SSH

Távoli elérés biztonságosan

- A telnet, rcp, rsh, rlogin titkosítás nélkül továbbítja az információt
- SSH – Secure Shell
- Kereskedelmi vált.: SSH Tectia
- Szabad vált.: **OpenSSH** (main Ubuntu tároló)
- Hitelesítés nyilvános/titkos kulcspáros alapú megoldással vagy egyes szolgáltatások esetén Kerberos kiszolgáló segítségével (Kerberos tikett)

Hitelesítés

- A kulcshozzáférést külön jelszóval is korlátozhatja
- Először a hoszt hitelesítése, majd a felhasználó hitelesítése
- A további információáramlás már a kiszolgáló és az ügyfél által közösen választott (vagy előre meghatározott) algoritmussal
- Nyilvános kulccsal titkosít a kiszolgáló

Kiszolgáló

- Kiszolgáló telepítése
  - sudo apt-get install openssh-server -y
- Kiszolgáló indítása, leállítása, újraindítása, állapota
  - sudo service ssh start|stop|restart|status
- A 22-es porton várja a kéréseket
- Nyilvános kulcsot a ~/.ssh/authorized_keys állományhoz kell hozzáadni

Kiszolgáló konfigurálás

/etc/ssh/sshd_config

- Port 22 (ez az alapért., de célszerű mást beállítani 1024… 49152, pl. 2222)
- Üdvözlőszöveg, figyelmeztetés, stb.
  - Banner /etc/issue.net
- Az autentikáció történhet jelszó vagy SSH kulcs alapon*
- Jelszó alapú letiltása:
  - PasswordAuthentication no
- Nyilvános kulcs alapú:
  - PubkeyAuthentication yes
  - RSAAuthentication yes

Konfigurálás

- Távoli asztal, grafikus alkalmazások, stb. engedélyezése a kapcsolaton
  - AllowTcpForwarding yes
  - X11Forwarding yes
- Mely felhasználói fiókok/csoportok használhatják
  - AllowUsers hallgato geza
- Mely felhasználói fiókok/csoportok nem használhatják
  - DenyUsers jeno istvan

Tűzfal

- Tűzfal profil települ:
  /etc/ufw/applications.d/openssh-server

```
[OpenSSH]
title=Secure shell server, an rshd replacement
description=OpenSSH is a free implementation of the Secure Shell protocol
.
ports=22/tcp
```

- sudo ufw allow OpenSSH

OpenSSH átngedése a tűzfalon

```
root@ubuntu-server:/# ufw allow OpenSSH
Rule added
Rule added (v6)
root@ubuntu-server:/# ufw status
Status: active

To                         Action      From
--                         ------      ----
Anywhere                   ALLOW       192.168.1.0/24 2049
Anywhere                   ALLOW       192.168.1.0/24 8975
Anywhere                   ALLOW       192.168.1.0/24 111
Anywhere                   ALLOW       192.168.1.0/24 8976
Anywhere                   ALLOW       192.168.1.0/24 Samba
137                        ALLOW       192.168.1.0/24
138                        ALLOW       192.168.1.0/24
139                        ALLOW       192.168.1.0/24
445                        ALLOW       192.168.1.0/24
OpenSSH                    ALLOW       Anywhere
OpenSSH (v6)               ALLOW       Anywhere (v6)
```

Ellenőrzés

- Fut-e? ps -A | grep sshd
- Milyen porton várja a kéréseket? ss -lnp | grep sshd

```
root@ubuntu-server:/etc/ssh# ss -lnp | grep sshd
LISTEN     0      128                        :::22                      :::
*      users:(("sshd",11409,4))
LISTEN     0      128                         *:22                       *:
*      users:(("sshd",11409,3))
root@ubuntu-server:/etc/ssh# _
```

- Helyi bejelentkezés: ssh -v localhost

```
d6:06
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is d4:49:70:d8:54:2d:23:31:65:7e:9d:c0:5d:44:d6:06.
Are you sure you want to continue connecting (yes/no)? yes_
```

Ellenőrzés

- Fogad-e kapcsolatot?
  - sudo netstat --inet -lpn | grep sshd
  - tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN <PID>/sshd

Ügyfélgép

- Ügyfélszoftver telepítése
  - sudo apt-get install openssh-client
- Kulcsok létrehozása RSA vagy DSA titkosítással
- ssh-keygen -t rsa|dsa
- Kulcsok: ~/.ssh/id_rsa.pub és ~/.ssh/id_rsa
- Titkos kulcsok betöltése a memóriába
  - ssh-add -l

Kulcsok generálása

```
hallgato@ubuntu-server:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/hallgato/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/hallgato/.ssh/id_rsa.
Your public key has been saved in /home/hallgato/.ssh/id_rsa.pub.
The key fingerprint is:
a5:35:0a:8e:8e:50:63:88:c4:82:46:df:42:3f:bc:23 hallgato@ubuntu-server
The key's randomart image is:
+--[ RSA 2048]----+
|+o .             |
|=+o +            |
|= +o =.   +      |
| o ..oo. = .     |
|.  E.o. S        |
| . o. .          |
|  . .            |
|                 |
|                 |
+-----------------+
```

Ügyfélprogramok

- **ssh** – parancssori és grafikus (-X kapcsoló) távoli kapcsolatoknál
  - ssh felhasznnálónév@gépnév
- **scp** – fájlok másolása gépek között. Pl. helyi gépről távoli gépre
  - scp forráfájl felh@gépnév:/könyvtár/célfájl
  - -r egész könyvtár másolható
- **sftp** – a kiszolgálón sftp-server kell fusson (SSH File Transfer Protocol)
  - sftp gépnév
- **ssh-copy-id** – nyilvános kulcs átmásolása a kiszolgálóra
  - ssh-copy-id felhasználó@gépnév