Uge 12 – Logning i Linux og introduktion til detektering

I denne uge arbejdes der videre med **logning som fundament for systemsikkerhed**.
Fokus er på, hvordan logs genereres, struktureres, roteres og beskyttes i Linux – og hvordan disse logs senere kan anvendes til **detektering og overvågning** i et SIEM-system som Wazuh.

Ugen bygger direkte videre på uge 11, hvor der blev arbejdet konceptuelt med *hvornår* og *hvorfor* der skal logges, og omsætter nu dette til **konkret teknisk praksis**.

Forberedelse

- Se kolonen *Forberedelse og pædagogisk tilrettelæggelse* i planen på It's learning

---

♂ Øvelser

- Introduktion til Linux logsystem
- Introduktion til rsyslog
- Opsætning af rsyslog-regler
- Logrotation i Linux
- Nedlukning af logindsamling
- Applikationslogs
- Opsætning af windows server 2022
- Introduktion til logning i windows
- Introduktion til microsoft sysmon
- Analyse af bruteforce angreb på windows

Eftermiddags øvelse

- Opsætning af Wazuh-agent
- Detektering med Wazuh – PoC (gruppeøvelse)

Læringsmål der arbejdes med i faget denne uge

Overordnede læringsmål fra studieordningen

Viden

Den studerende har viden om:

- Relevante it-trusler
- Relevante sikkerhedsprincipper til systemsikkerhed
- Logning som grundlag for overvågning og detektering

Færdigheder

Den studerende kan:

- Implementere systematisk logning og monitorering af enheder *(påbegyndt)*
- Analysere logs for incidents og følge et revisionsspor *(påbegyndt)*

Kompetencer

Den studerende kan:

- Udvælge og anvende praktiske mekanismer til at detektere it-sikkerhedsmæssige hændelser

---

Praktiske mål for ugen

- Den studerende kan redegøre for, hvad der bør logges
- Den studerende har kendskab til Ubuntu/Linux logningssystemer
- Den studerende kan udføre grundlæggende arbejde med Linux-logsystemet
- Den studerende forstår sammenhængen mellem logning og detektering

---

Afleveringer

- Ingen.

Skema

Tirsdag

Tid	Aktivitet
08:15	Introduktion til dagen og oplæg om logning
08:45	Øvelser med logning i Linux (samt introduktion til Wazuh)
11:20	Opsamling på dagen

Kommentarer

- Ugens fokus er at opbygge et **solidt logningsfundament**, som senere anvendes direkte i SIEM- og detektionsøvelser.
- Øvelserne danner grundlag for forståelse af, hvordan hændelser opdages, analyseres og dokumenteres.
- Erfaringerne fra denne uge anvendes direkte i senere arbejde med Wazuh, threat hunting og semesterprojektet.

Last update: 2026-03-20 13:58:28