

Mérési útmutató a
„Secure Shell (SSH) kontroll és audit”
című méréshez

2018. április 16.



BALABIT

A mérést kidolgozta: Höltzl Péter (2016)
Frissítette: Ládi Gergő (2018)

Balabit Europe Kft.

BME, CrySyS Adat- és Rendszerbiztonság Laboratórium

1. Elméleti összefoglaló

A következőkben rövid áttekintést nyújtunk az SSH protokollról és funkcionalitásáról.

Itt szerepelhet:

- háttérismeretek
- mérés célja

1.1. Az SSH protokoll

Az SSH protokoll rejtjelezett távoli shell hozzáférést nyújtó alkalmazás POSIX szerverek menedzselésére. A protokoll 3 fő lépésből áll:

1. **Kulcscsere:** A kliens és a szerver megegyezik a használt protokollról (ssh-1 vagy ssh-2), a használt titkosítási és hashing algoritmusokról, valamint a kulcsméretekről, majd felépítik a rejtjelezett kapcsolatot a további lépések számára.
2. **Authentikáció:** A kliens meggyőződik, hogy az igazi szerverhez kapcsolódott (nincs Man-in-the-Middle típusú támadás), majd végrehajtja a user autentikációt. Az SSH protokoll 4 féle autentikációs módot támogat:
 - Password: usernév/jelszó alapú azonosítás
 - Keyboard Interactive: usernév/jelszó alapú azonosítás, mely támogatja a challenge-response alapú és többlépcsős azonosítást
 - Public Key: nyilvános kulcsú rejtjelezésen alapuló azonosítás
 - X509: az X.509-es tanúsítási rendszeren alapuló felhasználói azonosítás
3. **Csatornák:** A protokoll csatorna orientált, mely azt jelenti, hogy az SSH által nyújtott funkciókat dedikált csatornákon lehet továbbítani. Akár több csatornát egyszerre egyetlen kapcsolaton. Az SSH által támogatott csatornák:
 - Session Shell
 - Session Exec
 - Session exec SCP
 - Session SFTP
 - Remote Forward
 - Local Forward
 - Agent Forward

- X11 forward
- Session Subsystem

További információk az SSH protokollról:

1. <https://www.digitalocean.com/community/tutorials/understanding-the-ssh-encryption-and-connection-process>
2. <http://ttmk.nyme.hu/fmkmmk/gab/Documents/SSH-leiras.pdf>

1.2. A Balabit Shell Control Box

A Balabit Shell Control Box (SCB) egy proxy alapú activity monitoring (megfigyelő) eszköz, mely a távoli hozzáféréseket nem csak passzívan megfigyelni képes, de a proxy technológiából adódóan (a kapcsolatok végződtetése és a protokollok pontos értelmezése) az elérhető funkciókat is képes befolyásolni. A főbb SCB funkciók:

- Kapcsolat engedélyezés, mentés és visszajátszás
- Kapcsolat korlátozás (IP, port, hálózat, protokoll)
- Csatorna kontroll (mely csatornák használhatóak, és azok módja)
- Authentikáció kontroll (authentikációs metódusok kontrollálása)
- User ID kontroll
- Protokoll monitoring (tartalom ellenőrzés)
- Password Management Integráció

