Insamling av nätbaserade bevis

Avlyssning
Dataloggning

Målen med avlyssning

- Bekräfta eller avvisa en misstanke
- Samla in ytterligare bevis
- Verifiera, tex. omfattningen av en insats
- Identifiera andra inblandade parter
- Skapa en tidslinje

- (174)

Förutsättningar

- Vilket mål?
- Lagligt stöd?
- Verktyg – hårdvara och mjukvara
- Säkerhet, signalmässigt och fysiskt
- Placering av utrustning
- Utvärdering av systemet

Olika typer av avlyssning

- Händelsestyrd
- ”Trap & trace”
- Full kopia

- (175-176)

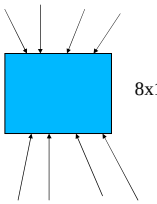
Konfigurera avlyssningsutrustning

- Syfte?
  - Hur mycket data ska loggas?
  - Hur fort?
- Hårdvara?
  - Processor
  - RAM
  - Hårddisk
- Mjukvara?
- Operativsystem?
  - NetBSD
- Fjärråtkomst?
  - VLAN
  - Krypering
- Dimensioneringsexempel

- (177-181)

Dimensioneringsexempel

- 8*100MBit/s=100MByte/s
- HDD=1.2TByte
- 1.2TByte/100MByte/s=12240s=3,4h



Att tänka på

- Silent sniffers
  - Mjukvara
  - Hårdvara
- Filformat
  - Öppna filformat
- (183)

Användning

- Inkoppling?
- SPAN
- Fysisk tillgång
- (184)

Utvärdering

- Diskanvändning
- Minnesutnyttjande
- Processorutnyttjande
- Inte bara i obelastat eller normalläge
  - Överbelasta och stresstesta
- (185)

Trap & trace – fånga och undersök

- tcpdump
- windump
- (186-190)

Full content

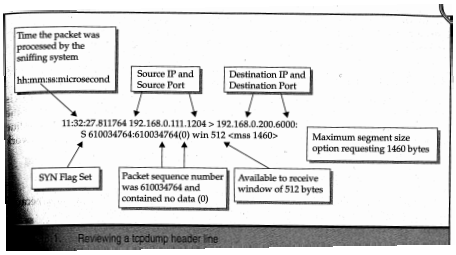
- Filtrering
  - Filtrera inte bort bevis
- Katalogisera
- (190-192)

Nätbaserade loggar

- Routrar, brandväggar, servrar …
  - Speciellt DHCP-servrar
- Nätet är vägen in och det är utmed denna väg som bevisen kan hittas.
  - Försök att spåra bakåt
- (193)

Tekniskt stöd

tcpdump



Reviewing a tcpdump header line

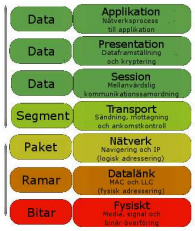
TCP-segment

TCP Header

Bit offset	Bits 0–3	4–7	8–15	16–31
0	Source port			Destination port
32	Sequence number			
64	Acknowledgment number			
96	Data offset	Reserved	CWR ECE URG ACK PSH RST SYN FIN	Window Size
128	Checksum			Urgent pointer
160	Options (optional)			
160/192+	Data			

- Källa: Wikipedia Licens: GFDL

Protokollstacken



- Källa: Wikimedia Commons Licens: sv:GFDL

Kodning/ modulering