SSH

Az SSH helyes használata

A hálózatra kötött számítógépek elterjedése óta mind inkább széles körben igény mutatkozott arra, hogy ezeket a gépeket az üzemeltetk (rendszergazdák), fejlesztk távolról is el tudják érni. Természetesen nem csak szerverekre lehet belépni távolról, hanem különböz hálózati eszközökbe (router, switch, stb.) is.

Ehhez az eléréshez többféle protokoll is használatban van/volt (RDP, TN3270, rlogin, telnet, http, https, stb.).

Az újabb igény a távoli elérésben az volt, hogy mindezt biztonságosan, valamilyen titkosítással érhessük el. Erre szolgál többek között az SSH (Secure Shell) protokoll.

Az SSH Protokoll

A **Secure Shell** (röviden: **SSH**) egy szabványcsalád, és egyben egy protokoll is, amit egy helyi és egy távoli számítógép közötti biztonságos csatorna kiépítésére fejlesztettek ki. Az SSH-t leggyakrabban arra használják, hogy egy távoli gépre belépjenek vele és ott parancsokat adjanak ki. Az ssh szerverek alapértelmezésben a 22-es TCP porton futnak.

Az SSH protokollnak jelenleg már csak a 2-es verzióját használjuk.

SSH használata

Ahhoz, hogy egy távoli gépre ssh-val be tudjunk jelentkezni több mindenre érdemes odafigyelni. Elször is telepíteni kell egy ssh szervert (OpenSSH) arra a Linux/Unix operációs rendszerrel rendelkez gépre, amelyikre távolról be szeretnénk jelentkezni. Mindig az adott operációs rendszerhez tartozó legfrissebb ssh szervert telepítsük fel.

Természetesen nem csak Linux/Unix operációs rendszereken lehet ssh szervert (OpenSSH) futtatni. Ma már Windows operációs rendszerekhez is van ssh szerver program, amit csak fel kell telepíteni.

Napjainkban már a hálózati eszközökön is egyre inkább terjed az ssh-n keresztül történ belépés lehetsége. St bizonyos szerverek menedzsment portjait is el lehet már így érni.

Ha már fut az elérni kívánt gépen az ssh szerver, akkor a mi távoli gépünkre is kell valamilyen kliens program, amelynek segítségével kapcsolódni tudunk a szerverhez. Ez Linux/Unix operációs rendszer esetén egy ssh kliens, ami általában gyárilag telepítdik az operációs rendszerrel együtt. Windows operációs rendszer esetén a PUTTY programot érdemes ehhez feltelepíteni és használni.

Miután mind a szerveren fut az ssh szolgáltatás mind az általunk használt kliens gépen van olyan program ami képes ssh-n keresztül kapcsolódni a szerverhez nem marad más hátra, mint létrehozni azokat a felhasználókat, akik kapcsolódhatnak ssh-n keresztül a hálózatunkhoz.

Felhasználók hozzáférése

- **Belépés jelszóval**

– Hozzuk létre az adott gépen azokat a felhasználóinkat, akiket szeretnénk, hogy a gépet távolról elérjék és generáljunk nekik központilag valamilyen kellen bonyolult jelszót. A legjobb az ilyen jelszót személyen megmondani a felhasználóan és nyomatékosan megkérni, hogy ne árulja el senkinek, ne írja fel a monitorára, stb. hanem próbálja megjegyezni, vagy speciálisan jelszókezelésre fejlszetett szoftverben tárolni. Ezt a jelszót a szerveren is állítsuk be a felhasználóhoz.

- **Belépés RSA/DSA kulccsal**

– A kulcspárral történ felhasználói belépés bonyolultabb, mint a hagyományos felhasználónév/jelszó alapú belépés. Ilyenkor a belépés RSA/DSA publikus/privát kulcspárokkal történik. A felhasználót ilyenkor is létre kell hozni a szerveren, de nem kell neki jelszót tárolni. A publikus kulcsot a felhasználótól az els belépés eltt el kell kérni és be kell másolni a felhasználó .ssh könyvtárába az authorized_keys fájlba. Ha a megadott felhasználónévhez tartozó privát és publikus kulcsok ellenrzése olyan eredményt ad, hogy minden rendben, akkor a szerver beengedi a felhasználót.

– Ha a kulcs kompromittálódik, akkor azonnal vissza kell vonni és újat kell csinálni és a rendszer továbbra is használható.

- **Jelszó vagy kulcs alapú felhasználó kezelés?**

– Sok fórumon vitáznak/vitáztak arról, hogy a hagyományos jelszó alapú belépés vagy a kulcspár alapú belépés a biztonságosabb. SSH-2

protokoll esetén a titkosított csatorna már létezik, így a jelszavak lehallgathatósága nem merül fel, mint veszélyforrás. Sokkal nagyobb problémát okoz, ha a jelszót tároló szervert feltörik, akkor hozzájut még az igazán ers jelszavakhoz is.

– A kulcspár alapú belépésnek a hagyományos felhasználónév/jelszó alapú belépéssel szemben az a nagy elnye, hogy ha a szervert esetleg feltörik és hozzá is férnek a publikus kulcsunkhoz, attól még a privát kulcs a saját gépünkön van, így a nevünkben nem tudnak belépni, hacsak nem szerzik meg a gépünket is. A privát kulcsot a gépünkön a nagyobb biztonság érdekében védjük meg egy általunk ismert ers jelszóval.

