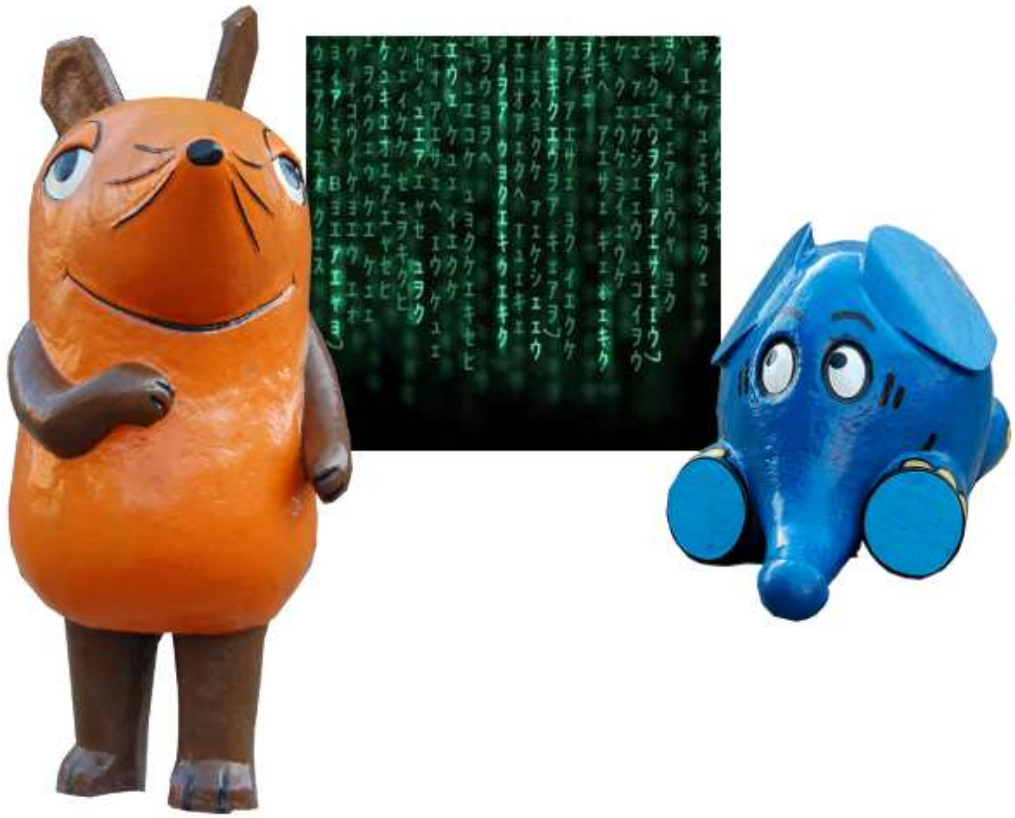
Infrastruktur



Einleitung – Wie funktioniert Forensik

Schritte

1. Vorbereitung
2. Ereignis
3. Identifizierung
4. Datensicherung
5. Informationsanalyse
6. Aufbereitung
7. Präsentation



Vorbereitung Räumlichkeiten

War-Room

Sicherer Aufbewahrungsraum, abschliessbar

Schlüssel, Schliessplan, Badges

Zutrittserlaubnis, Wochenendzutrittserlaubnis

Bei sich / beim Kunden!!!!

Tempest-sicherer Analyseraum

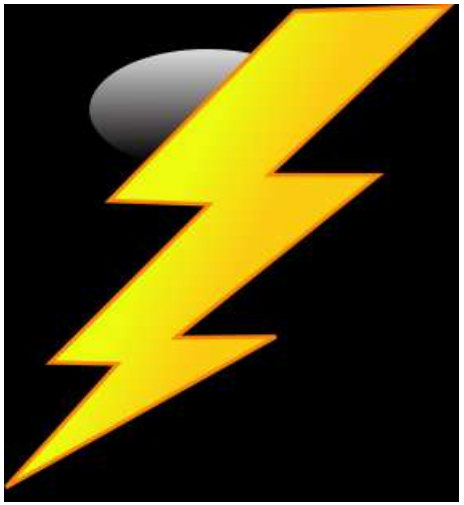
Leitungsführungspläne

Badgereaderlogs

Schlosslogs → Ausleseleute, ext. Firmen

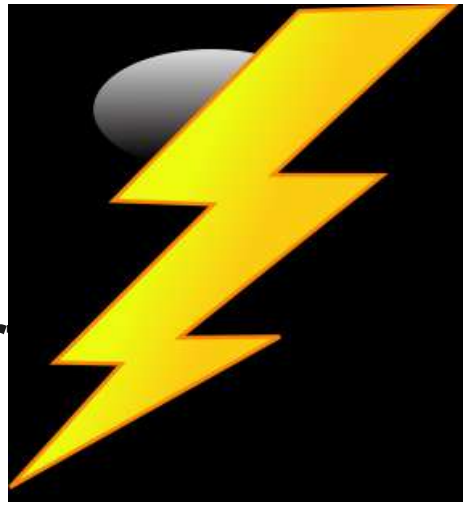
Vorbereitung Beweissicherungsmaterial

- Einweghandschuhe
- Malereinwegkombi (auch wegen Staub)
- Plastiksäcke / Gefrierbeutel
- Klebe-/ Schnur-Etiketten
- Plomben
- Wasserfester Filzstift
- Isolierband/Malerband
- Plastikboxen
- Abschliessbare Behältnisse
- Transportkoffer!!!!!

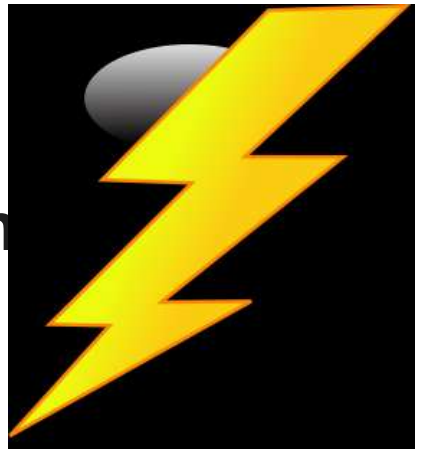


Vorbereitung Beweiserfassungsmaterial

- Write-Blocker
- Imager
- NAS
- Rechenpower/Server
- Netzwerk-Switch (8port, 1GB, Monitor Por
- Wire/Fiber TAP
- USB-Hub (aktiv)
- USB-Disk
- USB-Stick
- Laptop(s) (>3)



Vorbereitung Werkzeug



- Lockpick-Set (für Racks)
- Multifunktionstool
- Schraubenzieher, Allzweckschalen
- Kamera
- Diktiergerät / Aufnahmegerät
- GPS
- Bleistift, Kugelschreiber, Schreibblock (Laborblo
- Tablet / Handy
  (mit Threema, Signal, Wire,→Diktiergerät, Kamera,GPS)
- Powerbank

Vorbereitung Versorgungswerkzeug

Taschenlampe - Licht

Stromadapter

Mehrfachsteckerleiste

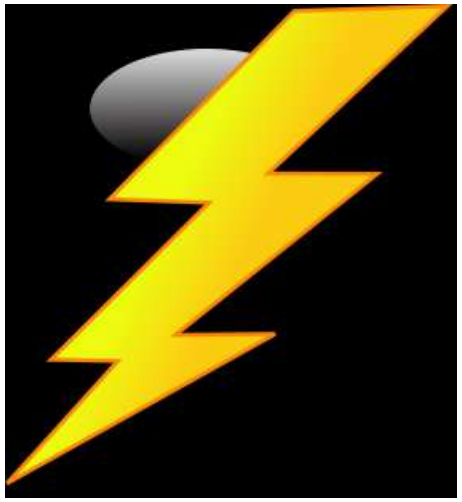
Verlängerungskabel

USV - Portable

USB-[Serial|DVI|VGA|SATA…]

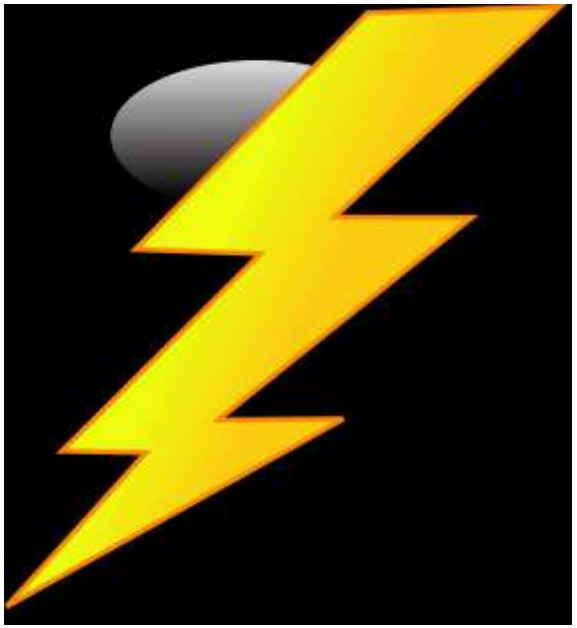
Ethernetkabel

SFP(+) - Module, Multimode/Monomode, Fibre-Cable



Vorbereitung Privacy Material

- Packpapier
- Packetklebeband
- Malerklebeband
- Isolierband
- Leim/Sekundenleim
- Kabelbinder
- Schrumpfschlauch
- Feuerzeug
- Bargeld (Notfallkasse)



Vorbereitung
Persönliches Material

Kleidung, Ersatzwäsche, Schuhe

Nahrung, Getränk, Snacks (Zigaretten für Rauch

Notfallmedikamentenset

- Zahnbürste, Zahnpasta, Zahnseide, Zahnpu
- Hygiene (Seife, Duschmittel, Deo)
- Mediamente
  - Allergie
  - Durchfall
  - Kopfschmerz
  - Sodbrennen

Vorbereitung Logische

Letzte Version von Malware Detection

Letzte – getestete – Version der Analystools

Clean Equipment

Verschlüsselte Container für dieses Projekt

Baselines

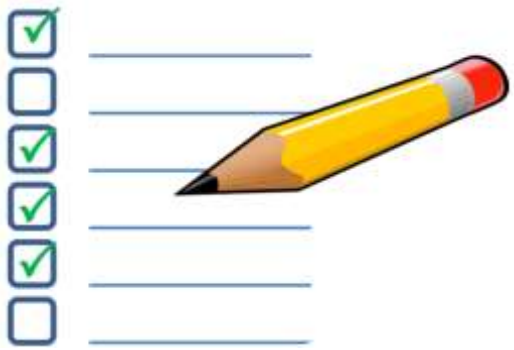
Kontaktlisten mit Tel, Mail

Zugriffserlaubnis (Wer, Was, Wann, wie lang, wofür)

Passworte auf Default (NAS, Administrator, ...)

