

# ▮ Øvelse 48 – (Gruppeøvelse) Ubuntu CIS Benchmarks

## ▮ Formål

Formålet med denne øvelse er at give jer en grundlæggende forståelse for, hvad **CIS Benchmarks** er, og hvordan man kan bruge dem til at evaluere og forbedre sikkerhedskonfigurationen på et system. I skal som gruppe gennemføre en manuel mikro-revision af en Ubuntu-server og vurdere, hvorvidt systemet overholder de valgte benchmarks.

---

## ▮ Baggrund

**CIS Benchmarks** er konfigurationsstandarder og best practices, der bruges til at sikre, at systemer lever op til kravene i **CIS kontrollerne**. For hvert systemtype – fx Ubuntu Server, Apache HTTP Server, Kubernetes osv. – findes detaljerede anbefalinger til konfiguration.

CIS Benchmarks er knyttet til **CIS18-kontrollerne** og forklarer, hvordan man med konkrete systemindstillinger (safeguards) kan understøtte kravene. I denne øvelse arbejder I med Ubuntu-serverens benchmark.

Selvom der findes automatiserede værktøjer, gennemføres øvelsen **manuelt**, så I får dybere indsigt i processen.

Et eksempel på et automatiseret værktøj til test af operativ system for CIS compliance, er CIS-CAT som findes i både betalt, og gratis udgave. Derudover kan man også købe CIS hardende images som ud af æsken, lever op til kravene fra cis kontrollerne. Derudover findes der også *Host intrusion systemer* som understøtter løbende revisioner, såsom Wazuh, som vi arbejder med senere dette semester.

---

## ▮ Instruktioner

1. Hent dokumentet *CIS Benchmark for Ubuntu Linux Server* fra It's Learning (under dagens lektionsmaterialer).
2. Læs afsnittet *Overview*, og bemærk at alle handlinger i dokumentet forudsætter root-rettigheder (ikke sudo).
3. Udvalg én eller flere relevante benchmarks (fx inden for brugerstyring, netværk eller logning).

4. Brug en af jeres Ubuntu-serverinstanser til at gennemgå de valgte benchmarks.
5. Undersøg for hvert punkt under *Audit*-sektionen, om systemet overholder anbefalingen.
6. Notér afvigelser, hvor systemet ikke lever op til benchmarken.
7. Implementér evt. nødvendige foranstaltninger (fra *Remediation*-sektionen), og dokumentér ændringerne.
8. Diskutér jeres resultater og overvej, hvad der har størst betydning for systemets sikkerhed.

Øvelsen kan ses som en mini-CIS-complianceaudit – og kan bruges som inspiration til sikkerhedshærdning af systemer i projekter.

---

## □ Nyttige links

- [CIS Benchmarks – Officiel oversigt](#)
- [CIS Hardened Images](#)
- [CIS-CAT Pro Assessor - betalt værktøj til revision](#)
- [CIS-CAT Lite - Gratis værktøj til revision](#)

---

## □ Refleksionsspørgsmål

- Hvad er formålet med CIS Benchmarks, og hvordan adskiller de sig fra CIS18-kontrollerne?
- Hvordan kan man bruge benchmarks til at vurdere sikkerhedsniveauet på en server?
- Hvilke benchmarks gav anledning til de største afvigelser i jeres test – og hvorfor?
- Hvilke af de ændringer, I implementerede, havde størst sikkerhedsmæssig effekt?
- Hvad er konsekvensen af ikke at følge et benchmark?

---

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