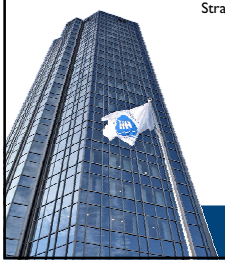
Analys

Strategi för UNIX-system



Wecksten, Mattias
2009

Översikt

- Kontroll av loggar
- Nyckelordssökningar
- Kontroll av relevanta filer
- Kontroll av ej autentiserade användare/grupper
- ”Skumma” processer
- Kontroll av otillåtna accesspunkter
- Analys av accessberoenden
- Moduler/rootkits

- (336)

Wecksten, Mattias
2009

Loggar

- Slå på (/etc/syslog.conf)
- Logga till fjärrserver
- Kapslad loggning
- Applikationsspecifika loggar
- su/sudo
- Användarlogg/logon-logg
- Cron
- Processföljning/ skalhistorik

- (338-342)

Wecksten, Mattias
2009

Strängsökningar

- grep
- skapa en uppsättning med ”heta” ord
  - root
  - PROMISC
  - password
  - /dev/sd#
- find
  - utför en grep för filnamnet
  - (343-344)

Viktiga filer

- Lista filer i ett visst tidsintervall (m/a/c)
- SUID/SGID
- Gömda filer (filnamnet börjar med .)
- Konfigurationsfiler
- Uppstartsfiler
- /tmp
- (347-350)

Användare/ grupper

- /etc/passwd
- /etc/groups
- Spåra ändringar
- Okänt system
  - Analysera privilegierna
  - (350-351)

”Skumma” processer

- Flera småsaker som inte stämmer?
- Körs på fel sätt?
- Ligger i fel folder?
- Har fel storlek/innehåll?

- (351)

Accesspunkter

- NFS
- telnet
- finger
- rlogin
- xserver
- ftp
- telnet
- dns
- sendmail
- snmp
- imap
- pop
- http
- https
- …

- (352)

Förtroendekedjor

- rhosts
- /etc/hosts.equiv

- Avtagande
- Delat nätverkssegment = implicit förtroende
  - Vanligt med helt switchade nät.
  - arpredirect

  - (352-353)

Trojaner/ rootkits

- Infekterat system
  - Kan leda till att din verktygslåda blir lurad
  - Jämför med extern verifikation av samma kommando
- chkrootkit
- kstat
- Kräver ofta expertkunskap så lösningen blir troligtvis att detektera men inte dissikera.

- (355-358)