Vorbereitung Logische

CheatSheets/Checklists/Cookbooks



- GPG
- RSYNC
- SSH
- NMAP
- JUMP-HOST (VPN)
- BASH-CMD
- GDB
- EMACS

Vorbereitung AKV

Vorbereitung

- Ausbildung / Weiterbildung / Community → Budget
- Toolbox & Training → Zeit
- Verantwortlichkeiten (Template)
- Geheimhaltungsvertrag (Template)
- GAG (Gehe aus Gefängnis) (Template)
- Pressemitteilung
- Informationsfluss (Need to know) → Wer liefert, wer bekommt
- Abos (Malware-Signaturen)
- Kronjuwelen, Risikobewertung, Priorisierung

Vorbereitung AKV

Einsatz

- SPOC, PL Team Forensik
- SPOC, PL Team Firma/Abteilung
- Zutritt
- Verantwortlichkeiten (TL/PL/Prozess/Comm)
- Informationfluss (Need to know)
- Geldfluss (Wer zahlt, wieviel, welche Leistungen)
- Erlaubnis global
- Erlaubnis für einzelne Aktivitäten (pro Gerät)

Vorbereitung AKV

Nachbearbeitung (Lessons learned)

- Material an Ort aufgeräumt, gereinigt
- Schlüssel vernichtet
- VMs von Template neu gemacht
- Daten entfernt, gelöscht
- Neue Tools für neu gefundene Probleme
- Community

CIP (Clean-in-place)!!!

Entlastung einfordern

Scope & Permission

-Ziele und Zielsysteme

-Festplatten, Dumps, Memory

-Netzwerke, IPs, Protokolle

-Entlastung aus der GL

-Entlastung von Legal

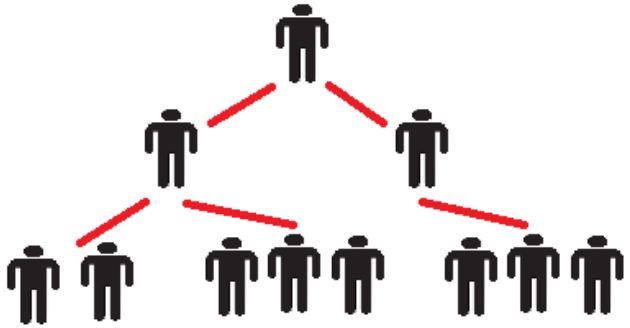
-ev Entlastung vom Betroffenen

KEINE ARBEIT OHNE ERLAUBNIS

Entlastung einfordern

Step 1 Einfrieren und Änderungen protokollieren

BCM / CISO definieren



- Weiterbetrieb
- Netzwerk blocken
- Ausschalten
- Weitere Massnahmen (bezahlen, AV,...)
- Root-Cause-Analysis durch forensische Analyse

Sichern des «Tatorts»

-Polizei beiziehen? - im Zweifel JA!

-Rechner Sicherstellen

→Flüchtige Informationen sichern

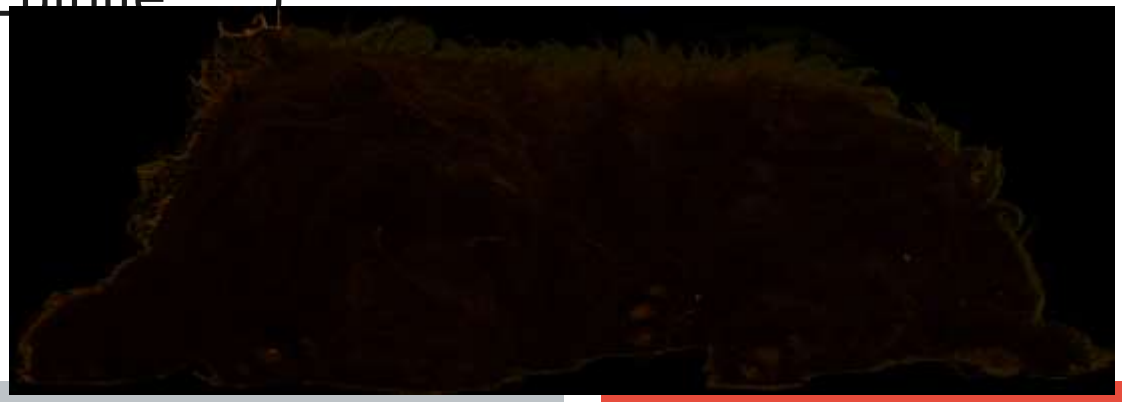
→Image erstellen

-Rechner duplizieren (schlafende Hunde nicht weck

-Wiretaps installieren → Dumps vom Netzwerk erstellen

-Logs sichern (System, Netzwerk, Zutritte)

-Kameraaufnahmen sichern



Einleitung – Vorgang Daten sicherstellen

HDD/SSD

Immer erst Raw-Image erstellen

Immer mit Image-Copy arbeiten

Informationen / Hashes vor und nach der Analyse

Write-Blocker

Fotos

Zeitpunkte

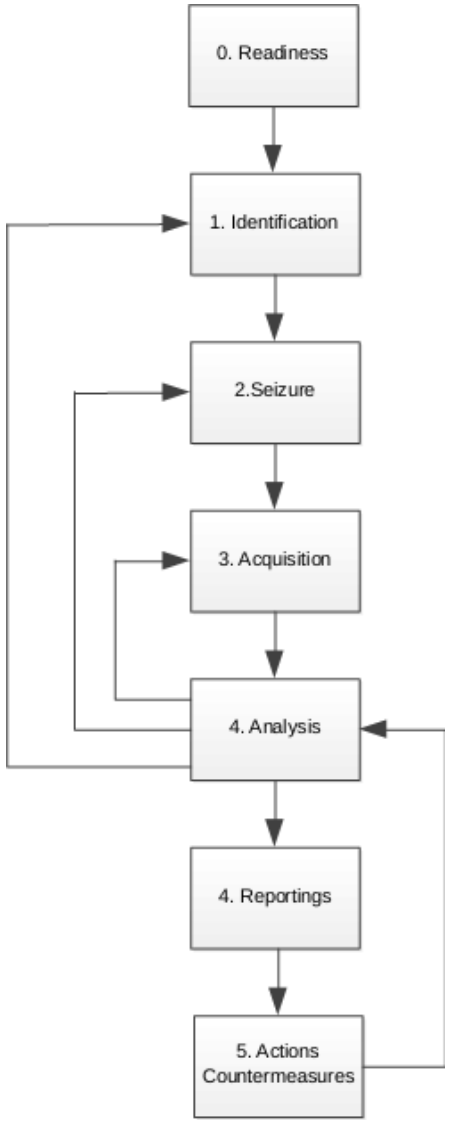
Plastikbeutel / Anschreiben

Lagern: geeignet, trocken (Silica), kühl,

Beweissichtung und Untersuchung

- Triage
- Analyse der Diskimages
- Analyse der Netzwerkdumps
- Analyse der Logs
- (Analyse der Kameraaufnahmen)
- Korrelation der gefundenen Artefakte
- Korrelation mit externen Informationen
- Herleiten des Vorganges

Beweiserbringung

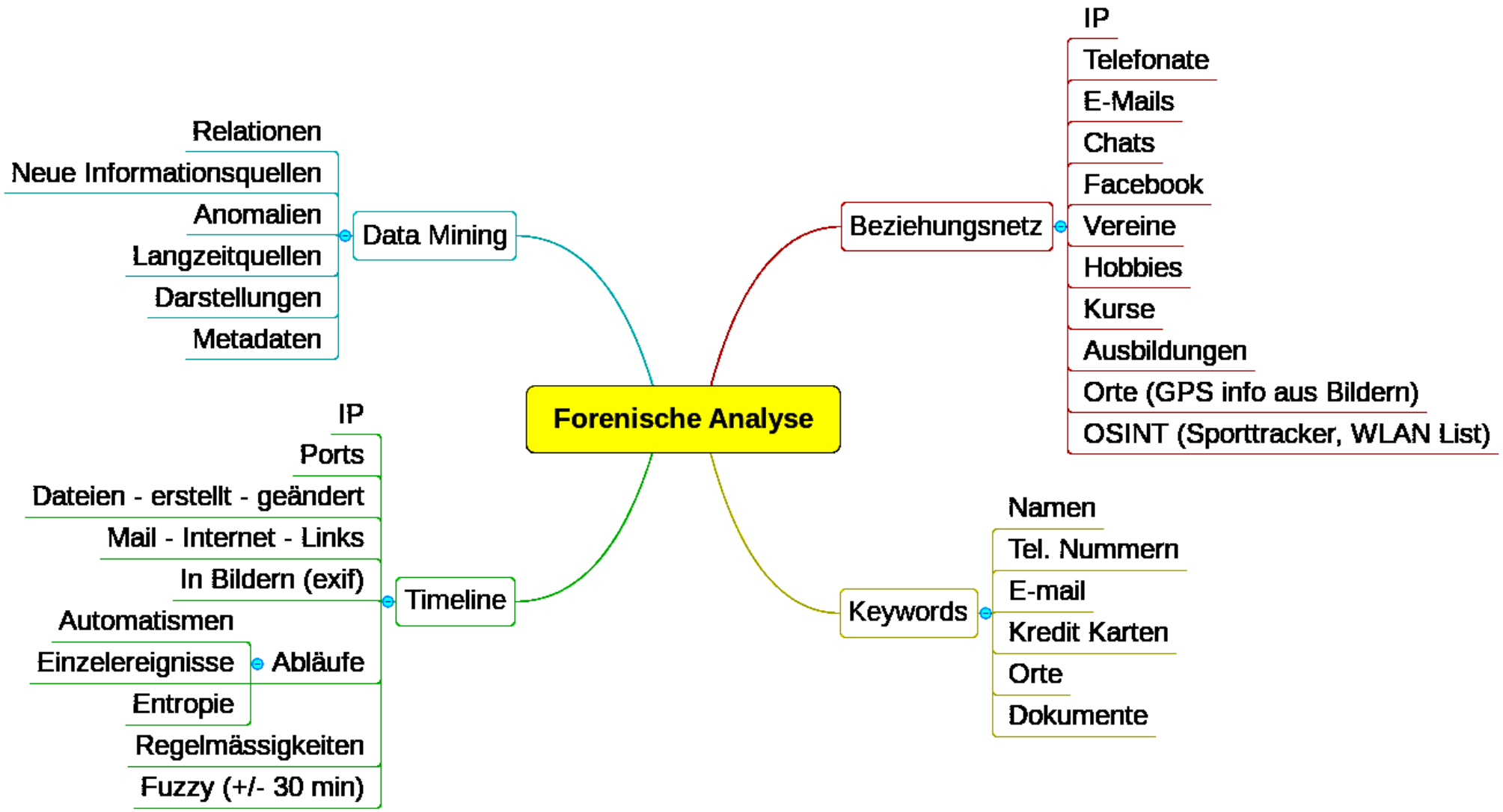


Verifikation/Falsifikation gegen die Artefakte

(Gegebenenfalls zurück zur Untersuchung)

Lückenlose Darstellung

Fadenanfang finden - Korrelation



Verteidigung

Management Zusammenfassung

Detailliertere Beschreibung

Ausschluss oder Wahrscheinlichkeit begründen

Herleitung und Schluss


Praxis
Theorie

Flüchtige Informationen

Step 2 Eigene CD / USB mit 32bit/64bit(LE/BE) des betroffenen Systems mounten.

DATE=`date "+%F-%H%M%S"`

Mkdir -p /tmp/${DATE}_ToolBox

Mkdir -p /tmp/${DATE}_DataSink

Mount -o nodev,**ro** /dev/sdx /tmp/${DATE}_ToolBox

Mount -o noexec,nodev */dev/*sdy /tmp/${DATE}_DataSink

! Möglicherweise AUTOMOUNT !

