Uge 13 - *audit & efterforskningsproces*

Emner

Ugens emner er:

- Efterforsknings proces.
- Linux audit system

Mål for ugen

Herunder kan du læse ugens forskellige mål

Praktiske mål

- At hver studerende har en grundlæggende viden efterforsknings processen
- Den studerende kan udføre audit logning med audit daemon
- At hver studerende har prøvet at opsætte en audit regel for en enkelt file.
- At hver studerende har prøvet at opsætte en audit regel for et directory.
- At hver studerende har prøvet at opsætte en audit regel for et system kald.

Læringsmål der arbejdes med i faget denne uge

Overordnede læringsmål fra studie ordningen:

- **Viden:**
  - Den studerende har viden om væsentlige forensic processer
  - Den studerende har viden om relevante it-trusler
  - Relevante sikkerhedsprincipper til systemsikkerhed
- **Færdigheder:**
  - Den studerende kan analysere logs for hændelser og følge et revisionsspor
- **Kompetencer:**
  - Håndtere udvælgelse, anvendelse og implementering af praktiske mekanismer til at dektekter specifikke it-sikkerhedsmæssige hændelser.

Øvelser

- Installation af Audit daemon
- Lav et audit for file ændringer i Linux
- Lav et audit for ændringer i et directory
- Lav et audit for system kald
- Lav en hash værdi ud fra en file
- (Først efter oplæg om efterforskningsprocess)Efterforskningsprocess & detection in depth

Skema

Tirsdag

Tid	Aktivitet
08:15	Introduktion til dagen
08:30	Oplæg om Audit daemon (AuditD)
08:45	Øvelser med AuditD
09:45	Pause
10:00	Øvelser med AuditD forsat
10:20	Oplæg om efterforsknings processer
10:40	Gruppe øvelse: Efterforskningsprocesser
11:15	Opsamling på øvelse om efterforskningsprocess
11:30	Lektion slut

2025-04-03 05:55:59