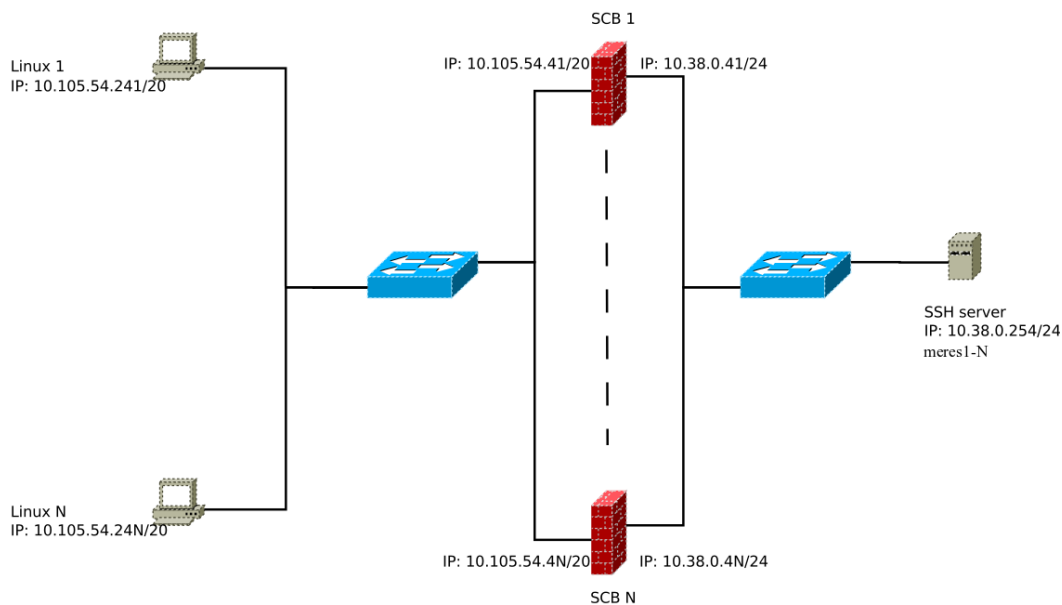
A méréshez szükséges dokumentáció (SCB Admin Guide) a mérés weboldalán érhető el! A dokumentációban megtalálható fontosabb részek a következők:

- Hálózati beállítások
- Általános kapcsolat engedélyezés
- Channel policy
- User list
- SSH Server host keys
- Gateway Authentication
- Inband destination selection

2. Mérési eszközök

A mérés során SSH kapcsolatokat kell engedélyezni, azok paramétereit konfigurálni. A méréshez a következő eszközök szükségesek:

- **SCB:** Balabit Shell Control Box 4 F2 előtelepített activity monitoring eszköz (IP: 10.105.54.41-48)
- **Browser:** Az SCB appliance elsődleges beállító felülete
- **SSH kliens:** A teszt SSH kapcsolatok kliens oldala (IP 10.105.54.241-248, USER: meres JELSZÓ: labor)
- **SSH szerver:** A teszt SSH kapcsolatok szerver oldala (IP 10.38.0.254, USER: meres1-8 JELSZÓ: labor)



1. ábra. Virtuális gépek topológiája

3. A mérés előkészítése

Lépjen be az SCB webes adminisztrációs felületére. Futtassa le az inicializáló varázslót az alábbi beállításokkal:

1. **Welcome:** Másik SCB-ből exportált konfiguráció feltöltésének lehetősége (cold spare). Ezt a lépést hagyja most ki.

2. **License:** Az SCB felhasználói szerződés elfogadása valamint a licen-
se feltöltése. Töltse fel a megkapott licenc fájlt az Upload gombra
kattintással, majd lépjen tovább (Next).
3. **Networking:** Hálózati beállítások. A felület kötelező paraméterei
 - **IP:** 10.105.54.41-48
 - **Netmask:** 255.255.240.0
 - **Default gw:** 10.105.48.1
 - **Hostname:** scb
 - **Domainname:** client.lan
 - **DNS Server:** 10.105.48.1
 - **SMTP Server:** 10.105.48.1
 - **Administrator mail:** scb@fake.mail
 - **Timezone:** Europe/Budapest
4. **Users:** Adminisztrátori jelszavak beállítása
 - **Admin:** A webes adminisztrátor jelszava
 - **Root:** Az appliance root jelszava
5. **Certificate:** A HTTPS felület tanúsítványának kötelező paraméterei
 - **Country:** HU
 - **Organization:** BME
 - **Organization unit name:** CrySys
 - A paraméterek beállítása után nyomja meg a **Generate certifi-
cate** gombot.
6. **Finish:** Összefoglaló oldal. Ellenőrizze a beállításokat. Amennyiben
megfelelőek, a **Finish** gombbal mentse el. A felület a böngészőt auto-
matikusan az SCB IP címére irányítja.

A sikeres inicializálás után az alkalmazás a böngészőt a login ablakhoz irányítja.