Flüchtige Informationen

Step 2 Data ins DataSink

date

who

ps -ef

ifconfig -a

netstat -nutlp

rsync -av

./etc/hos

./etc/fsta

./var/log/

./var/log/

./tmp/*

[redacted]

cfldd

roc/kcore

roc/kallsyms

roc/interrupts

ev/mem

dev/sdx

SHUTDOWN

Nicht so flüchtige Informationen

Step 3 Abbild mit Writeblocker erzeugen und HASH

Booten mittels External Boot Media (e.g. SystemRescueCD)

Oder Disk ausbauen und physikalischen Writeblocker verwenden

Mounten lokal oder Netzwerk Speicher


```
dcfldd if=/dev/sdx hash=md5,sha256 hashwindow=1G \
md5log=md5.txt sha256log=sha256.txt hashconv=after \
bs=512 conv=noerror,sync split=1G splitformat=aa \
of=/mnt/usbdisk/20140314_sda_laptop1.dd hashlog=dcfldd.log
```

Vorbereitung - BASH

BASH

Bash für Forensic

- Keine History von aktiven Sessions
- Order ist shell exit NICHT execution (^D, exit, logout, SIGTERM, SIGHUP, SIGKILL, shutdown, reboot) sonst nicht
- Alte Bash History Blocks sind NICHT überschrieben
- Timestamps: export HISTTIMEFORMAT='%F %T '
- Prompt: export PS1="[\$(date +%F-%T) \u@\h \W]\\$ "
- Am besten in */etc/*bashrc als default

Vorbereitung - BASH

Step 4 Analyse Prep

BASHRC

- HISTFILESIZE=
- HISTSIZE=
- Remove HISTCONTROL=ignoreboth:erasedups o.ä.
- Shopt histappend

TOOLS updaten, für System beschaffen (FS, CPU….)

EXPERTEN ZUZIEHEN – keine Schande!

Vorbereitung - BASH

Antiforensic – Mittel des Feindes

- Export HISTFILE=/dev/null
- Export HISTFILESIZE=0 / -1
- Export HISTSIZE=0 / -1
- Add in .bashrc alias date=“ssh -C 123.213.132.111“

Linux Vorbereitung

Step 5 Analyse

- Informationen über/von Systemen
- Wann wurde es wahrgenommen
- Wie wurde es wahrgenommen
- Was wurde unternommen
- Wer hat es gemacht

Linux Vorbereitung

Informationen über/von Systemen

- Dein Name, ID, Erreichbarkeit
- FallNummer – Ein-Ein-Deutige Identifikation
- Datum, Zeit
- Serielle Nummer, PartNo, Bios-No
- Unter ID für ein Beweissstück e.g. HDD1_<UUID>→ HDPARM
- Was mit der HD gemacht wurde – z.B. Aufbewahrungsort

Tiefer suchen

Step 5.1 Analyse – gelöschte Daten

Scalpel, testdisk&photorec

Scalpel /dev/sdx1 -o /mnt/forensic_xxx/scalpel/

Inverse Analysis: Leere Plattenbereiche
→ Entropieanalyse

→ Gelöschte Partitionen / Container

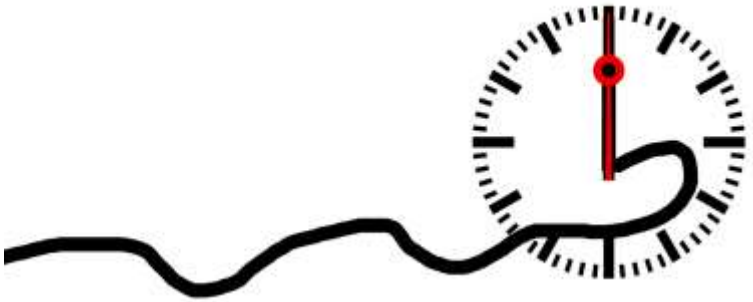
Wo suchen

Step 5.2 Files of Interest

System	User
Logins	Recent Files
Syslog	Browser Files
Last	Cmd history
Leases	Data, Document
	Email

Zeit-Zusammenhänge (FS, Last, Syslog,Mail)

Step 5.3 Timeline



Mactime

Supertimeline (plaso – log2timeline)

log2timeline -p -r -f linux -z GMT /mnt/windows_mount -w timeline.csv --partition all

„Traditionelle Timeline“

fls -m / -a -r /*dev*/vg0/part1 | mactime -b - > timeline

FileSystem Evidence

Step 5.3 Timeline

Nach Waisen (Orphaned), gelöschten (deleted) reallocated, mac (modified, added, changed) Dateien suchen

Oder

Nach der Zeit/Datum vor/nach dem Bekanntwerden und sukzessiv verlängern.

Step 5.4 keywordsearch

DMRAID / LVM / Mount (kpartx)

Mount with offset → Blocksize 512, startsector vom fdisk -l

mount -o loop,ro,offset=$((${BlockSize} * ${StartSect},sizelimit=$(($BlockSize)) * ${EndSect} */ImageDir/Image /mnt/mountpoint*

Kpartx

Create : # kpartx -v -ar logging-test.img

Remove: # kpartx -v -d logging-test.img

Div. Dateitypen

Step 5.4 keywordsearch

file/TriD

```
find ${src_path}  -type f -executable -exec ls  {} \; >> ${dst_path}/Files_exe.txt 2>&1
find ${src_path} -iname "*.wav" -type f -exec ls {} \; >> ${dst_path}/Files_wav.txt 2>&1
find ${src_path} -iname "*.vol" -type f -exec ls {} \; >> ${dst_path}/Files_vol.txt 2>&1
find ${src_path} -iname "*.log" -type f -exec ls {} \; >> ${dst_path}/Files_log.txt 2>&1
find ${src_path} -iname "*.dmp" -type f -exec ls {} \; >> ${dst_path}/Files_dmp.txt 2>&1
find ${src_path} -iname "*.jpg" -type f -exec ls {} \; >> ${dst_path}/Files_jpg.txt 2>&1
find ${src_path} -iname "*.mov" -type f -exec ls {} \; >> ${dst_path}/Files_mov.txt 2>&1
find ${src_path} -iname "*.mpg" -type f -exec ls {} \; >> ${dst_path}/Files_mpg.txt 2>&1
find ${src_path} -iname "*.mp4" -type f -exec ls {} \; >> ${dst_path}/Files_mp4.txt 2>&1
find ${src_path} -iname "*.doc*" -type f -exec ls {} \; >> ${dst_path}/Files_doc.txt 2>&1
find ${src_path} -iname "*.xls*" -type f -exec ls {} \; >> ${dst_path}/Files_xls.txt 2>&1
find ${src_path} -iname "*.ppt*" -type f -exec ls {} \; >> ${dst_path}/Files_ppt.txt 2>&1
find ${src_path} -iname "*.ost*" -type f -exec ls {} \; >> ${dst_path}/Files_ost.txt 2>&1
find ${src_path} -iname "*.pst*" -type f -exec ls {} \; >> ${dst_path}/Files_pst.txt 2>&1
find ${src_path} -iname "*.txt*" -type f -exec ls {} \; >> ${dst_path}/Files_txt.txt 2>&1
find ${src_path} -iname "*.odp*" -type f -exec ls {} \; >> ${dst_path}/Files_txt.txt 2>&1
find ${src_path} -iname "*.ods*" -type f -exec ls {} \; >> ${dst_path}/Files_txt.txt 2>&1
find ${src_path} -iname "*.odt*" -type f -exec ls {} \; >> ${dst_path}/Files_txt.txt 2>&1
```

Und zum Schluss * und grep -v von wav, vol, log, dmp, jpg, mov …… → Besenstaub……

Data of Interest

Step 5.4 keywordsearch

file/TriD

Strings

ASCII: # strings –t d file_to_analyse > <case><src><date>.str

Unicode: # strings –t d –e l file_to_analyse > <case><src><date>.str

Grep: → erstellen kleiner Scripte (gute Vorbereitung)

z.B. Email: grep -E '(^|[[:space:]])[[:alnum:]]{1,}@[[:alnum:]]{2,}\.[[:alpha:]]{2,6}([[:space:]]|$)' <filename>

grep -rE '[E|e]v?l' <filename>

grep -l 'file with matches' <filename>

Viren und Trojaner

Step 5.4 keyword search

DMRAID / LVM / Mount (kpartx)

Strings

file/TriD

src_path=$1; dst_path=$2

clamscan -z -o -r ${src_path}/* -l ${dst_path}/clamscanOutputDisk.txt --detect-pua=yes --detect-broken=yes >> ${dst_path}/clamscanOutputScreen.txt 2>&1 &

savscan -ns -b -c -f -archive -rec -all -sc -oe -suspicious -mime ${src_path}/ -p=${dst_path}/sophosOutputDisk.txt 2>&1 ${dst_path}/sophosOutputScreen.txt &

Rkhunter: rkhunter –update && rkhunter –propupd
rkhunter –check --skip-keypress
cat /var/log/rkhunter.log

Chkrootkit: /usr/sbin/chkrootkit 2>&1 >> ${DATE}_chkrootkit.txt

Anomalien

Step 5.5 Anomalien

Bash

Top10neueste files

find . -type f -printf '%T@ %Tc %P\n' | sort -rn | head -n 10 | sed -r 's/^.{22}//'

Top10älteste files

find . -type f -printf '%T@ %Tc %P\n' | sort -n | head -n 10 | sed -r 's/^.{22}//'

Top10grösste

find . -printf '%s %p\n'| sort -nr | head -10

SUID/SGUID-Files

find . -perm /u=s,g=s -exec ls -la {} \; (=find . -perm /6000 -exec ls -la {} \;)

Anomalien

Step 5.5 Anomalien

Hidden Dirs und …

#find . -type d -iname „*.*“ -print

Good reading at SANS.ORG
e.g. https://www.giac.org/paper/gsec/3133/introduction-hiding-finding-data-linux/105105

Interessante Quellen

Quellen

- Flüchtiger Speicher/ Permenenter Speicher
- Logs – lokal
- Logs - Server
- Caches - Proxies
- Zeit
- Prozesse
- Data

Interessante Quellen

Quellen

- Memory, Swap
- OS, Installed, Uptime, Release
- Timezone, Timeglitches
- User Profile
- SYSLOG
- Lastlog
- Internet History
- Email
- USB History, Cloud Access
- Network / WLAN History

Scoreboard:

https://mellivora.paganotto.ch

Das selbstsignierte Zertifikat aktzeptieren, Email / PW eingeben

ZEIT: Bis 12:15h

CHEATSHEETS / Gedächtnissstütze / Gedankliche Hilfsmittel / Fauler Knecht

Forensik Linux Gedankliche Hilfsmittel

Einhängepunkt	Beschreibung des Inhalts	Beschreibung des Grundes
/bin		
/boot	Initramfs, kernel, uefi	Grundlegend zu vertrauen
/dev	Geräte	Muss mit System übereinstimmen
/etc	Konfigurationsdateien	
/home	User Verzeichnisse	Achtung lokale Ausführung
/lib	Bibliotheken	Modifikationen BIN-LIB?
/media	externe Medien (USB,..)	
/mnt	externe/Netzwerk Mountpoints	Kommunikation / Exfiltration
/opt	3-Hersteller Binaries	
/root	Systemadministrator	The Boss
/sbin	System Binaries	
/tmp	temporäre Dateien/pipes	
/var/lib	Dynamische Daten, Datenbank info	
/var/log	Log Daten von System, Services, Programmen	

