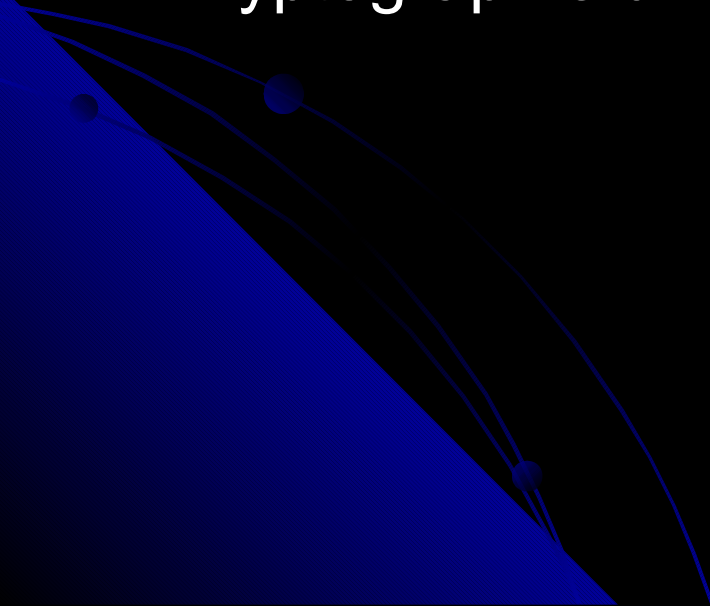


Digitale Forensik mit Open Source Tools

für Anfänger !!!!!



Agenda

- Grundlagen der Forensik
 - Datensicherung erstellen
 - Untersuchung von Datensicherungen
 - Virtualisierung von Datensicherungen
 - Kryptographie und andere Probleme
- 

Allgemeines

- Bei der Forensik zählen vor allem:
 - ERFAHRUNG und WISSEN
- Das heißt:
 - Es gibt keine Pauschallösung
 - Es gibt kein allumfassendes Tool
 - Jeder handelt individuell
- Es gibt zahllose coole Forensiktools
 - meist ist die Nutzung nicht selbsterklärend
 - der Vortrag umfasst nur einen geringen Teil
- Ich werde viele Frage NICHT beantworten können!

Grundlagen

Fragestellungen:

- Was ist Forensik?
- Gründe für eine forensische Untersuchung?
- Habe ich eine organisierte Vorfallsbearbeitung?
- Ist der Angriff aktuell?
 - Live-Forensik vs. Post Mortem Analyse
- Beweissicherung vs. Produktivität
 - Abwägung zum Schaden durch Ausfallzeiten
- Welche Daten befinden sich auf den Systemen?
- Virtualisierung, Kryptographie
- Kommerzielle oder Open Source Tools

Datensicherung

- Physikalische vs logische Datensicherung
- Bezeichnungen:
 - Disk
 - Volume
 - Dateisystem
 - Datenblöcke (Cluster)
 - Metadaten
 - Dateien im weitesten Sinne
- Populäre Forensik Live-CD's
 - Helix, Deft, Caine, Paladin, Backtrack, GRML

Dateisystem ext 2/3/4

ext-Partition



Blockgruppen



Aufbau einer Blockgruppe (Superblock und Gruppendedesk. nur in best. Gruppen)



Superblock (Anzahl Inodes, Blöcke, Mounts, letzter Mount, usw.)



Gruppendedeskriptor (Pos. BlockBitmap, InodeBitmap, usw. f. jede Gruppe)



Blockbitmapblock (Belegungszustand Blöcke)



Inodebitmapblock (Belegungszustand Inodes)



Inodebitmable (128 Byte pro Datei, Rechte, Blockadressen, usw.)



Datenblöcke

Dateisystem ext 2/3/4

Datenblock 4096 Byte = 8 Sektoren a -derzeit noch typisch- 512 Byte

dies ist ein kleiner test text und hat nicht viel	dies ist ein kleiner test text und hat nicht viel	dies ist ein kleiner test text und hat nicht viel	dies ist ein kleiner test text und hat nicht viel	dies ist ein kleiner test text und hat nicht viel	dies ist ein kleiner test text und hat nicht viel	dies ist ein kleiner test text und hat nicht viel	dies ist ein kleiner test text und hat nicht viel
--	--	--	--	--	--	--	--

Der obige Block gehört zu der Datei „Betriebsgeheimnisse.txt“

Die Datei „Betriebsgeheimnisse.txt“ wird gelöscht.

Ein User erstellt eine neue Datei namens „Brief an Oma.txt“.

