SSH na Linuxe – Poznámky

*Základy SSH čo to je a ako funguje*

* SSH (Secure Shell) je **protokol na bezpečnú vzdialenú správu počítača v textovom režime**.  
   Prebieha cez port 22 - default pre SSH
* Verzie SSH:   
   SSH-1 (zastaral),   
   SSH-2 (aktuálna)
* Používané šifrovanie:  
   Asymetrické (autentizácia) – verejný/súkromný kľúč  
   Symetrické (dátový prenos) – Používa jeden spoločný kľúč  
   Po autentizácii sa vytvorí a dohodne tento kľúč (napr. cez Diffie-Hellman)  
   Tento kľúč sa potom používa na šifrovanie dátovej prevádzky
* Vlastnosti bezpečnej komunikácie:   
   Dôvernosť  
   Integrita  
   Autentickosť pôvodu dát

*Autentizácia v SSH*

* Založená na kľúčoch: (asymetrické)  
   **Server má súkromný a verejný kľúč.**  
   **Klient si stiahne verejný, zašifruje ním správu, server ju dešifruje súkromným.**
* Autentizácia môže prebiehať cez:  
   **meno + heslo** (menej bezpečné)  
   **verejný kľúč** (doporučené!)
* Priečinky a súbory:  
   ~/.ssh/authorized\_keys → verejné kľúče, ktoré môžu pristupovať  
   .ssh = 700, authorized\_keys = 600 → práva

*Konfiguračné súbory*

| /etc/ssh/ssh\_config | nastavenie klienta |
| --- | --- |
| /etc/ssh/sshd\_config | nastavenie servera |
| /etc/ssh/ssh\_host\_\*\_key | rôzne druhy súkromných kľúčov servera |

~/.ssh/known\_hosts klient si tu ukladá verejné kľúče serverov, na ktoré sa pripojil

*Prenos súborov*

* scp (Secure Copy) – funguje ako cp, ale cez SSH

| **Príkaz** | **Vysvetlenie** |
| --- | --- |
| scp file.txt user@server: | Pošle file.txt do domovského priečinka na serveri |
| scp -r folder user@server: | Pošle priečinok folder |
| scp file user@server:/tmp/ | Pošle súbor do /tmp |
| scp user@server:/tmp/file.txt . | Stiahne súbor z /tmp do aktuálneho priečinka |
| scp file user@server:file2.txt | Pošle súbor a zároveň ho premenuje na serveri |

* sftp (SSH File Transfer Protocol) – Interaktívna alternatíva SCP  
   Po prihlásení pracuješ v prostredí sftp>  
   put, get, lls, lpwd, lcd, lmkdir, cd, pwd

| **Príkaz** | **Význam** |
| --- | --- |
| put file.txt | Nahraje súbor na server |
| get file.txt | Stiahne súbor zo servera |
| cd priecinok | Zmení priečinok na serveri |
| lcd priecinok | Zmení priečinok u teba (lokálne) |
| lls | Vypíše tvoje súbory |
| lpwd | Zobrazí tvoju aktuálnu cestu |
| lmkdir nový | Vytvorí priečinok u teba |

* Grafické nástroje:  
   Linux: Nautilus, Midnight Commander, gFTP  
   Windows: WinSCP, FileZilla (s FTP, SFTP, SCP podporou)

*Spúšťanie grafických aplikácií cez SSH*  
- Pomocou prepínača ssh -X (X11 forwarding)  
 Na Windows treba nainštalovať X server (napr. Xming)  
  
- V sshd\_config musí byť X11Forwarding yes

*Bezpečnosť a logy*  
- fail2ban - ochrana proti brute-force, sleduje pokusy o login  
 ochrana pred opakovanými pokusmi o prihlásenie – blokuje IP po niekoľkých zlých heslách  
 fail2ban-client status ssh  
- Logy login pokusov:  
 tail -f /var/log/secure

*ssh-agent* - **Funguje ako „správca odomknutých kľúčov“**  
 - Beží na pozadí a keď mu raz zadáš passphrase, nemusíš ho zadávať stále  
 - Nevýhoda: ak ti ukradnú PC, môžu sa dostať všade

*Príkazy*

| **Príkaz** | **Vysvetlenie** |
| --- | --- |
| ssh user@server | Pripojí sa na vzdialený server ako user |
| ssh-copy-id user@server | Skopíruje verejný kľúč na server → umožní prihlásenie bez hesla |
| scp file user@server:/tmp | Skopíruje súbor do priečinka /tmp na serveri |
| scp user@server:/tmp/file ./ | Stiahne súbor z /tmp do aktuálneho priečinka |
| sftp user@server | Spustí interaktívny sftp prenos (bezpečné FTP cez SSH) |
| fail2ban-client status ssh | Zobrazí stav ochrany SSH proti bruteforce útokom |
| tail -f /var/log/secure | Sleduje login pokusy v reálnom čase (logy) |
| ssh-keygen -lf /etc/ssh/ssh\_host\_rsa\_key.pub | Zobrazí fingerprint verejného RSA kľúča servera (na overenie) |