INFO:http://tldp.org/LDP/Linux-Filesystem-Hierarchy/html/Linux-Filesystem-Hierarchy.html

Forensik Linux Gedankliche Hilfsmittel

date

Zeigen/Setzen von Zeit/Datum
Konvertiere Epoche-Sek (1970-01-01 UTC)
in akt Datum $ date --date='@2147483647'
$ date +Format
%F volles Datum; dasselbe wie %Y-%m-%d
%H Stunde (00..23)
%I Stunde (01..12)
%j Tag des Jahres (001..366)
%m Monat (01..12)
%M Minute (00..59)
%N Nanosekunden (000000000..999999999)
%p AM oder PM in der Lokale; leer sonst
%r Zeit im 12-Stunden-Format (z. B. 03:11:30)
%R Zeit im 24-Stunden-Format; wie %H:%M
%s Sekunden seit „1970-01-01 00:00:00 UTC“
%S Sekunde (00..60)
%T Zeit; dasselbe wie %H:%M:%S
%u Tag der Woche (1..7); 1 steht für Montag
%Y Jahr
%:::z num Zeitzone mit Zahl „:“ (z. B. +01)
%Z alpha Zeitzone (z. B. CET)

grep/egrep

Durchsucht text

-A n n Zeilen nach Treffer anzeigen
-B n n Zeilen vor Treffer anzeigen
-c Anzahl Treffer
-f Muster aus Datei
-i Groß- und Kleinschrift ignorieren
-l Dateinamen ausgeben
-o nur den Treffer zeigen
-P Pattern als Perl Regex
-v verkehrt
(zeigt Zeilen ohne Match an)

Grep -E ‚found|detect‘ file
Grep -E ‚found.*working| detect.*operating‘

file

Identifiziert Dateien anhang MagicKey
-m zeigt die Schlüssel
-z versucht komprimierte Dateien zu betrachten
-f Liste der Dateien aus der Datei
-i mime-Type und -Kodierung
-k weitersuchen
-l Vertrauenswürdigkeit

less

-L ignore env
-S lange Linien ab-schneiden
-x 55 tab stops setzen
/ vorwärts suchen
? rückwärts suchen
ESC-n weitersuchen

Forensik Linux Gedankliche Hilfsmittel

hostname

Host Name des aktuellen Systems
Hostname
IP Adresse des aktuellen Systems
hostname -i

dig

DNS IP
dig a domain-name [+short] @nameserver [A|AAA]
NS
dig NS domain-name @nameserver
Canonical Name
dig CNAME domain-name @nameserver
MX Record
dig mx domain-name @nameserver
SOA Rec
Dig SOA domain-name @nameserver
Zone Transfer
dig axfr domain-name @nameserver
TTL
Dig TTL domain-name @nameserver
ALLES
Dig ANY +noall domain-name.@nameserver

whois

DNS enum
whois domain-name-here.com

host

DNS IP für akt. System
Host domain-name
SOA
HOST -C domain-name
Andere params mit -t
SOA, CNAME, NS, A, MX …
Ipv4 / IPv6
-4 / -6
Zone Transfer
Host -la domain-name

Passwort Generator

URANDOM
< /dev/urandom tr -dc _A-Z-a-z-0-9 | head -c6
SSL
openssl rand -base64 32

Forensik Linux Gedankliche Hilfsmittel

uniq

Identische Einträge aussortieren
-c Vorkommenszahl voranstellen
-d nur doppelte Zeile ausgeben
-f ersten N Felder überspringen
-i Gross/Kleinschrift ignorieren
-s N ersten N Zeichen ignorieren
-u nur einmal vorkommenden Zeilen ausgeben
-w N nicht mehr als N Zeichen vergleichen

strings

Zeigt druckbare Zeichen in Datei
-a alles durchsuchen
-d nur Datenbereich
-f Zeigt Dateinahmen an
-e {sS,bl,BL} s=7bit, S=8bit, endian
big/little 16 bit,
Big/Little 32 bit

find

-[i]name Name / ohne Gross/Kleinschrift
-maxdepth Tiefe für Dirs
-exec <> {} \; cmd ausführen ls -la {} \;
-not invertieren
-inum inondes suchen
-type [b(block) c(char) d(dir) f(file) p(pipe) l(link) s(socket)]
-executable ausführbare Dateien
-delete gelöschte
-uid <uid>
-perm -g=r,…. 040 → -4000 = SUID
-mtime <n> File letzte modif >=n*24h
-atime <n> File letzte access >=n*24h
-ctime <n> File letzte change >=n*24h
-regex <reg.exp> EX. ".*/\..*" \)
Ex.
find / -type f -exec ls -s {} \; | sort -n -r | head 5
find / -mtime -1 –
fine / -atime -1 –
Dateien mit referenz
#find -newer /etc/passd
#find -anewer /etc/hosts
#find -cnewer /etc/fstab
find . -type f -iname .mp* -exec mv„s/ /_/g“ {} \;
Tar alle Files mit Änderung heute
tar -cvzf ../files_created_today.tgz `find /path/to/search -type f -daystart -ctime -1`

cut

-b <xy> Byte x-y der Zeile
-c <xy> Char x-y der Zeile
-d <ch> Delimiter CH
-f <Feld> Nummer der Felder
--complement → NOT
Ex.
cut -d: -f1,2,7 passwd.bak

BASH

Uname -ai
Mount
Date
Uptime
Whoami
Man
Info
Pwd
Mkdir
Ls -lar[S|t]
Watch -n <x> <CMD>
Ps -efx
Top
Chowm
Chmod
Cat
more|less

Forensik Linux Gedankliche Hilfsmittel

sort

Sortieren
-b führende Leerzeichen ignorieren
-d Leer und alphanum beachten
-h menschenlesbar (2k)
-i ignoriere nicht druckbare Zeichen
-n numerische Sortierung
-r umgekehrte Sortierung
-u uniq

sed

sed ist ein Strom-Editor.
echo "hallo" | sed 's/a/e/'
Outputs: hello
For global substitution use:
echo "Hello elle" | sed 's/e/a/g'
Outputs: Hallo alle
In Dateien zu ersetzen -i flag
sed -i „ 's/e/a/g' file.txt

TCPDUMP

-i {eth0|any} Interface
-v[vv] verbose
-n[nn] numerisch
-w <file> schreiben
-r <file> lesen
-s 65535 packetgrösse
-X[X] ascii / hex out
-A ascii out
-e ethernet out

FILTER
-F Filterfile
Host <ip>
{ip|ip6|arp|rarp]
{src|dst}host <ip>
Port 22 [and|or ….]
Tcp, upd, icmp
Vlan <vlanid>
tcpdump -i eth0 -w wwwtraffic.pcap \
'host www.badmac.net and port 80'

SSH

FILTER
ssh -C forensicuseri@123.45.67.89 -p 12345 -L 24100:10.20.4.100:22
X-Connection (X or Y)
ssh -CY 127.0.0.1 -p 25100 -L 15900:127.0.0.1:5900 -L 15902:127.0.0.1:5902
ssh -C forensicuseri@123.45.67.89 -i <identity_File.priv>

Forensik Linux Gedankliche Hilfsmittel

awk

awk -F [Separator] [-v var=val] -f progfile [f1 f2…] Pattern {Action}
Für jedes file, jede input Linie, jedes pattern,
Trifft pattern zu, führe Action aus
"pattern"
BEGIN : Action vor Start der Inputanalyse (Titel)
END
: führt Action nach Ende der Inputanalyse aus (Schluss)
Other
: regular, numeric oder string (oder Kombination) lässt Action ausführen
if (expression) statement1 else statement2
while (expression) statement
for (expr1;expr2;expr3) statement
do statement while (expression)
break / continue : immediately leave / start next iteration
of innermost enclosing loop
exit / exit expression : go immediately to the END
action; if within the END action, exit program

Eingebaute Variablen
$0 ganze Linie
$1, $2 ... **$NF** erstes, zweites,… Feld
ARGC Anz. Cmd line Argument
ARGV Array der geg. Argumente
FILENAME Name des input file
FS, RS Field / record separator (def: one space, \n)
NF Anz. Felder in akt. Record
NR, FNR Anz. Gelesener Records
OFMT Nummer Output format (default: %.6g)
OFS, ORS Ausgabe Separator
(default: one space, \n)
RESTART, RLENGTH Start / Stringlänge für die match Funktion
SUBSEP Subscript separator (default: \034)

Eingebaute Funktionen
r: regex ; s,t: strings ; n,p: integers
int(n), sqrt(n), exp(n), log(n),
sin(n), cos(n)
Rand() Zufallszahl zw. 0 und1
Close (File oder command)
getline [var] Nächste Linie vom Eingabefile
getline [var] < file oder spez. file
command | getline [var] oder Pipe
Rückgabe 1 (record found), 0 (eof), -1 (error)
gsub(r,s) Global Ersetzen von s durch r in $0
gsub(r,s,t) mit Anz. Der Ersetzungen t
index(s,t) Erstes Auftreten von t in s oder 0
length(s) Anz. Char in s
match(s,r) existiert r in s -Pos oder 0
split(s,a) Teilt s in array a
split(s,a,fs) Feldsep fs, gibt Anz zurück
sprintf(fmt,expr-list) Rückgabe von expr-list gems dem Format fmt
sub(r,s) Ersetzt den ersten längsten s wenn r gefunden wird
sub(r,s,t) t = Anz. Ersetzungen
substr(s,p) Rückgabe vom Substr s (len n)
substr(s,p,n) Von Pos p an
tolower(s), toupper(s) Klein-/Gross-schrift

Operatoren
Logische
&& || ! UND, ODER, NOT
Ex: !($2<4 || $3<20)
Vergleich
< <= == != >= > grösser, grösser-gleich, gleich, ungleich, grösser-gleich, grösser
~ !~ Trifft (nicht) zu,
Bedingung
selector?if-true-exp:if-false-exp

Forensik Linux Gedankliche Hilfsmittel

awk

Beispielprogs

awk '{print NR, $0 }' x.txt Eine Zeilenummerrierung vornstellen
awk '{$1 = NR; print}' x.txt Erstes Feld durch eine Zeilennummer ersetzen
awk '{ $2 = log($2); $3 =”” ; print }‘ Ersetze 2 Feld durch seinen Log und entf. Feld 3
awk ' NF > 0' x.txt Keine leeren Zeilen ausgeben
awk ' NF > 0 {print $1, $NF}' x.txt Erstes und letztes Feld der nicht leeren Linien
awk ' NF > 4' x.txt Ausgeben wenn es mehr als 4 Felder hat
awk ' $NF > 4' x.txt Letztes Feld ausgeben, falls es mehr als 4 Felder hat
awk ' NR%2==0 ' x.txt Gerade Zeilen ausgeben
awk ' NR==10, NR==20 ' x.txt Zeile 10 bis 20 ausgeben
awk ' /regex/, EOF' x.txt Von Auftreten regex bis eof ausgeben
awk '/regex/ {print $1}‘ x.txt Erstes Feld der Zeile mit match
awk '{ if ($1 ~ /Die/) print $0 }' x.txt Nur Zeile mit match ausgeben
awk ' ORS=NR%5?",":"\n" ' x.txt immer 5 Zeilen zusammenfügen mit Komma als Trennz
awk ' /regex/ {x++} END {print x} ' x.txt Auftritt vor pattern zählen und ausgeben
awk '{ nc += length($0) + 1; nw += NF } END { print NR, "lines", nw, "words", nc,"characters" }' x.txt = wc x.txt
awk '{ sum += $1 } END { print sum, sum/NR }' x.txt Print sum and average
awk '{ x[NR] = $0 } END {for (i = NR; i > 0; i--) print x[i]} ' x.txt Datei Zeilenweise rückwärts
awk '{for (i=NF;i>0;i--) printf("%s ",$i)} {printf("%s","\n")}' x.txt Zeile Worte rückwärts
awk '{ for(i=length;i!=0;i--)x=x substr($0,i,1);}END{print x}' x.txt Zeile Worte und Buchstaben rückwärts
echo "10 2" | awk 'function pwr(a,b) { return exp(b*log(a)) } NF >= 2 { print pwr($1,$2) }' Funktionen !!!
awk ' BEGIN { RS=""; FS="\n" } { print "Name: ",$1 "Address: ",$2 } ' x.txt Multiline rec, entf. \n

