Kimenő hálózati kapcsolatok védelme

Számítástechnika tanár szak
Rendszertechnika II.
előadás

Védtelen és védett kimenő kapcsolatok

- Titkosítás nélküli megoldások
  - A hálózaton az adatforgalom elfogható és értelmezhető
    - telnet, ftp, rlogin, rcp stb.
- Az SSH protokoll
  - SSH: Secure Shell
  - Számos hálózati feladathoz nyújt megfelelő tehnológiát
  - OpenSSH: szabadon elérhető SSH
  - Szinte minden linux disztribúció tartalmazza

OpenSSH programok és állományok

Kliensprogramok	
ssh	távoli bejelentkezés, távoli parancsvégrehajtás
scp	állományok másolása két számítógép között
sftp	ftp-hez hasonlító interaktív megoldás a gépek között titkosított állománycserére
Szerverprogramok	
sshd	az SSH szerverdémon
Titkosító kulcsok előállítására és kezelésére szolgáló programok	
ssh-keygen	nyilvános és titkos kulcsok létrehozására, módosítására
ssh-agent	saját SSH kulcsok tárolására, a jelszavak begépelésének elkerülésére
ssh-add	az ssh-agent által kezelt kulcsok manipulálására
Állományok és könyvtárak	
~/.ssh	a felhasználó kulcsait és SSH beállításait tartalmazó könyvtár
/etc/ssh	a teljes rendszerre érvényes kulcsokat és konfigurációkat tartalmazó könyvtár
~/.ssh/config	a felhasználó által használt kliens konfigurációs állománya
/etc/ssh/ssh_config	a teljes rendszerre érvényes kliens konfigurációs állomány

Az ssh és az scp használata

- Távoli bejelentkezés
  `ssh -l távoli_felhasználó távoli_kiszolgáló`
  `ssh távoli_felhasználó@távoli_kiszolgáló`
  Például: `ssh c-ta@iatt.ttk.pte.hu`
- Távoli parancsvégrehajtás
  `ssh -l ruser rhost command`
  Például: `ssh -l c-ta iatt.ttk.pte.hu w`
- Állományok másolása
  `scp állomány távoli_kiszolgáló:távoli_állomány`
  `scp távoli_kiszolgáló:távoli_állomány állomány`

Távoli programok futtatása

- Interaktivitást nem igénylő programok esetén
  `ssh -l ruser rhost command`
  Például: `ssh -l c-ta iatt.ttk.pte.hu w`
- Interaktivitást igénylő programok esetén
  `ssh -t -l ruser rhost command`
  Például: `ssh -t -l c-ta iatt.ttk.pte.hu vi`
- X Window programok esetén
  `ssh -X -f -l ruser rhost command`
  Például: `ssh -X -f c-ta@iatt.ttk.pte.hu xterm`
  (`/etc/ssh/sshd_config X11forwarding yes | no`)

Távoli állományok másolása

- Egy állomány másolása
  `scp állomány távoli_kiszolgáló:`
  `scp távoli_kiszolgáló:állomány .`
- Egy állomány másolása más néven
  `scp állomány távoli_kiszolgáló:másolat`
  `scp távoli_kiszolgáló:állomány másolat`
- Több állomány másolása
  `scp állomány* távoli_kiszolgáló:`
  `scp távoli_kiszolgáló:állomány\* .`

Távoli állományok másolása

- Másolás könyvtárba

```
scp állomány távoli_kiszolgáló:dir/subdir
scp távoli_kiszolgáló:dir/subdir/állomány .
```

- Rekurzív másolás más felhasználónéven

```
scp -r könyvtár user@távoli_kiszolgáló:
scp -r user@távoli_kiszolgáló:könyvtár .
```

- Attribútumok megőrzése

```
scp -p állomány* távoli_kiszolgáló:
scp -p távoli_kiszolgáló:állomány\* .
```

Állományok tükrözése

- Biztonságos tükrözés az scp használatával
  - `scp -pr` parancs használatával
  - hátrányai:
    - az scp automatikusan követi a szimbolikus linkeket
    - minden állományt másol (akkor is ha már létezik)
- Az rsync és az scp kombinálása
  - optimalizált, szimbolikus linkek követése nélkül
  - `rsync -a -e ssh dir1 távoli:dir2`
  - `rsync -a -e ssh -v --progress dir1 távoli:dir2`

Hitelesítés nyilvános kulccsal OpenSSH szerver és kliens között

- Kulcsok helyének előkészítése ha szükséges

```
mkdir -p ~/.ssh
chmod 700 ~/.ssh
```

- Szükséges kulcsok generálása

```
cd ~/.ssh
ssh-keygen -t dsa
```

- A nyilvános kulcs másolása a távoli kiszolgálóra

```
scp -p id_dsa.pub user@távoli_kiszolgáló:
```

Hitelesítés nyilvános kulccsal OpenSSH szerver és kliens között

- A nyilvános kulcs telepítése a távoli kiszolgálón

```
mkdir -p ~/.ssh
chmod 700 ~/.ssh
cat id_dsa.pub >> ~/.ssh/authorized_keys
chmod 600 ~/.ssh/authorized_keys
```

- Belépés a távoli kiszolgálóra
  - Hitelesítés a nyilvános és titkos kulcs alapján
  - Jelszó megadását nem igényli

```
ssh user@távoli_kiszolgáló
```

Az ssh-agent

- Szeretnénk elkerülni minden egyes bejelentkezéskor a jelszó megadását
- Az ssh-agent közvetítő indítása

```
eval `ssh-agent`
```

