

Mérési utasítás 3.

(Protokollok és szoftverek I.)

A gyakorlat célja:

Az Berkeley r* és ssh programok megismerése, ismerete.

Szükséges előismeret:

Unix alapok és minden, ami az előadásokon elhangzott.

Feladatok:

Jelentkezzen be diak felhasználóként (login/pass: diak/diak)!

1. r-* megismerése.

- 1.1 Győződjön meg róla, hogy a gépén nem léteznek az alábbi fájlok: ~/.rhosts /etc/hosts.equiv.
(*ls ~/.rhosts /etc/hosts.equiv*)
- 1.2 Hozza létre a .rhosts fájlt, hogy a szemben lévő gépről a diak felhasználó be tudjon jelentkezni az Ön gépére. (*echo „velemszembenlevogepnev” > .rhosts*)
- 1.3 Jelentkezzen be, a szemben lévő gépre, diak felhasználóként az rlogin parancs segítségével. Hajtson végre egy parancsot, majd lépjen ki, az exit, logout vagy a <CTRL>+<D> billentyűkombináció segítségével. (*rlogin gépnév*)
- 1.4 Hajtson végre egy olyan parancsot a távoli gépen rsh segítségével, ami bizonyossá teszi, hogy a parancs valóban nem a saját gépén futott le. Pl.: listázza ki ifconfig segítségével az ipcímet. (*rsh gépnév ifconfig eth0*)
- 1.5 Hozzon létre a saját gépén, egy üdvözlő tartalmú fájlt, a fájl neve tartalmazza a saját gépének nevét, majd rcp segítségével másolja a szemben lévő távoli gépre, rsh segítségével győződjön meg valóban átmásolta a fájlt. (*echo „szia” > engepamneve-udvozlet.txt; rcp engepamneve-udvozlet.txt tavoligep:/ahova/masolni/akarom; rsh tavoligep ls /ahova/masolni/akarom*)
- 1.6 Törölje a .rhosts nevű fájlt.

2 SSH, SCP megismerése

- 2.1 Győződjön meg róla, hogy a gépén nem léteznek az alábbi fájlok: ~/.ssh/{authorized_keys,id_dsa,id_dsa.pub} (*ls ~/.ssh/{authorized_keys,id_dsa,id_dsa.pub}*)
- 2.2 ssh program segítségével lépjen be az Önnel szemben lévő számítógépre, majd hajtson végre parancsokat. (*ssh -l felhasznalonev gepnev* vagy *ssh felhasznalonev@gepnev*)
- 2.3 ssh segítségével, hajtson végre távolról parancsokat a szemben lévő gépen. (*ssh -l felhasznalo gepnev „parancs”*)
- 2.4 scp parancsal másoljon fel egy üdvözlő szöveget a szemben lévő gépre. (*scp mitmasoljak felhasznalo@gepnev:/hova/masoljak*)

2.5 ssh-keygen segítségével generáljon public és private, kulcspárokat, majd scp segítségével a publikus kulcsot másolja fel a távoli gép .ssh könyvtárába authorized_keys néven. (*ssh-keygen -b 1024 -t dsa; scp .ssh/id_dsa.pub felhasználó@gepnev:~.ssh/authorized_keys*)

2.6 ssh segítségével lépjen be a ta132k5.tilb.sze.hu számítógépre, a felhasználónév a saját neve amit a neptunba megadott, kis,ékezet nélküli betűkkel egybeírva, ha Ifj. szerepel akkor az is a név része (a pont is). A jelszava a neptunkódja nagy betűkkel. Sikeres login után generáljon új 10 karakter hosszú jelszavat a pwgen segítségével. (*ssh -l felhasználonev ta132k5.tilb.sze.hu; pwgen -n 10*)

2.7 Lépjen ki a ta132k5.tilb.sze.hu számítógépből.