Forensik Linux Gedankliche Hilfsmittel

dd und Verwandte

Backup / Restor

1Plug in the device to / from imaging
2. dmesg the dev e.g. /dev/sda is built in...
3. mount the device e.g. mount /dev/sdb1 /mnt
4. BACKUP disk -l /dev/sda > /mnt/sda_info.txt
dd if=/dev/sda conv=sync,noerror bs=64K | gzip -c > /mnt/BACKUP1.img.gz
5. RESTORE gunzip -c /mnt/sda.img.gz | dd of=/dev/sda conv=sync,noerror bs=64K

ddcfldd / ddrescue

```
dcfldd if=/dev/sda hash=md5,sha256 hashwindow=10G md5log=md5.txt sha256log=sha256.txt hashconv=after \ bs=512 conv=noerror,sync split=10G \
        splitformat=aa of=/mnt/usbdisk/20140314_sda_laptop1.dd hahslog=dcfldd.log
dcfldd if=/dev/sda vf=/mnt/usbdisk/20140314_sda_laptop1.dd verifylog=/media/disk/verifylog.txt
ddrescue -f -n /dev/sda /mnt/usbdisk/20140314_sda_laptop1.iso ddrescue.log
ddrescue -d -f -r5 /dev/sda /mnt/usbdisk/20140314_sda_laptop1WError.iso rescue.log
```

dd / gdd

```
dd if=/dev/sda1 of=/mnt/usbdisk/20140314_sda_laptop1.iso bs=4K conv=noerror,notrunc,sync status=progress

dd if=/dev/sda1 bs=4K conv=noerror,notrunc,sync status=progress | xz -c -T -9e | dd of=/mnt/usbdisk/20140314_sda_PC1.iso.xz

ssh forensicuser@123.45.67.89 "dd if=/dev/sda1 bs=4K conv=noerror,notrunc,sync" | xz -c -T -9e | dd of=/mnt/usbdisk/20140314_sda_laptop1.iso.xz status=progress

dd if=/dev/sda1 bs=4K conv=noerror,notrunc,sync status=progress | xz -c -T -9e |ssh forensicuser@123.45.67.89 "dd of=/mnt/usbdisk/20140314_sda_laptop1.iso.xz"
```

Forensik Linux Gedankliche Hilfsmittel

Virtual memory dd / gdd

dd if=/proc/kcore of=/mnt/usbdisk/20140314_kcore_laptop1.bin
dd if=/proc/kcore | hexdump -C | less
#loaded modules:
dd if=/proc/kallsyms of=/mnt/usbdisk/20140314_kallsyms_laptop1.bin
dd if=/proc/kallsyms | hexdump -C | less
#interrupt table:
dd if=/proc/interrupts of=/mnt/usbdisk/20140314_interrupts_laptop1.bin
dd if=/proc/interrupts | hexdump -C | less
 # uptime
dd if=/proc/uptime | hexdump -C | less
#Memory stats:
dd if=/proc/meminfo | hexdump -C | less
#ram memory to a file
dd if=/dev/mem of=/mnt/usbdisk/20140314_mem_laptop1.bin bs=1024
dd if=/dev/mem | hexdump -C | grep 'some-string-of-words-in-the-file-you-forgot-to-save-before-the-power-failed'

Forensik Linux Gedankliche Hilfsmittel

rsync

```
rsync -abv --stats --iconv=ISO-8859-15,UTF-8 --links --suffix="_20171112" --exclude="*~" /home/forensicuser/* /mnt/Archiv/BACKUP/forensicuser/

sshfs forensicuser@123.45.56.78 /mnt/nfs/ssh/tmp/
rsync -rltbv --suffix="_20170401" --exclude="*_201*" --exclude="*~" --exclude="*RECYCLE*" /home/forensicuser/* /mnt/nfs/ssh/tmp/forensicuser/

DATE=`date "+%F-%H%M%S"`
rsync -ncrltbv --suffix="_${MYDATE}" --exclude="*~" --exclude="*RECYCLE*" --progress /home/forensicuser/* /mnt/nfs/ssh/tmp/forensicuser/
```

Forensik Linux Gedankliche Hilfsmittel

lsof

```
 # List all open files
lsof
# Processes using a file? (fuser equivalent)
lsof /path/to/file
# Open files within a directory
lsof +D /path
# Files by user
lsof -u name1 -u name2
# By program name
lsof -c apache
# AND'ing selection conditions
lsof -u www-data -c apache
# By pid
lsof -p 1
# Except certain pids
lsof -p ^1
# All network activity by a user
lsof -a -u name1 -i
# TCP and UDP connections
lsof -i tcp # TCP connections   lsof -i udp # UDP connections
lsof -N # NFS use    lsof -U # UNIX domain socket use
# By port
lsof -i :25  =  lsof -i :smtp
lsof -i udp:53
lsof -i tcp:80
# List PIDs
lsof -t -i
```

netstat

```
# list all Ports (tcp/udp/numeric)
Netstat -an[t|u]
# listening connections
UNIX = x
Netstat -l[t|u|x]
# Statistik -p = PID
Netstat -s[t|u|p]
Netstat -i
# promisc Mode
Netstat -ac
#Routing
Netstat -r
#Interface table (Ifconfig)
Netstat -ie
--verbose
```

[f|g]disk

```
# list
Fdisk -l {/dev/sda}
# print part table
Parted /dev/sdx print
```

parted

```
# list block dev
Parted -l
# print part table
Parted /dev/sdx print
```

last

```
# shows last reboot
Last reboot
# last user
Last <username>
# last remotely
Last -d
# system events
Last -x
```

Forensik Linux Gedankliche Hilfsmittel

log2timeline

1. Mount Image → siehe mount / [k]partx
2. log2timeline -p -r -f linux -z GMT /mnt/image -w EForCase_timeline_disk_part.csv
3. Filter
   l2t_process -b EForCase_timeline_disk_part.csv -k keywords.txt <von MM-DD-YYYY>..<bis MM-DD-YYYY>

Forensik Linux Gedankliche Hilfsmittel

gpg

Schlüsselerstellung
gpg --gen-key
Die Defaults sind genügend. Keine Schlüssel mit mehr als 2048 für PGPDesktop/Windows Kommunikation.
Export eines Public Schlüssels in eine Datei
gpg --export -a "User Name / ID" > PUB_ENTERPRISE_name.key.asc
Export eines privaten Schlüssels: (PRIVAT!!!)
gpg --export-secret-key -a "User Name" > PRIV_ENTERPRISE_name.key
Import eines öffentlichen Schlüssels
gpg --import public.key
Import eines privaten Schlüssels
gpg --allow-secret-key-import --import private.key
Löschen eines öffentlichen Schlüssels
gpg --delete-key "User Name"
gg. erst den privaten Schlüssel entfernen
Löschen eines privaten Schlüssels
gpg --delete-secret-key "User Name"
Schlüssel anzeigen
gpg --list-keys
Private Schlüssel anzeigen
gpg --list-secret-keys
Fingerprints erstellen
gpg --fingerprint > fingerprint

Den öffentl. Schlüssel auf Server schicken
gpg --keyserver serverurl --send-keys XXXXXXXX
Schickt Schlüssel mit ID XXXXXXXX zum Schlüsselserver mit URL serverurl
Einen öffentl. Schlüssel vom Server holen
gpg --keyserver serverurl --recv-key XXXXXXXX
Holt den Schlüssel mit ID XXXXXXXXâ vom Server mit URL serverurl

Verschlüsseln
gpg -e -s -u "TXName" -r "RXName1" -r "RXName2" -o gpgfile clearfile
-e encrypt, -s = sign , -u= name als Schlüssel , -c für symmetrische Verschl.
Wx.: gpg -e -us "me" -r "me" -r "you" somedata.tar
Erstellt verschlüsseltes "somedata.tar.gpg". Mich selbst drin – verify.
Achtung: „somedata.tar ist immer noch da!
Entschlüsseln
gpg -d somedata.tar.gpg -o somedata.tar
-d decrypt
Eingabe der Passpharse. Somedata.tar und somedata.tar.gpg sind da.

Forensik Linux Gedankliche Hilfsmittel

Suche Rootkits

RKHunter
Update
#rkhunter --versioncheck
#rkhunter –update --propupd
Kompletter System-Scan nur Befunde
#rkhunter -c –rwo

Lynis
Update
#Lynis update info
System-Scan
#Lynis audit system

CHKROOTKIT
#chkrootkit

CLAMAV
Update
#freshclam
#freshclam -d (wenn Daemon)
System-Scan
Clamscan -i -r /

Kompression

Komprimieren
7z a -t7z -m0=lzma2 -mx=9 -mfb=256 -md=32m -ms=on
Komp. Mit Verschlüsselung
7z a -t7z -m0=lzma2 -mx=9 -mfb=256 -md=32m -ms=on -mhe=on -mem=AES256 -p
Entpacken
7z e

Komprimieren
bzip2 –best
rar a -ep1 -m5 -md4096 -r -s
lzma --best -z
xz -9e

Entpacken
bzip2 -d
unrar
lzma -d
unxz

```
clamclamscan -z -o -r ${src_path}/* -l ${dst_path}/clamscanOutputDisk.txt  --detect-pua=yes --detect-broken=yes \
>> ${dst_path}/clamscanOutputScreen.txt 2>&1 &
```

Forensik Linux Gedankliche Hilfsmittel

AIDE

Init

```
# we do an init of the first time of the DB
MYDATE=`/bin/date +%Y-%m-%d`
DBDIR="/var/lib/aide/"
DBFILE="aide.db"
mkdir -p /var/log/${MYDATE}
/usr/bin/aide -i   >> /var/log/${MYDATE}/aide.log
```

Check only

```
usr/bin/aide -c
```

Check & Update

```
# we do an init of the first time of the DB
MYDATE=`/bin/date +%Y-%m-%d`
DBDIR="/var/lib/aide/"
DBFILE="aide.db"
mkdir -p /var/log/${MYDATE}
/usr/bin/aide -i   >> /var/log/${MYDATE}/aide.log
```

Forensik Linux Gedankliche Hilfsmittel

Identifiziere böse Prozesse → Analysiere Prozesse, Daemons, DLLs, Handles → Suche dazugehörige Netzwerk Artefakte → Gibt es Anzeichen für Code Injection → Zeichen von Trojaner oder Rootkits → Verdächtige Prozesse Daemons sichern