Die Datei endet in dem zuvor gelöschten, obigen Block.

FOLGE → Slackspace

Gruß Jan	dies ist ein kleiner test text und hat nicht viel	dies ist ein kleiner test text und hat nicht viel	dies ist ein kleiner test text und hat nicht viel	dies ist ein kleiner test text und hat nicht viel	dies ist ein kleiner test text und hat nicht viel	dies ist ein kleiner test text und hat nicht viel	dies ist ein kleiner test text und hat nicht viel
----------	--	--	--	--	--	--	--

File Slack

Auswertesystem

Caine 2.5

- Ubuntu basierte Forensik CD
- diverse Pakete sollte man nachinstallieren:
 - Netzwerkttools
 - Packer
 - kvm (qemu)
- und selbst kompilieren:
 - Digital Forensic Framework (DFF)
 - Log2timeline

Datensicherung erstellen

Forensikformate:

- Raw (dd, img), Encase (E01), Advanced Forensic format (aff)
- Kommandozeilentools:
 - Raw Image: dd, dc3dd
 - Encase-Image: ewfacquire
 - AFF-Image: aimage
- Sicherung mittels GUI-Tools
 - guymager
- Sicherung über das Netzwerk
 - sshfs
 - nc
- VMDK einbinden und sichern

Datensicherung untersuchen I

Zu findende Informationen:

- Vorhandene Dateien
- Gelöschte Dateien
 - nur der Dateisystemlink wurde entfernt
 - Link zwischen Dateiname und Metadaten weg
 - Metadaten und Dateiname gelöscht
 - Datei partiell überschrieben
 - Datei vollständig überschrieben
- File Slack (X-Ways = Schlupfspeicher)
- RAM Slack (mittlerweile quasi bedeutungslos)

Datensicherung untersuchen II

Struktur der Toolsammlung TSK (The Sleuth Kit):

- mm = media management
- fs = filesystem
- i = inode
- f = file
- stat = statusinformationen
- ls = auflisten von Informationen
- cat = entspricht dem normale cat
 - fls = listet Dateien auf
 - icat = erstellt Inhalt anhand eines Inodes

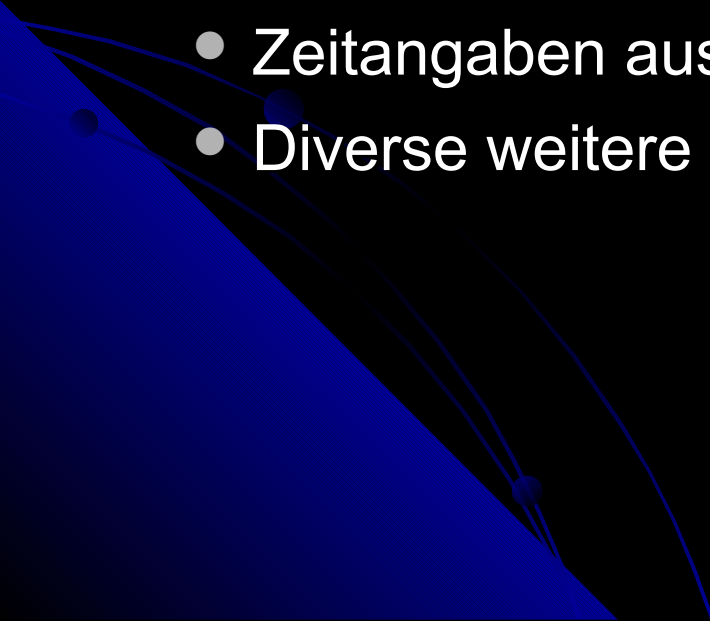
Datensicherung untersuchen III

- Carving bezeichnet das Suchen nach Dateien anhand bekannter Dateiheder
 - foremost
 - scalpel
 - photo-rec
- md5deep kann rekursiv Hashwerte erstellen
 - herausfiltern un/bekannter Dateien
- ssdeep kann Dateiähnlichkeiten erkennen
 - splittet Dateien in Blöcke, Hasht diese und vergleicht die Inhalte