- Kulcsok hozzáadása a közvetítőhöz

```
ssh-add
```

- Bejelentkezés jelszó nélkül a távoli gépekre

```
ssh user@távoli_kiszolgáló
```

Az ssh-agent

- Kulcsok hozzáadása az ssh-add segítségével
  - `ssh-add` – alapértelezett kulcsok hozzáadása
  - `ssh-add ~/.ssh/kulcs1` – kulcs1 hozzáadása
- Kulcsok eltávolítása
  - `ssh-add -D` – minen kulcs eltávolítása
  - `ssh-add -d ~/.ssh/kulcs1` – kulcs1 törlése
- Az ssh-agent működése
  - csak addig használhatjuk amíg ki nem jelentkezünk
  - ismételt bejelentkezéskor újra meg kell adni a kulcsokat
  - keychain …

Az SSH kulcsok előnyei

- Nagyobb biztonság a jelszavaknál
  - A titkos kulcsot soha nem továbbítjuk a hálózaton a (titkosított) jelszavakkal ellentétben
  - A kulcsok tárolása titkosított is lehet, így ellopásuk esetén sem használhatók fel, ellentétben egy jelszóval
  - Nem kell minden egyes bejelentkezésnél a hitelesítéssel bajlódnunk, ez automatikusan megtörténik a kulcsok segítségével

Nyílt szöveges kulcsok

- Használatuk általában nem szerencsés
  - A kulcsokat tartalmazó állomány ellopása komoly problémát jelentene
- Az emberi beavatkozástól mentes folyamatoknál (kötegelt feladatok, cron feladatok) szükséges lehet
- Szűkíteni kell a kulcs felhasználásának lehetőségeit
  - Csak az általunk engedélyezett parancs(ok) legyen(ek) végrehajtható(k) a kulccsal

Nyílt szöveges kulcsok a gyakorlatban

- Nyílt szöveges kulcsok készítése
  `ssh-keygen -t dsa -f key2 -N ""`
- Kulcs telepítése a kiszolgálón
- Kényszerparancs megadása a kiszolgálón
  - `command="/usr/bin/uptime" ssh-dss AAAAB3NzaC1kc …`
- Egyéb lehetőségek tiltása
  - `no-port-forwarding, no-X11-forwarding, no-agent-forwarding, no-pty, from="kliens.pte.hu", command="/usr/bin/uptime" ssh-dss AAAAB3NzaC1k …`
- A kulcs felhasználása
  - `ssh -i key2 távoli_kiszolgáló`

OpenSSH és SSH Secure Shell

- SSH1 esetén kompatibilisek
- SSH2 esetén eltérő állományformátumok
- A nyilvános kulcsok formátuma
  - OpenSSH esetén:

```
ssh-dss AAAB3NzaC1kc3MAAAC …
ssh-rsa AAAB3NzaC1kc3MAAAC …
```

  - SSH Secure Shell esetében:

```
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1kc3MAAACBAJNN2CbURaTm7oW5F2Z …
---- END SSH2 PUBLIC KEY ----
```

OpenSSH és SSH Secure Shell

- Nyilvános kulcsok telepítése
  - OpenSSH
    - `~/.ssh/authorized_keys` állományban
  - SSH Secure Shell
    - `~/.ssh2` könyvtárba másolva
    - `~/.ssh2/authorization` állományban hivatkozva
- Titkos kulcsok
  - OpenSSH
    - Nincs megkötés
  - SSH Secure Shell
    - `~/.ssh2/identification` állományban hivatkozva

OpenSSH és SSH Secure Shell

- OpenSSH kulcs exportálása SSH2 formátumú nyilvános kulccsá

```
ssh-keygen -e -f id_dsa > mykey-ssh2.pub
```

- SSH2 nyilvános kulcs élesítése

```
mv mykey-ssh2.pub ~/.ssh2/
echo "K1 mykey-ssh2.pub" >>authorization
```

- SSH2 titkos kulcs átalakítása OpenSSH formára

```
cp -p is_dsa_ssh2 kulcs_másolat
ssh-keygen2 -e kulcs_másolat
ssh-keygen -i -f kulcs_másolat > imp_ssh2_key
ssh-keygen -p imp_ssh2_key
```

Az SSH bejelentkezés egyszerűsítése

- Kiszolgálói alias-ok készítése a ~/.ssh/config állomány használatával
- ~/.ssh/config

```
Host akarmi
 HostName akarmi.akarhol.hu
 User root
 IdentityFile ~/.ssh/akarmikey_dsa
 Port 33333
 Protocol 2
```

Az SSH kliens alapértelmezett beállításai

- Kiszolgálói alias a ~/.ssh/config állományban "*" néven
- Ha ez az első bejegyzés, minden mást felülír
- Ha ez az utolsó bejegyzés, akkor csak tartalék szerepet tölt be
- Például

```
Host *
  User c-ta
Host iatt.ttk.pte.hu
  User root
  Port 3453
Host *
  Protocol 2
```

SSH alagutak készítése

- Nem biztonságos TCP kapcsolatok alagúton történő továbbítása, SSH használatával
- Alagút létrehozása
  - `ssh -f -N -L helyi_port:localhost:távoli_port távoli_kiszolgáló`
- Az adatok áramlásának folyamata
  - az alkalmazás adatokat küld a helyi_port-ra
  - a helyi SSH kliens olvassa a portot, titkosítja az adatokat és az alagúton keresztül elküldi a távoli SSH szervehez
  - a távoli SSH szerver dekódolja az adatokat és helyben továbbítja a távoli_port értékével megadott portra