1. Speichererfassung 2. Dumps und Auslagerungsdatei 3. Speicher Zeitlinie 4. Registry Analyse 4. Speicher Analyse

Speichererfassung

Win32dd / Win64dd (32/64bit Systeme
/f Zielpfad und -Name
/s Hash 0=kein, 1=SHA1, 2=MD5, **3=SHA256**)
/t Netzname / IP des Empfängers
/p Port des Empfängers
/l Empfänger hört (listen)
ex.: C:\> win32dd.exe /f E:\mem.img /s 2

Auslagerung und Fehlerreports

Volatility imagecopy
-f Name des Quellfiles (dump/hibernation)
-O Ausgabe Name
--profile QuellOS (vom imageinfo plugin)
Ex.
vol.py imagecopy -f hiberfil.sys -O win7.img

Speicheranalyse

Volatility (Windows memory)
http://code.google.com/p/volatility/

Mandiant Redline (Windows memory)
http://www.mandiant.com/products/free_software/redline

SpeicherZeitablauf

Volatility Timeliner Plugin
#vol.py -f machname.img timeliner \
--output-file machnametimel.csv \
--profile=Win7SP1x86

Volatility Registry Analyse Plugins

Hivelist Vorhandene Registry Einträge aufzeigen
 # vol.py hivelist
Hivedump Ausgabe aller Schlüssel inkl. Unterschlüssel
-o Offset vom registry zur Speicherung
 # vol.py hivedump –o 0xe1a14b60
Printkey Ausgabe eines Schlüssels, Unterschlüssel und Werte
-K "Registry key path"
-o Nur in diesem Abschnitt suchen
 # vol.py printkey –K "Software\Microsoft\Windows\CurrentVersion\Run"
Userassist Finden und durchsuchen von userassist key values
-o Nur in diesem Abschnitt suchen
 # vol.py userassist
Hashdump NTLM / LANMAN Hashes sichern (NTPASSWD)
-y Virtueller Offset des SYSTEM Registries
-s Virtueller Offset des SAM Registries
 # vol.py hashdump –y 0x8781c008 –s 0x87f6b9c8

Check/Baseline

- □ Prozesserstellzeit
- □ Threaterstellzeit
- □ Treibercompilierzeit
- □ DLL/EXE compilierzeit
- □ Netzwerksockelerstellungszeit
- □ Letzter reg. Key Schreibzugriff
- □ Letzter Logeintrag

Forensik Linux Gedankliche Hilfsmittel

Volatility

vol.py -h Hilfe
vol.py plugin -h Plugin Hilfe
vol.py plugin –info Info zu OS Profiles
Aufruf
vol.py -f <image> --profile=<Profil> <Plugin>

Verdächtige Prozesse

Pslist - high level
vol.py pslist
Psscan -Speicher n EPROC blöcken
vol.py psscan
Pstree -Eltern Proc Beziehungen
vol.py pstree

Rootkits suchen

psxview
vol.py pssview
driverscan
vol.py driverscan
Apihooks -p PID -k kernel not usermode
vol.py apihooks
Ssdt system servive descriptor table
(ignorieren von ntoskrn order win32k)
vol.py ssdt | egrep -v '(ntoskrnl|win32k)'
Driverirp -r mit regexp name
vol.py driverirp -r tcpip
Idt Interrupt descriptor table
vol.py idt

SYSTEM Profile Identifikation
vol.py -f speicher.img imageinfo
Nützlich
Systemweite Image
export VOLATILITY_LOCATION=file://img1/speicher.img
Systemweites Profil
export VOLATILITY_PROFILE=Win7SP1x86

Verd.Prozesse dump

dlldump - dll von Proz.
-p spez. PID
-b phys. Mem offset
-r regex name
--dump-dir Dir für img Speicherung
vol.py dlldump –dump-dir ./this -r xx
moddump -Kernel Driver
-o offset (vom Driverscan)
-r regex name
--dump-dir Dir für img Speicherung
vol.py moddump -r w0rm
Procmemdump -mem zu exec
-p spez. PID
-o phys. mem offset
--dump-dir Dir für img Speicherung
vol.py procmemdump
Memdump - mem zu Dateisektion
-p spez. PID
--dump-dir Dir für img Speicherung
vol.py memdump –dump-dir ./memout

Netzwerk Artefakte

connections - offene TCP Verb
vol.py connections
Connscan - TCP Verb. Auch geschl
vol.py connscan
Sockets - Offene sockets
vol.py sockets
Sockscan - ID sockets
vol.py sockscan
Netscan - Suche Verb. Und Sockets
vol.py netscan

Forensik Linux Gedankliche Hilfsmittel

DLL / Proc Analyse

Dlllist - dlls
-p spez. PID
vol.py dlllist
Getsids ! Security Identifiers
-p spez. PID
vol.py getsids -p 76
Handles offene datei hand pro Proc
-p spez. PID
-t typ
{Process, Threat, Key, Event, File, Mutant, Token, Port, ..}
vol.py handes -p 128 -t Process, Port
Filescan Speicher nach Obj suchen
#vol.py filescan
Svscan Windows Service Info
vol.py svcscan

Anzeichen Code Injection

Malfind - injected code finden
-p spez. PID
-s mittels psscan (besser)
-y YARA Regeln
- - dump-dir Speicherort
vol.py malfind -s –dump-dir ./this_dir
Ldrmodules - dangling DLLs finden
-p spez. PID
-v verbose
vol.py ldrmodules -v

Forensik Linux Gedankliche Hilfsmittel

Regular Expressions

Cool : https://txt2re.com

[]	[0-9][A-Za-z0-9]	Genau eine Ziffer soll vorkommen. (Bindestriche definieren einen Bereich)
.	Ein beliebiges Zeichen	
\s	Ein Whitespace = Leerzeichen, Zeilenumbruch, Tabulator, etc.	
\n	newline	
\r	return	
\t	tab	
\d	Eine beliebige Ziffer	
^	1. [^0]2. ^www	Falls in Klammer [] : Negiert nachfolgende Zeichenauswahl a[]c = „aec“ „acc“ … NICHT „abc“
	Beispiel: Alles ausser Zahl 0 Sonst: Zeile beginnt mit der Zeichenkette „www“	
!	!html	Negierung: Alles außer nachfolgenden Zeichen
?	Domain.ch\/?	Das direkt davor stehende Zeichen kann muss aber nicht vorkommen ma?ke = „make“, „mke“
	Beispiel: Trailing Slash kann vorhanden sein	
*	[a-z]*	Der voranstehende Ausdruck darf >=0 vorkommen
+	[a-z]+	Der voranstehende Ausdruck muss >0 vorkommen 12+3 heisst „123“, „1223“, „12223“
$	\?$	Zeile oder String endet mit vorangehendem Zeichen
	Beispiel: Eine URL endet mit einem Fragezeichen	
()	(\.pdf)$	Gruppiert mehre Zeichen zu einer zusammenhängenden Zeichengruppe, um Teilmuster zu erfassen
	Beispiel: PDF-URLs sollen gefunden werden.	
{}	12{3}4	Der direkt davor stehende Ausdruck muss exakt vorkommen. Heisst 12224
|	(a|A)	Agiert als ODER. Nur eines der beiden Zeichen(-ketten) darf vorkommen
\	*	Escape a*c =“a*c“
\b...\b	\bTest\b	Ausdruck innerhalb der Grenzen „Test“ in „Das ist ein RegExp Test“

Ex:

IPv4: ^(?:(?:25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9][0-9]|[0-9])\.){3}(?:25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9][0-9]|[0-9])$

IPv6: '([A-f0-9:]+:+)+[A-f0-9]+'

Beide;-) '/^(?>(?>([a-f0-9]{1,4})(?>:(?1)){7}|(?!(?:.*[a-f0-9](?>:|$)){8,})((?1)(?>:(?1)){0,6})?::(?2)?)|(?>(?>(?1)(?>:(?1)){5}:|(?!(?:.*[a-f0-9]:){6,})(?3)?::(?>((?1)(?>:(?1)){0,4}):)?)?(25[0-5]|2[0-4][0-9]|1[0-9]{2}|[1-9]?[0-9])(?>\.(?4)){3}))$/iD'

Credit Card

^(?:4[0-9]{12}(?:[0-9]{3})?|[25][1-7][0-9]{14}|6(?:011|5[0-9][0-9])[0-9]{12}|3[47][0-9]{13}|3(?:0[0-5]|[68][0-9])[0-9]{11}|(?:2131|1800|35\d{3})\d{11})$

Forensik Linux Gedankliche Hilfsmittel

TC / Cryptocontainer

TC mount

```
cryptsetup open --type tcrypt /media/mydisk/mycontainer mytruecrypt1
mount -t ntfs-3g /dev/mapper/mytruecrypt1 /home/michi/truecrypt
```

TC umount

```
sudo sync
sudo umount /home/michi/truecrypt
sudo cryptsetup close mytruecrypt1
```

Create Cryptocontainer

```
dd if=/dev/urandom of=/tmp/container.bin bs=1024 count=20000
# welches LoopBackDevice wurde genommen
losetup -f
losetup /dev/loop2 /tmp/container.bin
cryptsetup -c aes -s 256 --verify-passphrase luksFormat /dev/loop2
cryptsetup luksOpen /dev/loop2 container
# FS wählen (XFS. NTFS)
mkdosfs /dev/mapper/container
mount /dev/mapper/container /mnt/crypto
umount /mnt/crypto
cryptsetup luksClose container
losetup -d /dev/loop2
```

```
mkdir /mnt/crypto
# welches LoopBackDevice wurde genommen
losetup -f
losetup /dev/loop1 /mnt/usbstick/cryptocontainer.luks
cryptsetup luksOpen /dev/loop1 container
mount /dev/mapper/container /mnt/crypto
```

```
losetup -d /dev/loop1
```

Forensik Linux Gedankliche Hilfsmittel

LVM

lvmdump -d <dir>
dmsetup [info|ls|status]

pvdisplay -v
pvs -[a|v]
pvs --segments
Scannen
pvscan -v
Hinzufügen
pvcreate /dev/sdx3
Entfernen
pvremove /dev/sdx3
Prüfen
pvch -v /dev/sdcx2
Verschieben
Pvmove -v /dev/sdcx2 /dev/sdx3

vgdisplay -v
vgs -[v|o +dev]
Scannen
vgscan -v
Hinzufügen
vgcreate vg0 /dev/sdx1 /dev/sdx2 /dev/sdx3
-l max. log. Vol
-p max. phys. Vol
-s phys ext. Size
-A autobackup
Entfernen
vgremove vg0 /dev/sdx3
Erweitern
vgextend vg0 /dev/sdx3
Reduzieren
vgreduce vg0 /dev/sdx3
Prüfen
vgck vg0
Backup
vgcfgbackup -f /mnt/backupdir/vg0.backup%s vg0
vgcfgrestore -f /mnt/backupdir/vg0.backup vg0
Spezial
vgmknodes vg0 # erstellt die spez. Nodes in /dev

lvdisplay -v
lvs -[v|a -o +dev]
lvs -a -o +devices,stripes,stripesize,seg_pe_ranges --segments
Scannen
lvscan -v
lvmdiskscan
Erstellen
lvcreate -l 10G -n NameVG vg0
Entfernen
lvremove /*dev*/vg0/lv01
Erweitern
lvextend -L+20G /dev/vg0/lv01 -r
xfsgrowfs / resize2fs -p
Reduzieren
lvreduce -L 5M /dev/vg0/lv01
lvresize -L 5M /dev/vg0/lv01
Snapshotting
lvcreate –size 10G –snapshot -name snaps01 dev/vg0data01