4. Feladatok

4.1. SSH kapcsolat engedélyezése

Kapcsolja az SCB-t router üzemmódba, majd engedélyezzen SSH kapcsolatot a Linux kliensről a Linux szerverre a TCP/22-es porton router üzemmódban.

1. Állítsa be az SCB mögötti (Internal) hálózatot (IP: 10.38.0.41-48 Netmask: 255.255.255.0)
2. A beállításokat mentse el a COMMIT gombbal.
3. A Linux kliens gépen vegyen fel route-ot a **Internal** hálózatra a `’/sbin/route add -net 10.38.0.0 netmask 255.255.255.0 gw 10.105.54.41’` paranccsal (gateway: az Ön SCB external IP-je)

4.1.1. Engedélyezzen kapcsolatot a Linux kliensről

Hozzon létre kapcsolatot, majd állítsa be a következő paramétereket (SSH Control > Connections):

- ID: A kapcsolat neve
- FROM: A kapcsolat lehetséges forrása (host vagy subnet)
- TO: A kapcsolat lehetséges célja (host vagy subnet)
- PORT: A kapcsolat lehetséges célportja

4.1.2. Feladat

1. Építsen fel SSH kapcsolatot, lépjen be a **meres1-8** felhasználóval (**jelszó: labor**)
2. Mutassa meg az élő kapcsolatot az Active Connections menüben. Készítsen screenshotot.
3. Indítson el valamilyen alkalmazást a szerveren, majd lépjen ki a szerverről.
4. Ellenőrizze az aktív kapcsolatokat, majd keresse ki a kapcsolatot a Search menüben.
5. Nyissa meg a kapcsolat adatait az (i) gombra kattintva, generálja le az audit trail videóját (Render Video), majd játssza is le. Készítsen screenshotot.
6. Mutassa meg a kiépült kapcsolatot a Search menüben. Készítsen screenshotot.

4.2. File transfer (SCP) engedélyezése

Próbáljon `scp` paranccsal fájlt tölteni a szerverre. Amennyiben a feltöltés sikertelen (elvárt eredmény), ellenőrizze a következőket:

- SCB kapcsolat info (Search > Verdict)
- SCB naplók (Basic Settings > Troubleshooting > View log files: Logtype SSH)

4.2.1. SCP engedélyezése

Engedélyezzen SCP protokollt csak a linuxos kliensről (IP: 10.105.54.241-248) a Linux szerverre a 22-es porton:

1. Vizsgálja meg 4.1-es Feladat melyik channel policyt használja (SSH Control > Connecion > Channel policy: alapértelmezetten shell-only)
2. Módosítsa a megfelelő channel policyt (SSH Control > Channel Policies)
3. Adjon hozzá új csatornát, engedélyezze a **Session exec SCP** csatornát
4. Módosítsa a **Session exec SCP** csatornát úgy, hogy csak a linuxos gépről működjön (SSH Control > Connecion > Channel policy: From)
5. Engedélyezze a csatorna tartalmának mentését audit trailbe (SSH Control > Connecion > Channel policy: Action)
6. Engedélyezze a file transfer syslog-ba naplózását (Log file transfers to syslog)
7. Engedélyezze a file transfer adatbázisba naplózását (Log file transfers to database)

4.2.2. Feladat

- Engedélyezés után töltsön fel valamilyen fájlt
- Ellenőrizze a file transfert a naplókban (Basic settings > Troubleshooting > View log files: Logtype SSH). Másolja be a legrelevánsabb naplóbejegyzéseket.
- Ellenőrizze a file transfert a search menüben (Search > Customize Columns: adja a File Operations-t a látható oszlopok közé), majd keresse ki a kapcsolatot és ellenőrizze a file transfert. Készítsen screenshotot.

4.3. User ID korlátozása

Hozzon létre olyan konfigurációt, melyben az előző feladat **scp** parancsa csak a **meres1** és **meres2** user ID-vel lehetséges.

