Opgave 30 - Checksum af en fil

Formålet med øvelsen

Formålet med denne øvelse er at **forstå, hvordan checksums kan bruges til at verificere data-integritet**.
Ved hjælp af hashfunktioner kan man opdage selv de mindste ændringer i en fil, hvilket gør dem nyttige til **dataintegritet, sikkerhed og verifikation** af filer. Denne metode er blandt andet anvendt i efterforksningsprocesser, til at sikre at log filer ikke er blevet ændret.

Information

For at sikre integriteten af data benytter man ofte en **hashværdi** som checksum. Checksums bruges til:

- At verificere filers integritet efter overførsel eller lagring.
- At opdage uautoriserede ændringer i systemfiler.
- At kontrollere, om en fil er identisk med en referenceversion.

En **hashfunktion** anvendes til at generere en checksum. Hvis blot et enkelt tegn ændres i inputtet til en hashfunktion, bliver outputtet **helt anderledes**. Derfor er checksums en pålidelig metode til at opdage dataændringer.

Instruktioner

1. **Installer** `hashalot` (hvis den ikke allerede er installeret):

   ```
   sudo apt install hashalot
   ```

2. **Opret en testfil**, der indeholder teksten "Hej med dig":

   ```
   echo "Hej med dig" > testfil.txt
   ```

3. **Lav en checksum af filen** ved hjælp af SHA-256 hashfunktionen:

   ```
   sha256sum testfil.txt
   ```

4. Notér checksummen.
5. **Lav en ny checksum af filen**, og verificér, at den er identisk:

```
sha256sum testfil.txt
```

6. Checksummen bør være den samme, da filens indhold ikke har ændret sig.
7. **Tilføj et ekstra tegn** til teksten i filen:

```
echo "f" >> testfil.txt
```

8. **Generér en ny checksum**, og bemærk ændringen:

```
sha256sum testfil.txt
```

9. Da filens indhold er ændret, vil checksummen nu være helt anderledes.

Yderligere anvendelser

Checksums bruges bredt i IT-verdenen til: - **Digitale signaturer og kryptering**. - **Dataintegritet i backup- og gendannelsessystemer**. - **Bekræftelse af softwaredownloads** (f.eks. ISO-filer).

For at verificere en fil mod en kendt checksum kan du sammenligne værdien med en officiel kilde:

```
sha256sum -c checksumfil.txt
```

Checksum og logfil-integritet

I en **efterforskningsproces** er det afgørende at sikre, at **logfiler ikke er blevet manipuleret**. Checksums kan bruges til at: - Verificere, at en logfil ikke er blevet ændret mellem indsamling og analyse. - Dokumentere, at en bestemt fil er intakt og uændret under en efterforskning. - Sikre pålidelighed i retssager eller compliance-audits.

For at anvende checksums på en logfil:

```
sha256sum /var/log/audit/audit.log > log_checksum.sha256
```

For at verificere logfilens integritet senere:

```
sha256sum -c log_checksum.sha256
```

Hvis checksummen matcher, er logfilen uændret. Hvis den ikke gør, kan der være sket manipulation.

Links

- Hashalot-manualside
- SHA256SUM-manualside

2025-04-03 05:55:59