SYSLOG (NG)


```
@version: 3.7
# $Header: /var/cvsroot/gentoo-x86/app-admin/syslog-ng/files/syslog-ng.conf.gentoo.3.2,v 1.1 2011/01/18 17:44:14 mr_bones_ Exp $
# Syslog-ng default configuration file for Gentoo Linux
# https://bugs.gentoo.org/show_bug.cgi?id=426814
@include "scl.conf"
options {
                        chain_hostnames(yes);
        threaded(yes);
                        # The default action of syslog-ng is to log a STATS line
                        # to the file every 10 minutes.  That's pretty ugly after a while.
                        # Change it to every 12 hours so you get a nice daily update of
                        # how many messages syslog-ng missed (0).
                        stats_freq(43200);
                        mark_freq(3600);
        flush_lines(10);
        use_fqdn(no);
        #keep_hostname(yes);
        time_reopen(1);
        time_reap(300);
        use_dns(yes);
        dns_cache(yes);
        dns_cache_expire(3600);
        dns_cache_expire_failed(10);
        #long_hostnames(yes);
        #gc_idle_threshold(300);
        #gc_busy_threshold(1000);
        log_fifo_size(16777216);
        log_msg_size(8192);
        owner(root);
        group(root);
        perm(0644);
        dir_perm(0755);
        create_dirs(yes);
        #ts_format(iso);
};
```

SYSLOG (NG)


```
source src {
    unix-dgram("/dev/log" max-connections(256));
    system();
    internal();
    file("/proc/kmsg");
       ## network source using the UDP protocol. If you do not
       ## want to bind to a specific interface use 0.0.0.0.
       # udp <ip>,<port>
       udp();
       ## network source using the TCP protocol.
       # tcp <ip>,<port>
       ## local source used on Solaris system
       # sun-streams <filename>
};

# loghost by michael semling
#destination loghost{ udp("loghost" port(514)); };
#log { source(src); destination(loghost); };

# By default messages are logged to tty12...
destination console_all { file("/dev/tty12"); };
# ...if you intend to use /dev/console for programs like xconsole
# you can comment out the destination line above that references /dev/tty12
# and uncomment the line below.
#destination console_all { file("/dev/console"); };

log { source(src); destination(messages); };
log { source(src); destination(console_all); };
```

SYSLOG (NG)


```
#
# Destinations
#
destination authlog { file("/var/log/$YEAR-$MONTH-$DAY/auth.log"); };
destination cron { file("/var/log/$YEAR-$MONTH-$DAY/cron.log"); };
destination crit { file("/var/log/$YEAR-$MONTH-$DAY/crit.log"); };
destination daemon { file("/var/log/$YEAR-$MONTH-$DAY/daemon.log"); };
destination debug { file("/var/log/$YEAR-$MONTH-$DAY/debug"); };
destination err { file("/var/log/$YEAR-$MONTH-$DAY/err.log"); };
#destination firewall { file("/var/log/$YEAR-$MONTH-$DAY/firewall"); };
destination kern { file("/var/log/$YEAR-$MONTH-$DAY/kern.log"); };
destination localmessages { file("/var/log/$YEAR-$MONTH-$DAY/localmessages"); };
destination lpr { file("/var/log/$YEAR-$MONTH-$DAY/lpr.log"); };
destination mail { file("/var/log/$YEAR-$MONTH-$DAY/mail.log"); };
destination mailinfo { file("/var/log/$YEAR-$MONTH-$DAY/mail.info"); };
destination mailwarn { file("/var/log/$YEAR-$MONTH-$DAY/mail.warn"); };
destination mailerr { file("/var/log/$YEAR-$MONTH-$DAY/mail.err"); };
destination messages { file("/var/log/$YEAR-$MONTH-$DAY/messages"); };
#destination d_mysql { pipe("/tmp/mysql.pipe" template("INSERT INTO logs (host, facility, priority, level, tag, date, time, program, msg) VALUES \
 ( '$HOST', '$FACILITY', '$PRIORITY', '$LEVEL', '$TAG', '$YEAR-$MONTH-$DAY', '$HOUR:$MIN:$SEC', '$PROGRAM', '$MSG' );\n") template-escape(yes));};
destination news { file("/var/log/news.all"); };
destination newscrit { file("/var/log/$YEAR-$MONTH-$DAY/news.crit"); };
destination newserr { file("/var/log/$YEAR-$MONTH-$DAY/news.err"); };
destination newsnotice { file("/var/log/$YEAR-$MONTH-$DAY/news.notice"); };
destination user { file("/var/log/$YEAR-$MONTH-$DAY/user.log"); };
destination uucp { file("/var/log/$YEAR-$MONTH-$DAY/uucp.log"); };
destination warn { file("/var/log/$YEAR-$MONTH-$DAY/warn"); };
# R_DATE is human but not machine readable
#destination pgsql {
#   sql(type(pgsql)
#   host("127.0.0.1") username("syslog") password("gggggg") port("5432")
#   database("syslog")
#   table("syslogmessages")
#   columns("datetime varchar(12)", "host varchar(32)", "program varchar(64)", "pid integer", "facility int", "priority int", "message varchar(200)")
#   values("$UNIXTIME", "$HOST", "$PROGRAM", "$PID" ,"$FACILITY_NUM", "$PRIORITY_NUM", "$MSG")
#   indexes("datetime", "host", "program", "pid", "facility", "priority", "message"));
#};
#
```

SYSLOG (NG)


```
#
# Chaining the input, destination and the filter definitions
#
log { source(src); filter(f_authpriv); destination(authlog); };
log { source(src); filter(f_cron); destination(cron); };
log { source(src); filter(f_console); destination(console_all); };
log { source(src); filter(f_crit);  destination(crit); };
log { source(src); filter(f_daemon); destination(daemon); };
log { source(src); filter(f_debug); destination(debug); };
log { source(src); filter(f_emergency); destination(console_all); };
log { source(src); filter(f_err); destination(err); };
log { source(src); filter(f_iptables); destination(firewall); };
log { source(src); filter(f_kern); destination(kern); };
log { source(src); filter(f_local); destination(localmessages); };
log { source(src); filter(f_lpr); destination(lpr); };
log { source(src); filter(f_mail); destination(mail); };
log { source(src); filter(f_mail); filter(f_info); destination(mailinfo); };
log { source(src); filter(f_mail); filter(f_warn); destination(mailwarn); };
log { source(src); filter(f_mail); filter(f_err); destination(mailerr); };
#log { source(src);  destination(d_mysql); };
log { source(src); filter(f_news); filter(f_newscrit); destination(newscrit); };
log { source(src); filter(f_news); filter(f_newserr); destination(newserr); };
log { source(src); filter(f_news); filter(f_newsnotice); destination(newsnotice); };
log { source(src); filter(f_messages); destination(messages); };
log { source(src); filter(f_user); destination(user); };
log { source(src); filter(f_uucp); destination(uucp); };
log { source(src); filter(f_warn); destination(warn); };
log { source(src); destination(console_all); };
#log { source(src); filter(f_console); destination(xconsole); };
log { source(src); destination(pgsql); };
```

SYSLOG (NG)


```
#
# filter definitions
#
#filter f_alert      { level(alert); };
filter f_auth       { facility(auth); };
filter f_authpriv   { facility(auth, authpriv); };
filter f_console    { level(warn) and facility(kern) or level(err) and not facility(authpriv); };
filter f_crit       { level(crit); };
filter f_cron       { facility(cron); };
filter f_daemon     { facility(daemon); };
filter f_debug      { not facility(auth, news, mail); };
filter f_emergency  { level(emerg); };
filter f_err        { level(err); };
filter f_info       { level(info); };
filter f_iptables   { facility(kern) and match("IN=") and match("OUT="); };
filter f_kern       { facility(kern); };
filter f_local      { facility(local0, local1, local2, local3, local4, local5, local6, local7); };
filter f_lpr        { facility(lpr); };
filter f_mail       { facility(mail); };
filter f_messages   { level(info..warn) and not facility(auth, mail, news); };
log { source(src); filter(f_news); destination(news); };
filter f_newsnotice { level(notice) and facility(news); };
filter f_newscrit   { level(crit)   and facility(news); };
filter f_newserr    { level(err)    and facility(news); };
filter f_news       { facility(news); };
filter f_notice     { level(notice); };
filter f_user       { facility(user); };
filter f_uucp       { facility(cron); };
filter f_warn       { level(warn, err, crit); };
```

Dokument zur Kenntnisnahme von klassifiziertem Material

Sicherstellung zur nachgewiesenen Abgabe für
<FIRMA EINSETZEN>
<Vertraulich|Geheim>
klassifiziertes Dokument.

Angeordnet durch **<CEO|Auftraggeber>**

.....

Dokumentenname: **Dokumentenname einsetzen**
Datum des Dokuments: **TT/MM/YYYY einsetzen**
Gültig bis: **TT/MMYYYY einsetzen**
Dokumentenverantwortlicher: **Erstautor/Ersteller des Dokumentes**

Nr.	Abgabedatum	Retournierung	Name	Unterschrift
1				
2				
3				
4				
5				
6				
7				
8				
9				

Genehmigt durch: .....

<Name Dokumentenabgebender, Unterschrift>

Dokument zur Kenntnisnahme von klassifiziertem Material

Dokumenten Mutationen

Nr.	Datum	Mutation/Rückzug/Vernichtung	Autor
1			
2			
3			
4			
5			
6			
7			
8			
9			

Auf dem Dokument sind das Datum und der Verteiler festzuhalten. Bei nummerierten Exemplaren ist sicherzustellen, dass die Abgabe nachgewiesen werden kann. (Das heisst, der Verfasser führt eigenverantwortlich schriftlich Kontrolle über die Abgabe der Information mit Abgabedatum, Empfänger, Mutationen, Rückzug, Vernichtung)

Aus der Ereignisbehandlung und der forensischen Untersuchung (SANS und andere) müssen folgende Punkte gelöscht werden. Dies soll Missbrauch und Fehler verhindern.

1. Welche rechtlichen Aspekte müssen berücksichtigt werden?◦ Offizielle Personen in der mündlichen Verhandlung, z. Mitarbeiter, Chef, HR, Ermittler
   - ◦ Beteiligte / betroffene Personen dürfen nicht im Incident-Prozess arbeiten.
   - ◦ Alle Beteiligten müssen eine NDA unterzeichnen, wenn das Ereignis geheim gehalten werden soll
   - ◦ Im Vorfeld muss bekannt sein, welche Verfahren zur rechtlichen Korrektheit eingesetzt werden müssen
   - ◦ Eine NDA (Non-Disclosure-Agreement) für die Daten muss unterzeichnet werden
   - ◦ Es muss eine Quittung für physische Geräte vorliegen, die zur Beweissicherung entfernt wurden
   - ◦ Wie die Daten gespeichert sind, dass Manipulationen eingeschränkt oder unmöglich sind. (z.B. Mehrfachsignierschlüssel / persönliche Passwörter)
   - ◦ Am Ende der Untersuchung muss ein schriftlicher Bericht an alle Verantwortlichen gesendet werden
   - ◦ Ein schriftlicher Bericht mit allen Ergebnissen muss an den Dateneigentümer gesendet werden
   - ◦ Der Ruf aller Beteiligten muss wiederhergestellt werden
   - ◦ Alle Beteiligten müssen informiert werden
   - ◦ Die Verfahren zur Datenerfassung und die mögliche Zerstörung von Daten (z. B. Neustart) müssen deutlich angegeben werden
   - ◦ Die Speicherung der Daten oder die permanente Entfernung (das Verfahren, z. B. Vier-Augen-Wischen und Vier-Augen-Verifizierung) muss klar sein.
   - ◦ Verstöße gegen die Behandlung von Vorfällen müssen als Vorfall betrachtet werden
   - ◦ POLITISCHE Verstöße müssen untersucht werden
   - ◦ Informationen zur Verhinderung von Gerüchten müssen vorbereitet werden

Der Angriff und die Gründe für den Angriff müssen erklärt werden.