4.3.1. User ID korlátozása

Hozzon létre User List-et (Policies > Users Lists) **Default Reject** policyval:

1. Készítsen User Listet
2. Állítson be Policy ID-t (pl. meres1_2_only)

3. Vegye fel a meres1-et és a meres2-t a kivételek közé
4. Navigáljon a 2. feladatban használt Channel Policyhez és módosítsa a **Session Exec SCP** csatornát: A Remote Grouphoz írja be User List policy ID-jét

4.3.2. Feladat

- Töltsön fel fájlt a Linux szerverre meres1 UID-dal, majd a meres2 UID-dal. Mutassa meg a file feltöltést a Search menüben. Készítsen screenshotot.
- Próbáljon fájlt feltölteni meres3 UID-dal. Mutassa meg a Search menüben. Készítsen screenshotot.
- Másolja be a legrelevánsabb naplóbejegyzéseket a sikeres és sikertelen feltöltésekről.

4.4. Szerver oldali host kulcs ellenőrzés

Állítsa be a kapcsolatot úgy, hogy a proxy csak megbízható szerverekhez kapcsolódjon:

4.4.1. Server side hostkey beállítás

1. Módosítsa a kapcsolatot úgy, hogy a szerver oldali hostkey-ek esetében csak a megbízható (trusted) kulcsokat fogadja el (Server side hostkey settings: Plain host key check = **Only accept trusted keys**)
2. Keresse ki a Linux szerver host kulcsát az SCB-n tárolt kulcsok között (SSH Control > Server Host Keys > Show All)
3. Törölje a szerver kulcsát (törlés és **commit**)

4.4.2. Feladat

- Próbáljon kapcsolódni a Linux szerverhez.
- Mutassa meg a sikertelen kapcsolatot a Search menüben. Készítsen screenshotot.
- Mutassa meg a legrelevánsabb naplóbejegyzéseket.
- Tanítsa meg a Linux szerver host kulcsát (SSH Control > Server Host Keys)
 - Add IP és Port
 - Public key (RSA)

– Query

- Próbáljon kapcsolódni a Linux szerverhez
- Mutassa meg a sikeres kapcsolatot a Search menüben. Készítsen screenshotot.

4.5. Inband gateway authentication beállítása

Állítsa be a kapcsolatot úgy, hogy a felhasználóknak kétszer kelljen autentikációt végezniük. Először az SCB-n, majd sikeres autentikáció után a szerveren.

4.5.1. Inband gateway authentication beállítása

1. Készítsen autentikációs adatbázist a gateway autentikációhoz (Policies > Local User Databases)
 - (a) Állítson be ID-t
 - (b) Vegye fel a meres1 user ID-t
 - (c) Állítsa be a meres1 kliens oldali jelszavát
2. Készítsen Authentnication policnyt (SSH Control > Authentication Policies)
3. Állítsa a kliens oldali autentikációt None-ról Local-ra
4. Válassza ki az imént beállított Local User adatbázist
5. Hitelesítési módszernek a kulcsos hitelesítés helyett (Public Key) válassza a jelszó alapút (Password).
6. Szerver oldali "Relayed" authenticationnél csak a Password autentikációt engedélyezze
7. A kiválasztott kapcsolatban (SSH Control > Connections) válassza ki az imént létrehozott autentikációs adatbázist

4.5.2. Feladat

- Kapcsolódjon a Linux szerverhez meres5 felhasználóval
- Írja le, mit tapasztal
- Kapcsolódjon a Linux szerverhez meres1 felhasználóval
- Írja le, mit tapasztal

4.6. Kulcsos autentikáció

Állítson be olyan kapcsolatot, amely a szerver oldalon kulcsos autentikációt használ **agent forward** segítségével.

