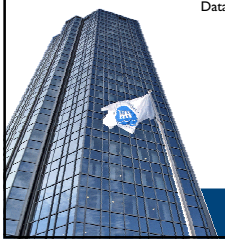
Datainsamling

Datautvinning från *NIX-system



Skapa ett respons-kit

- Unix-system/ Linux-system
  - oftast kompatibla vad gäller källkod
  - troligtvis inte kompatibla vad gäller körbara filer
  - kanske inte ens inom samma "familj"
- Du kan komma att bli tvungen att sätta upp ett likadant system som det som ska analyseras och kompilera på detta.
- (126)

Föreslagna verktyg

- ls
- find
- netstat
- strings
- more
- script
- dd
- icat
- pcat
- (127)
- truss
- gzip
- bash
- des
- lsof
- perl
- df
- last
- modinfo
- file
- md5sum
- ps
- vi
- vi
- w
- lsmod
- pkginfo
- netcat
- cryptcat
- strace
- cat
- rm
- ifconfig

Insamling av data - checklista

- Starta en betrodd kommandotollk
- Spara datum och tid
- Vem är inloggad?
- Spara filernas timestamps
- Detektera öppna portar
- Koppla processer mot portar
- Lista körande processer
- Lista uppkopplingar
- Spara datum och tid
- Logga vad som gjorts
- Spara checksummor
- (128)

Borttagna filer

- Metoden för att ta bort filer i *NIX är att avlänka dem.
- Avlänkade filer är lätta att återställa
- Finns en förteckning över avlänkade filer
- Det går att rädda filerna även om de raderats, men att återställa avlänkningen är lättare
- Detta gäller ext2. Trots vad du kan läsa på Internet så går även ext3 att återställa under vissa förutsättningar, men kråglar till det för oss redan från att filen raderats.
- (130)

Datum och tid

- date
- (131)

Vem är påloggad

- w
- (131)

Tidsstämplar hos filerna

- ls –alRu / > /mnt/extern/atime
- ls –alRc / > /mnt/extern/ctime
- ls –alR / > /mnt/extern/mtime
- (132)

Nätverk & portar

- netstat –an
- netstat –anp
- (133)

Dokumentera körande processer

- ps -aux
- (135)

Dokumentera vad som gjorts

- script /mnt/extra/command_log.txt
- md5sum /mnt/extra/* > /mnt/extra/md5sums.txt
- (137)

Automatisera!

Identifiera kända problem

- ”root kits”
- Kernelmoduler (moduler)
- Överskrivna kommandon
- (138)

Dumpa loggar

- /var/log
- /var/adm
- w – utmp
- last – wtmp
- lastlog – lastlog
- … - lastcomm
- Webtrafik - /var/log/httpd/access_log
- Överföringsloggar
- Historiker
- Kolla /etc/syslog.conf
- (140)

Dokumentera konfigurationsfiler

- /etc/passwd
- /etc/shadow
- /etc/groups
- /etc/hosts
- /etc/hosts.equiv
- ~/.rhosts
- /etc/hosts.allow , /etc/hosts.deny
- /etc/syslog.conf
- /etc/rc
- crontabs
- /etc/inetd.conf , /etc/xinetd.conf
- (141)

Nätverkskortet

- Om nätverkskortet används för sniffning så måste det vara i promiskuös mode.
  - Men ej om man bara loggar.
- Kolla med ifconfig
- Symptom -> sniffare måste logga data = stora datafiler som växer
- (142)

/proc

- All processinfo
- Demo
- (144)

Dumpa volatilt minne

- /proc/kmem
- /proc/kcore
- Svårt att analysera – men har man tur så står saker där i klartext
- Relaterat – swap.
- (147)

Varför Unix?

- I huvudsak serversidan
- Linux i företagsmiljöer ökar
- Linux i hemdatorer ökar
- (inbyggda system)
- (148)