- ◦ Welche Arten von Vorfällen treten auf? Handelt es sich um Virenangriffe, Denial-of-Service-Angriffe, gehackte Systeme, Kompromittierungen von Benutzerkonten oder andere Angriffe?
- ◦ Wie viel Zeit Ihres IT-Personals wird für die einzelnen Arten von Angriffen aufgewendet?
- ◦ Was ist der Schaden in der Arbeitszeit und der Produktivitätsverlust aufgrund jeder Art von Angriff?
- ◦ Was ist der Schaden an Daten aufgrund jeder Art von Angriff und was kostet das?
- ◦ Was ist das Risiko für Schäden an der Organisation aufgrund kompromittierter Daten oder verlorener Daten aufgrund jeder Art von Angriffen?
- ◦ Was ist das allgemeine Risiko für das Überleben der Organisation aufgrund jeder Art von Angriff?

2. Einige Elemente, die in Ihrem Computer-Sicherheitsvorfallformular enthalten sein sollten, umfassen:
    - Vorfalldatum und -zeit
    - Welche Prozesse, Werkzeuge werden eingesetzt und was wird gepflegt?
    - Name des Computersystems und / oder betroffene Nummern.
    - betroffene Systemlokation (en)
    - Betriebssystem (e) auf dem betroffenen System.
    - Art des betroffenen Systems (Arbeitsplatz, Mailserver, Dateiserver usw.)
    - Art des Eindringens (Datenkompromittierung, Virenvorfall, Denial-of-Service-Angriff usw.)
    - Wie wurde das Eindringen entdeckt?
    - Auswirkung des Eindringens
    - Wie ist das Eindringen aufgetreten?
    - Wie wurde das Eindringen entfernt?
    - Schritte, um die gleiche Art von Einbruch wieder zu verhindern
    - Wer wurde über das Eindringen informiert?
    - Zeit, die für den Umgang mit dem Eindringen und die Kosten des Eindringens in die Organisation aufgewendet wurde

Von http://www.forensics-intl.com/evidguid.html

Verarbeitungsschritte für Computernachweis

Allgemeine Richtlinien für die Verarbeitung von Beweisen folgen:

1. **Den Computer herunterfahren**
2. **Dokumentieren Sie die Hardware-Konfiguration des Systems**
3. **Transportieren Sie das Computersystem an einen sicheren Ort**
4. **Dokumentieren Sie die Hardware-Konfiguration des Systems**
5. **Erstellen Sie Bit-Stream-Sicherungen von Festplatten und Disketten**
6. **Daten auf allen Speichergeräten mathematisch authentifizieren**
7. **Dokumentieren Sie das System Datum und Uhrzeit**
8. **Erstellen Sie eine Liste mit Schlüsselwortern**
9. **Evaluieren Sie die Windows-Swap-Date**
10. **Datei-Slack auswerten**
11. **Nicht zugewiesenen Speicherplatz auswerten (Erased Files)**
12. **Durchsuchen Sie Dateien, Dateispeicher und nicht zugeordneten Speicherplatz für Schlüsselwörter**
13. **Document File Names, Dates and Times**
14. **Identifizieren Sie Datei-, Programm- und Speicheranomalien**
15. **Bewerten Sie die Programmfunktionalität**
16. **Dokumentiere deine Ergebnisse**
17. **Bewahren Sie Kopien der verwendeten Software auf**

IT-Forensik Ziele und Entlastung

Monat Jahr

Firma <Klassifizierung>

Disposition

Dieses Dokument deckt den Umfang der Analyse ab und dokumentiert die erlaubten Schritte für die elektronische forensische Analyse der Informationen und Datenträger und entlastet die Forensiker.

Klassifikation *	Nicht Klassifiziert ☐	Klassifikation INTERN ☐	<Klassifikation Vertraulich> ☐
Version:	1.0 (Abgenommen)		
Doc Mgmt:	IT-ForensikEntlastung_1		
Doc Typ:	Voranalyse Dokument		
Status	In Arbeit ☐	Prüfungsstatus ☐	Bereit zum Gebrauch ☐
Projekt Name:	IT-Forensik		
Autor	Firma		
Freigabe	Firma		

Liste der Autoren

Autoren:

Änderungsnachvollziehbarkeit

Sig	Datum	Änderung

Forensik Team Kontakt Information:

Erster Kontakt:	
Mobiltelefon:	
E-Mail:	
GPG-Schlüssel:	
Zweiter Kontakt:	
Mobiltelefon:	
E-Mail:	
GPG-Schlüssel:	
Dritter Kontakt:	
Mobiltelefon:	
E-Mail:	
GPG-Schlüssel:	
Vierter Kontakt:	
Mobiltelefon:	
E-Mail:	
GPG-Schlüssel:	

Kunde / Organisation Kontakt Information:

Erster Kontakt:	
Mobiltelefon:	
E-Mail:	
GPG-Schlüssel:	
Zweiter Kontakt:	
Mobiltelefon:	
E-Mail:	
GPG-Schlüssel:	
Dritter Kontakt:	
Mobiltelefon:	
E-Mail:	
GPG-Schlüssel:	

IT-Forensik Erlaubnis und Umfang Arbeitsblatt

Die Überprüfung der Informationssicherheit umfasst Techniken wie das Scannen von Schwachstellen in der Anwendungssicherheit, das Penetration und Testen der Anwendungen, die statische Analyse und die manuelle Codeüberprüfung. Diese Überprüfung ist ein wichtiger Teil des Prozesses, um sicherzustellen, dass eine Anwendung ordnungsgemäss vor möglichen Angriffen geschützt ist. Computerforensik ist ein wissenschaftlicher Ansatz zum Sammeln, Verarbeiten, Aufbewahren und Präsentieren elektronischer Beweise. Diese Erlaubnis gewährt dem Verantwortlichen das Recht auf

- ☐ den Zugang zu Räumlichkeiten, Gebäuden, Räumen
- ☐ den Zugang zu Arbeitsplätzen, Arbeitszonen
- ☐ das Zugreifen auf Serverorte, Serverzonen
- ☐ das anschliessen von Sicherheitsausrüstung an das Netzwerk
- ☐ das Durchführen von Netzwerkinformations-Scans
- ☐ Das Durchführen von Netzwerkport-Scans
- ☐ Das Durchführen von Netzwerk-Schwachstellen-Scans
- ☐ Das Ausführen von Netzwerk-Exploits
- ☐ Netzwerk-Denial-of-Service durchführen
- ☐ Das Durchführen Netzwerkgefährliche Checks / Exploits durchführen
- ☐ Das Durchführen von Netzwerk-Penstests
- ☐ Das Durchführen von Host-Informations-Scans
- ☐ Das Durchführen von Host-Port-Scans
- ☐ Das Durchführen von Host-Schwachstellen-Scans
- ☐ Das Ausführen von Host-Exploits
- ☐ Das Durchführen von Host-Denial-of-Service durchführen
- ☐ Das Ausführen gefährlicher Host-Prüfungen / Exploits
- ☐ Das Durchführen von Host-Audit durchführen
- ☐ Das Durchführen Host-Pentest durchführen
- ☐ Das Durchführen von Reverse Engineering bei Programmcode
- ☐ Das Durchführen von Passwort-Audit durchführen
- ☐ Das Durchführen von Kryptoanalyse durchführen
- ☐ Das Ausführen von Software-Exploits
- ☐ Das Durchführen von Software-Audits
- ☐ Das Durchführen von physischen Penetrationsversuchen
- ☐ Das Durchführung von Social Engineering
- ☐ Das Fuehren von Interviews führen
- ☐ Das Durchführen von Änderungen auf Anwendungsebene
- ☐ Das Durchführen von clientseitigem Java / ActiveX Reverse Engineering
- ☐
- ☐
- ☐

Daten / Netzwerkzugriff auf Layer (OSI – Model)

1: ☐ 2: ☐ 3: ☐ 4: ☐ 5: ☐ 6: ☐ 7: ☐

Maschinenzugriff auf Layer (OSI – Model)

1: ☐ 2: ☐ 3: ☐ 4: ☐ 5: ☐ 6: ☐ 7: ☐

Verantwortlicher Leiter	
Verantwortlicher Kunde	
Platz / Ort	
Start Datum und Zeit	
End Datum und Zeit	
Report Frequenz :	
Report Zeit / Ort:	

Was sind die grössten Sicherheitsbedenken der Zielorganisation? (Beispielsweise die Offenlegung sensibler Informationen, Unterbrechung der Produktionsverarbeitung, Reputationsschaden durch Webseitenänderung usw.)

Welche spezifischen Hosts, Netzwerkadressbereiche, Exploits oder Anwendungen sollten explizit **NICHT** getestet werden?

Was soll speziell analysiert werden	
Host	
Type	
Serial No	
Version No	
OS	
BIOS	
IP Address	
Network	
Server	
Infrastructure (FW, Router, switch,.)	
Address range	
Anwendung	
Typ (Office, Image,..)	
Daten	
Typ (Office, Image,..)	
Abbild	
Typ	
Zugriff	
Name	
Grösse	
SHA2-256	

Auflistung von Drittparteien, die Informationen, Systeme oder Netzwerke besitzen, die sich in ihrem Zielbereich/Organisation befinden, sowie deren Eigentümer sie sind (schriftliche Genehmigung muss vorab von der Zielorganisation eingeholt worden sein):	
Partei	Schriftliche Genehmigung (Name) erhalten durch (Name)

Wird die Analyse drchgeführt auf einer

☐	produktiven Umgebung	☐	nicht produktiven (Test/Entwicklung) Uumgebung

Interner Netzwerkzugriff wird erhalten von	Name, Datum

Sind Endbenutzer- oder Arbeitsstationen betroffen, so müssen die Betroffenen ihre Einwilligung mit Namen und Datum geben	

Falls Layer7 (Anwendungsdaten) betroffen sind, muss das Datenschutzgesetz berücksichtigt werden. Falls ja, sind die zuständigen Stellen informiert (Name, Datum)	

Alle betroffenen Personen sind informiert, bestätigt Name, Datum	

Ist das Kontrolling/Behörde informiert und ein vier-Augen-Prinzip erforderlich? Anforderungen gegen durch Name, Datum.	

_____

Unterschrift der hauptsächlichen Kontaktperson als Repräsentant der Zielorganisation

_____

Datum

_____

Signature of Head of Analysis Team

_____

Date

FERTIG

Und die Antwort „nach dem Leben, dem Universum und dem ganzen Rest“ ist…..

42

Zitat: „Per Anhalter durch die Galaxis“ Douglas Adams.