Dateianalyse

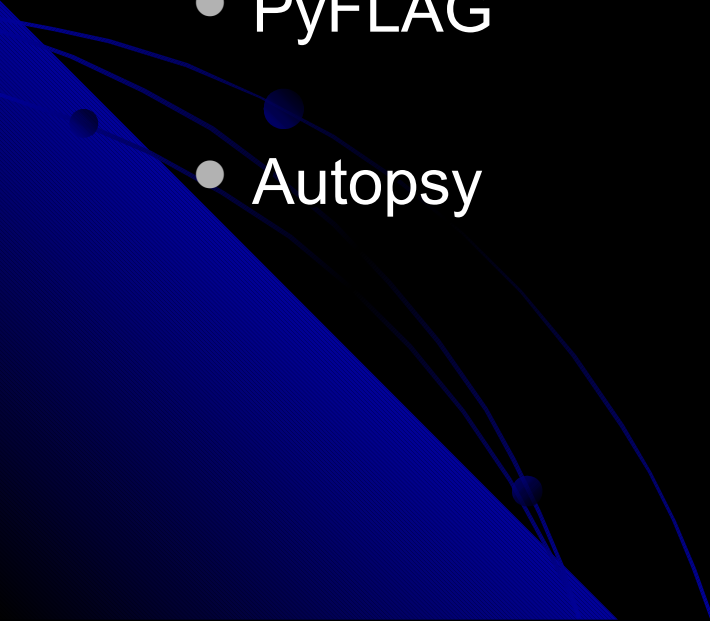
- Dateiinhalt + Dateimetadaten
- Content Identifizierung = um was für einen Dateityp handelt es sich (Magicfile)
- Metadaten = Extraktion der Daten die über den eigentlichen Dateiinhalt hinausgehen (Geodaten in Exif usw.)
- Content = der eigentliche Inhalt einer Datei
- Typische Dateitypen mit wertvollen Informationen:
 - Bilder
 - OLE-Dokumente
 - PDF-Dokumente

Zeitlinienanalyse

- Erstellen einer Timeline
 - Erweiterte Funktion mittels Log2timeline
 - Zeitangaben aus Metadaten
 - Zeitangaben aus Logfiles
 - Zeitangaben aus Dateien
 - Zeitangaben aus Browserhistory
 - Zeitangaben aus Recycler
 - Diverse weitere Daten
- 

Grafische Umgebungen

Tools die die zahlreichen Ermittlungsergebnisse unter einer Oberfläche zusammen führen.

- DDF
 - PyFLAG
 - Autopsy
- 

Datensicherung virtualisieren

Encasesicherung eines Windowssystems starten

- Umwandeln der Dasi mittels xmount
- Datenträgerstruktur betrachten
- Partitionen mounten mit Offset
- Kopieren der Windows Registry-Hives
- Passworte ermitteln mit Ophcrack
- Booten mit Opengates
 - Ändern von Treibern
 - WPA deaktivieren
 - ggf. Passwort löschen
- Image booten

Live-Systemanalyse I

PROBLEM: Angeschalteter Computer!

- Wie immer gibt es nicht DIE eine Lösung!
- Warum müssen flüchtige Daten gesichert werden
 - Was nicht gesichert wird, ist für immer verloren!
 - Manche Beweise (z.B. einige Rootkits) finden sich nur im RAM
 - ggf. relevante Daten wurden noch nicht gespeichert
 - Kryptographische Schlüssel
- Werden nicht Änderungen vorgenommen?
 - Ja, aber es gibt keine Alternativen!
 - Gute Dokumentaktion wichtig

Live-Systemanalyse II

Was muss beachtet werden?

- Nochmals! Alles gut Dokumentieren
- eigene Binaries verwenden
- so wenig wie möglich verändern
- Einstecken von USB-Sticks zieht bereits umfangreiche Änderungen nach sich
(Treiber, Kernelmodule, Timestamps)
- CD-Rom weniger, aber nicht immer verfügbar
- über das Netzwerk (z.B. netcat)
- Inhalte immer auf externe Datenträger oder auf Netzwerkfreigabe (sshfs) speichern
- ggf. fotografische Sicherung

Live-Systemanalyse III

Was soll gesichert werden und womit (Linux)?

- System und Zeit (uname, date, uptime)
- Netzwerkverbindungen (netstat, arp, route)
- Prozesse (ps, top)
- User (w)
- RAM (/dev/mem geht i.d.R. nicht, ggf. passendes Kernelmodul fmem extern kompilieren)
- geladene Module (lsmod)
- genutzte „Dateien“ (lsdf)
- gemountete Geräte (mount)
- Nutzung einer Bridge

Probleme

- Aniforensictools
 - Unterbinden der Datensicherung
 - Verändern der Datensicherung
 - Manipulieren von Berichten (X-Ways)
- Kryptographie
 - Truecrypt
 - Systemverschlüsselung
 - versteckte Systeme
 - Container
 - Angriffsmöglichkeiten i.d.R nur BruteForce
 - Stringsanalyse
 - RAM-Dump
- Rechtliche Probleme!!!
 -

Ende

Fragen?