– Ezért, ha csak valami különleges akadálya nincs (pl. hálózati eszközökbe való belépés), akkor ragaszkodjunk a kulcspár alapú belépéshez.

SSH biztonság

Korábban már említésre került, hogy amikor ssh szervert telepítünk a gépünkre, mindig a legfrissebb verziót tegyük fel. Ez persze nem jelenti azt, hogy soha többet nem kell ehhez hozzányúlnunk, vagy, hogy biztonságban vagyunk. Ezért mindig kövesük a frissítéseket, ill. a közzétett sérülékenységeket és azoknak megfelelen frissítsük saját rendszerünket.

A biztonsághoz az is hozzátartozik, hogy honnan lehet hozzáférni a szervereinkhez.

SSH Szerver konfigurációja

- Az ssh-d konfigurálása biztonsági szempontból

Az **/etc/sshs/sshd_config** file-ban az alábbiakat érdemes beállítani

Port – milyen porton hallgatózzon a szerver (alapértelmezett 22)ListenAddress – ha több IP cím van melyiken keresztül hallgatózzon az SSH démon (0.0.0.0 minden IP címen)PermitRootLogin no – ajánlott, hogy root felhasználóval ne lehessen ssh-n keresztül belépniAllowGroups – csak adott felhasználói csoportoknak engedélyezni az SSH-n keresztüli bejelentkezéstAllowUsers – az adott felhasználót engedi be az adott hostrólDenyGroups – az adott felhasználói csoport tiltásaDenyUsers – az adott felhasználó tiltásaPermitEmptyPasswords – engedélyezett -e az üres jelszavak alkalmazásaHostbasedAuthentication – host based alapú authentikáció engedélyezése vagy tiltásaStrictModes yes – a könyvtár jogosultságok rendben vannak-e

Távoli hozzáférés szabályozás

A távoli hozzáférés esetén nem csak arra kell figyelnünk, hogy a felhasználók milyen jelszóval, vagy kulcspárral férnek hozzá a rendszereinkhez, hanem az is fontos, hogy egyáltalán honnan (milyen címekrl) férhetnek hozzá távolról a szerverekhez.

- **Hozzáférés VPN-n keresztül**

Távoli hozzáférés esetén nagyon fontos, hogy minél védettebb hálózatból férjünk hozzá a rendszerünkhöz. A publikus IP címmel rendelkez szerverek esetén nem javasolt, hogy bárhonnan bejelentkezzünk a szerverünkre, hanem ilyenkor valamilyen VPN (Virtual Private Network) mögül engedélyezzük csak a belépést. Ezt megcsinálhatjuk úgy, hogy a szerverünknek van egy a VPN hálózatba tartozó IP címe és onnan engedjük be az ssh-t, vagy lehet olyan megoldás is, hogy bejelentkezünk egy VPN-be és annak a publikus címérl lépünk be a rendszerünkbe.

- **Tzfalazás**

Akár VPN mögül, akár nem védett hálózatról szeretnénk belépni ssh-n keresztül a távoli szerverünkbe, mindenképpen javasolt valamilyen tzfal megoldás. Ez a megoldás lehet a Linux rendszerben lev iptablesfelkonfigurálása úgy, hogy csak az általunk meghatározott IP címekrl engedjük a 22-es porton a kommunikációt.

- **Fail2ban**

Sokszor tapasztalhatjuk a logjainkban, hogy mindenféle idegen címekrl próbálkoznak bejutni a rendszereinkbe. Ennek megelzésére érdemes feltenni a Linux alapú szervereinkre a fail2ban programcsomagot és beállítani úgy, hogy ha egy adott címrl túl sok hibás belépési próbálkozás történik, akkor azt egy idre tiltsa ki. Az id lehet pár perc, pár óra, stb. Ez a brute force alapú jelszó feltörési próbálkozás ellen hathatós védelmet nyújt.

- **SSH nem default porton**

A nem default porton (22) porton történ ssh szerver üzemeltetése megosztja az ezzel a témával foglalkozó fórumok hozzászólóit. Ennek a megoldásnak vannak elnyei is és hátrányai is.Elnye az, hogy a normál portra szakosodott támadások ellen védelmet nyújt, hátránya viszont, hogy mind a szervert, mind a klienst fel kell erre készíteni, ráadásul a tzfalak üzemeltetit is tájékoztatni kell róla, mert fennakadhat valahol a más portra történ kommunikáció.

Összefoglalás

Szó esett az SSH protokoll fogalmáról, a felhasználó kezelésrl és a biztonságról. Mit is javasolhatunk összegzés képpen?

- törekedjünk a legfrissebb verziójú ssh-t futtatni
- hálózati eszközeinken is az ssh-n keresztüli elérést próbáljuk meg bevezetni
- ahol csak lehet, a felhasználók kulcspár alapú belépést használjanak, ahol ez nem megoldható ott ers jelszavakat használjunk
- a távoli hozzáférést szabályozzuk úgy, hogy csak valamilyen tzfal mögül lehessen a szervereket elérni
- kövessük figyelemmel a biztonsági riasztásokat, és ha szükséges, akkor alkalmazzunk egyedi javítást, amíg központi frissítés kiadásra kerül a használt operációsrendszerhez

- esetlegesen fontoljuk meg az ssh szerver default (22) portól eltér porton történ üzemeltetését