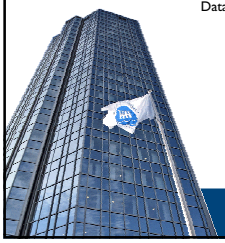
Datainsamling

Datautvinning från Windowssystem



Sammanställ din verktygslåda

- Kommandinterface
- Sessionshanterare
- Porthanterare
- Processhanterare
- Bibliotekshanterare
- Nätverksloggare
- Checksummagenerator
- Sharehanterare
- Loggverktyg
- Systemloggare

(97)

Verifiera verktygslådan

- Sammanställ på statiskt flyttbart media
- Måste man ha en verktygslåda per fall?
- Kontrollera beroenden
- Skapa checksummor

(99)

Spara information initialt

- Spara till lokal hårddisk
- Skapa en manuell hårdkopia
- Spara till flyttbart media
- Spara till fjärrdator

(100)

Bibehålla integriteten/ hemligheten

- Använd checksummor
- Kryptera data

(101)

Live-respons – volatil data

- Tid & datum
- Inloggade användare
- Tid och datuminformation för alla filer
- Lista över alla körande processer
- Lista över alla öppna portar
- Lista över processer som lyssnar på portar
- Lista över system som haft kontakt med systemet som undersöks

(103)

Jobba i en säker miljö

- Använd dina egna säkra och kontrollerade verktyg
- Var säker på att det är dessa du använder

(105)

Demonstration av inhämtning

- Datum och tid
- Kontrollera användarna
- Dokumentera filstatus
- Dokumentera öppna portar
- Dokumentera körande processer
- Dokumentera historik

(105-113)

Automatisera!

- Demonstration

(114)

Vad händer sedan?

- Gå på djupet
- Levande data
- Vad händer UNDER inhämtningen?

(115)

Lösenord och minne

- Hur funkar lösenord?
- När behövs lösenord?
- Hur knäcker man lösenord?
- Hur går man runt lösenord?
- Det volatila minnet (RAM) innehåller mycket intressant information
  - Ofta i klartext

(122)

Forensisk duplicering

- ”Byte för byte, bit för bit”
- När behövs det?
- Om du är osäker, ta en kopia.
  - Du behöver ju inte använda den
- (123)

Förbered

- Sätt samman en egen forensisk verktygslåda.
  - Utgå från förslagen i boken
  - Samarbeta gärna i hela klassen
  - Glöm inte att generera checksummor och kontrollera beroenden

Valfria fördjupningsuppgifter
- Läs fördjupning om hur man knäcker lösenord
- Läs fördjupning om hur Rainbowtables fungerar
- Läs fördjupning om hur Sandman fungerar

Datautvinning från digitala lagringsmedia 2009
Weckstén, M.