

DA-ODA2001: 2017/2018: Oblig 1

Thomas Nordli

September 11, 2017

Administrativt

- Innleveringen fremvises faglærer for godkjenning.
- Dere jobber *individuell* eller *parvis* dersom ikke annet er avtalt med faglærer.
- Bruk fortrinnsvis teknikker/språk som er gjennomgått i løpet av dette kurset for å løse oppgavene under. Spør faglærer dersom du er i tvil om hva som kan brukes.
- Innleveringen pakkes pent inn i en enkelt fil.
- Besvarelsene innleveres i Canvas.
- Innleveringsfrist settes i Canvas.

Studentene må *selv ta initiativ* til å vise besvarelsen til faglærer. Tilbakemelding gjøres muntlig av faglærer *i løpet av visningen*. Eventuell godkjenning registreres av faglærer i Canvas umiddelbart *etter visningen*. Dersom besvarelsen underkjennes må ny og forbedret versjon leveres og vises for ny vurdering. Husk at alle de obligatoriske oppgavene må være **godkjent innen to uker før eksamen**, for å kunne stille til eksamen.

Ikke nøl med å ta kontakt med faglærer for råd og veiledning underveis i arbeidet.

Oppgavetekst

Oppgave a) IDS

I denne oppgaven skal du lage to shell-skript som sammen fungerer som et IDS (Intrusion Detection System).

1. Lag et skript som lager SHA-summer av filer, og lagrer dem (sammen med filstiene) i en fil. Bruk et ferdig program for dette formålet, f.eks. `shasum(1)`.
 - Filen skal hete `hash.csv` og den skal være *semikolonseparert*.
 - Dersom filen finnes fra før skal den overskrives, slik at det opprinnelige innholdet forsvinner.
 - Filer skal oppgis som *absolutte filstier* og
 - skal overføres til skriptet som *argumenter*.

Tips: `tr(1)` og `sed(1)` kan brukes til å manipulere tekst.

2. Lag et annet skript som undersøker om innholdet i filene nevnt i `hash.csv` har endret seg siden `hash.csv` ble opprettet. Filstien skrives ut ved endring. Intet annet skrives.

Tips: `diff(1)` kan brukes til å sammenligne to filer.

3. Endre skriptene i 1. og 2. slik at det

- kjører på en android-enhet og
- rapportere hvilke av filene i katalogen `/sdcard` (ikke fra en brukarangitt liste som i 2.) som er endret
- i tillegg til skal den rapportere om eventuelle nyopprettede filer i katalogen.
- Tips:
 - (a) Bruk en enhet med `toybox` (Android 6.0 eller nyere) eller
 - (b) bruk appen `termux` (krever Android 5.0 eller nyere).

Dersom du ikke har en android-enhet, eller ikke ønsker å bruke den du har, så kan du bruke en virtuell android-enhet (som f.eks. er installert på lab'en).

b) Digitale signaturer

1. Generer et nøkkelpar og signer skriptetene fra a) ved hjelp av `gpg(1)`. Signaturene skal være i *separate filer* (en for hvert skriptet)
2. Gjør din offentlige nøkkel tilgjengelig på web ved å legge den (ASCII-armored) i filen `~/public_html/pub_key.asc` på debbie. (Hvis f.eks. *arne* gjør dette blir hans offentlige nøkkel bli tilgjengelig på `https://debbie.hbv.no/~arne/pub_key.asc`)

All informasjon om `gpg(1)`, som trengs for å løse denne oppgaven, finnes i første kapittel (Getting Started) av The GNU Privacy Handbook (<https://www.gnupg.org/gph/en/manual/c14.html>).