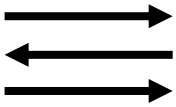
SYNerity



Analyse von Unix-Rechnern

Unix, aha! ... Welches genau?

- Linux
- BSD
- Solaris
- HP-UX
- True64
- AIX

SYNerity

Unix-Analyse Online

SYNerity

Willkommen in Babylon

Jeder Unix-Dialekt hat andere Befehle bzw. eigene Switches

SYNerity

Dokumentation unter Unix

- Befehl script protokolliert alle Eingaben
- Protokollierung nicht auf den Datenträger, der als Beweismittel benötigt wird

SYNerity

Dateisystem /proc

- Prozesse
  - Memory
  - Laufende Programme
  - Environment-Variablen
  - Befehlszeile
- Betriebssystem
  - Geladene Module
  - Gemountete Laufwerke
  - Netzwerk-Verbindungen

SYNerity

Hilfreiche Programme

- vmstat, mpstat
  - Schnelle Anzeige von Prozessorlast, Speicher etc.
- iostat
  - Konzentriert sich auf IOs
- lastcomm
  - Zeigt die letzten ausgeführten Befehle an
- ps
  - Zeigt die laufenden Prozesse
  - ps –aux bzw. ps –ef

SYNerity

Noch mehr Unix-Tools

- file, ldd
  - Identifiziert die vorliegende Datei (executable, library ...)
- strace (Linux) – truss (Solaris) – ktrace (BSD)
  - Zeigt, welche System-Funktionen ein Prozess nutzt
- strings
  - Filtert alle ASCII-Zeichen aus einer Datei
  - nützlich bei der Analyse von Rootkits

SYNerity

nc - netcat

- netcat kopiert Daten vom Netzwerk „Schweizer Taschenmesser“
- netcat-Listener starten
  - **Programmende bei Verbindungsabbau:**
    `nc -l -p port`
  - **Neustart des Listeners:**
    `nc -L -p port`

SYNerity

Output umlenken

- Output umlenken:
  - **ps -aux > outfile**
- Ausgabe an existierende Datei anhängen
  - **ls -lisaR >> outfile**
- Fehler abfangen:
  - **ps -aux > outfile 2> errormsg**

SYNerity

Festhalten flüchtiger Daten

- Prozess-Informationen kopieren
  - **ls -lisaR /proc | nc target port**
- Laufendes Programm von Platte gelöscht
  - **cp /proc/pid/exe programm**
- Memory
  - **dd bs=1024 < /dev/mem | nc target port**
  - **dd bs=1024 < /dev/kmem | nc target port**

SYNerity

Flüchtige Daten

- Offene Dateien
  - **lsof**
  - **lsof –p <pid>**
- Netzwerk-Verbindungen
  - **netstat –an**
- Routen
  - **route print** oder **route show**

SYNerity

Unix-Analyse Offline

SYNerity

Superblock

- Start des Dateisystems
- Enthält u. a. Informationen über
  - Mount-Zeit
  - Mount Count
  - Volumen Name

SYNerity

inode

- Metadaten über eine Datei
- Enthält u. a.
  - MAC-Zeiten
  - Liste genutzter Cluster
  - Indirekte Cluster:
    Verweis auf eine Liste weiterer Cluster
  - Doppelt indirekte Cluster:
    Verweis auf eine Liste von Verweisen weiterer Cluster

SYNerity

Journaling Filesystems

- Zuverlässig
- Weit verbreitet: ext3, reiserfs
- Journal-Datei enthält letzte Transaktionen

SYNerity

Suchen in

- /etc
  - Usernamen
  - Dienste
- /home/*/.history
- /var/log
- /dev
  - Suche nach Dateien

SYNerity

Integrität von Dateien

- Eigene Referenz-Systeme bereithalten
- Datenbanken mit verifizierten Hashcodes zu verschiedenen Unix-Versionen:
  - www.knowngoods.org (BSD, Solaris, Linux, Mac)

SYNerity

Rootkit entdecken

- Rootkit = Trojanisches Pferd für Unix
  - Betriebssystem liefert keine verläßlichen Informationen über Dateien,
- Entdecken über
  - RootkID, rk.cyberabuse.org
  - chkrootkid, www.chkrootkid.org

SYNerity

Fire-CD

- http://home.comcast.net/~fire.disk/
- Statische Binaries für
  - Linux
  - Solaris
  - Windows
- Checkrootkit
- Virenscanner F-Prot
- Autopsy, TCT, TCTUtils

SYNerity

TCT

- grave-robber
  - Analysiert MAC-Zeiten
  - Ergebnis wird in Datei body gespeichert
- ils
  - Zeigt Informationen zu ungenutzten inodes an
- ils2mac
  - Speichert das Ergebnis von ils in Datei body
- mactime
  - Erstellt Zeitlinie über die Rechnernutzung

SYNerity

TCT

- unrm
  - “dd” für nicht zugewiesene Plattenbereiche
- lazarus
  - Versucht Datei-Fragmente zu identifizieren und klassifizieren (C-Code, e-Mail …)
- icat
  - Wie cat, statt Dateiname dient I-node als Referenz

TCTUTILS

- istat
  - Zeigt Informationen über einen I-node
  - Input kommt vom .dd-File
- bcat
  - Extrahiert einen Block Rohdaten
- find_inode
  - Zuordnung Block-Nr. Zu I-node

TCTUTILS

- fls
  - Wie ls, zeigt auch Directory-Einträge zu gelöschten Dateien
- find_file
  - Zuordnung I-node zu Filename

SYNerity

Autopsy

- Web-Interface zu TCT und TCTUTILs
- Analyse eines Falls bestehend aus
  - Knoten
  - dd-Images
- http://station:8888/autopsy

SYNerity

FTimes

- http://ftimes.sourceforge.net
- Commandline-Tool
- Steuerung über Konfigurations-Datei
- Kompliziert in der Handhabung

SYNerity