Befehlsliste I

- Datensicherung erstellen:
 - `dc3dd if=/dev/sdx hof=blafa.dd bufsz=32K hash=md5 hlog=blafa.md5`
 - `ewfacquire /dev/sdx`
 - `aimage -o blafa.aff /dev/sdc`
 - Netzwerk: Auf Empfangsrechner: `nc -l 8888`
auf Senderechner: `dc3dd if=/dev/sdx bufsz=32K | nc IP-Empfangsrechner 8888`
- Datensicherungen untersuchen:
 - `mmls blafa.img` (Informationen über ein Volume)
 - `fsstat -o 2048 blafa.img` (Informationen über ein Filesystem, o=Offset zum Beginn des FS)
 - `ils -aZ -o 2048 blafa.img` (Listet die allozierten Inodes auf)
 - `ffind -o 2048 blafa.img 7779` (findet den zur Inode 7779 gehörenden Dateinamen)
 - `icat -o 2048 blafa.img 7779 > neu.xxx` (stellt die Datei mit d. Inode 7779 unter d. Namen neu.xxx wieder her)
 - `fls -rd -o 2048 blafa.img` (durchsucht das Image rekursiv nach gelöschten Dateien)
 - `fls -r -o 2048 -m „/“ blafa.img > blafa.bodyline` (Erstellt eine rekursive Dateiliste für eine Zeitlinie)
 - `mactime -b blafa.bodyline -d > blafa.csv` (Erstellt aus der o.a. Dateiliste eine Tabelle im csv-format)
 - `sigfind -b 4096 25504446 blafa.img` (sucht nach PDF-Header (25504446) an jedem Blockbeginn, hier 4k)
 - zahlreiche weitere Tools in TSK vorhanden!!!

Befehlsliste II

- Carving:
 - foremost -v -i blafa.img (durchsucht das Image nach bekannten Dateihheadern und kopiert die gefundenen Dateien nach output)
- Hashen
 - hashdeep -r /usr/sbin > blafa.txt (Hasht rekursiv das Verzeichnis /usr/sbin und schreibt dieses nach blafa.txt)
 - hashdeep -r -x -k blafa.txt /usr/sbin (vergleicht das Verzeichnis mit der erstellten Datei und gibt alle nicht identischen Dateien / Hashwerte auf der Standardausgabe aus)
 - ssdeep -br /home/user/Dokumente > blafa.txt (Splittet die Dateien blockweise und hasht diese)
 - ssdeep -brm blafa.txt /home/user/Dokumente (Versucht Ähnlichkeiten von Dateien anhand des Anteils übereinstimmender Blöcke festzustellen)
- Dateianalyse:
 - for file in *; do file \$file; done (Ermittelt anhand des Magicfiles, den Dateityp der Dateien im akt. Verzeichnis)
 - identify -verbose blafa.jpg (Metadaten aus einer Bilddatei feststellen)
 - exiftool blafa.pdf (Metadaten einer PDF-Datei feststellen)
 - hier gibt es eine riesige Zahl an Tools!!!
- Super Timelines
 - log2timeline -f apache2_access access.log > apache.body (Konvertiert das Log in ein Timelineformat)
 - log2timeline -f syslog syslog >syslog.body (wie oben nur mit syslog)
 - cat apache.body syslog.body | sort > timeline.csv (erstellt eine Zeitlinie im csv Format)
 - log2timeline -f list (listet alle konvertierbaren Dateitypen auf)
 - super mächtiges Tool, dass Zeitstempel aus verschiedensten Quellen zusammen führen kann!!!!

Befehlsliste III

- Virtualisieren einer Datensicherung am Beispiel Windows XP:
 - `xmount -in ewf -out dd -cache blafa blafa.E0? /mnt/xxx` (Konvertiert ein EWF-Image in ein virtuelles Raw-Image, der `cache`-Parameter virtualisiert eine Schreibmöglichkeit)
 - `mount -o loop,offset=$((512*2048)) /mnt/xxx/blafa.dd /mnt/yyy` (mountet das Image als Loopdevice)
 - `cp /mnt/yyy/Windows/system32/config/{SAM,system} ~` (Registry-Hives kopieren)
 - `opphcrack` (Rainbowtables laden und auf die kopierte SAM anwenden)
 - `qemu -m 1024 -boot d -cdrom opengates021.iso -hda blafa.img` (Startet die Opengates-CD)
 - Treiber verändern
 - Windows Produktaktivierung herausnehmen
 - Passwörter löschen
 - klappt alles nicht immer ;-)
 - Anschließend Neustart von `blafa.img`