5. laboratorijska vježba

Napredno korištenje operacijskog sustava Linux

Robert Vežnaver

1. svibnja 2012.

Pričica

Evan Stone želi pri svakom pokretanju računala biti siguran da određene datoteke nisu mijenjane. Pomozite mu napraviti init skriptu koja će to raditi za njega.

Zadatak

U datoteci */etc/chksig.conf* postoji popis datoteka i njihovih SHA-1 hasheva. Na kraju datoteke */etc/chksig.conf* nalazi se RSA digitalni potpis svih gore navedenih podataka.

Napisati init skriptu koja za datoteke navedene u */etc/chksig.conf* provjerava jesu li one mijenjane. Također, skripta mora provjeriti i digitalni potpis unutar datoteke da se utvrdi integritet navedenog popisa (ključeve sami generirate).

Ukoliko datoteka */etc/chksig.conf* ne postoji ili je digitalni potpis kriv ili je ijedan od hasheva različit od izračunatog potrebno je iz skripte izaći s greškom (kod 2) i odgovarajućom porukom (po volji). U suprotnom, iz skripte se izlazi kodom 0 i porukom "OK".

Primjer ulaza

/etc/chksig.conf:

```
-----BEGIN PGP SIGNED MESSAGE-----
/bin/cat 6039aaff9276c3ce71f99137c4dfc55393825ebc
/bin/ls d3e5fb0c582645e60f8a13802be0c909a3f9e4d7
-----BEGIN PGP SIGNATURE-----
Version: GnuPG vX.Y.Z

TestTestTestTestTestTestTestTestTestTestPotpisPotpisPotpisPotpisPotpisPotpis
PotpisPotpisPotpisPotpisPotpisPotpisPotpisPotpisPotpisPotpisPotpisPotpisPo
tpisTestTestTestTestTestTestTestTestTestTest=
-----END PGP SIGNATURE-----
```

Primjer izlaza

```
OK
```