4.6.1. Kulcsos autentikáció engedélyezése

1. Engedélyezze a megfelelő channel policyben a **Session exec** csatornát. *Megjegyzés: A Session exec csatorna csak a kulcs feltöltéséhez használatos ssh-copy-id parancshoz szükséges. Az authorized_keys fájl kézi szerkesztése esetén ez elhagyható.*
2. Készítsen kulcspárt az **ssh-keygen** segítségével, majd a publikus kulcsot másolja a szerveren a `~/.ssh/authorized_keys` fájlba. A kulcs feltöltésére használja az **ssh-copy-id** parancsot.
3. Ellenőrizze a feltöltött kulcsot (a szerveren a `.ssh/authorized_keys` megjelenítése).
4. Ellenőrizze a feltöltést a Search menüben (Search > Customize columns > Exec command).
5. Módosítsa az authentication policyt úgy, hogy szerver oldalon csak kulcsos autentikációt engedélyezzen (Authentication Policies > Relayed authentication methods > Publickey > Agent (Tiltsa a Password és a Keyboard Interactive autentikációs metódusokat).

4.6.2. Feladat

- Próbáljon kapcsolódni a szerverhez. Írja le, mit tapasztal. Másolja be legrelevánsabb naplóbejegyzéseket.
- Indítsa el az SSH Agentet:
 - Indítsa el az **ssh-agent** alkalmazást: `'ssh-agent bash'`
 - Ellenőrizze az agent kulcstárolóját a `'ssh-add -L'` paranccsal
 - Importálja a kulcsát `'ssh-add'`, majd adja meg a kulcs jelszavát
 - Ellenőrizze az importálást a `'ssh-add -L'` paranccsal
- Kapcsolódjon a szerverhez. Írja le, mit tapasztalt. (Az ssh '-A' kapcsolóját érdemes használni.)
- Mutassa meg az autentikációs metódust (Search > Customize columns > Authentication method)
- Másolja be a legrelevánsabb naplóbejegyzéseket.

4.7. Inband destination selection

Állítson be olyan kapcsolatot, amelyben a szerver oldali kapcsolat célját a user ID határozza meg. Ez esetben a login id meres1-ről meres1@10.38.0.254-re módosul.

4.7.1. Feladat

1. A kapcsolat célját (TO) állítsa az SCB IP címére (10.105.54.41-48)
2. A szerver oldali kapcsolat kiválasztáshoz (TARGET) állítsa be az `inband destination selection`-t.
3. Az `inband destination selection` targetjét állítsa be úgy, hogy minimálisan a Linux szerver (10.38.0.254/32) elérhető legyen.

4.7.2. Feladat

1. Kapcsolódjon az SCB IP címre az SSH klienssel, a usernév legyen a célszerver userneve és IP címe, pl. 'meres1@10.38.0.254'
2. Mutassa meg a kiépült kapcsolatot az Active Connections-ben
3. Másolja be a legrelevánsabb naplóbejegyzéseket.

4.8. SSH csatornák

Építsen ki több Session Shell csatornát egyetlen SSH kapcsolaton belül. Ehhez módosítsa az SSH kliens beállításait a `~/.ssh/config` szerkesztésével.

```
Host *
  ControlMaster auto
  ControlPath /home/meres/.ssh/controlmasters/%r%h:%p
  ControlPersist yes
  ServerAliveInterval 30
```

Hozza létre a `~/.ssh/controlmasters/` könyvtárat.

4.8.1. Feladat

1. Építsen ki több párhuzamos kapcsolatot ugyanazokkal a paraméterekkel
2. Mutassa meg a kiépült kapcsolatot az Active Connections-ben
3. Másolja be a legrelevánsabb naplóbejegyzéseket.
4. Töltse le a kapcsolatokhoz tartozó audit trailt és mutassa be a párhuzamos csatornákat. Készítsen screenshotot.

5. Előfordulható beugró kérdések

5.1. Kérdések az SSH témakörrel kapcsolatban

1. Mire használatos az SSH?
2. Milyen szállítási rétegbeli protokollra épül az SSH? Annak melyik portját használja?
3. Milyen autentikációs megoldásokat támogat az SSH?
4. Mit jelent az, hogy az SSH csatorna-orientált?
5. Soroljon fel legalább három dolgot (csatornát), amelyre az SSH-t használni lehet!
6. Mire használatos az ssh-keygen alkalmazás?

5.2. Kérdések a Shell Control Box szoftverrel kapcsolatban

1. Miben különbözik az SCB egy hagyományos tűzfaltól?
2. Mi az audit trail?
3. Mire való az Inband Gateway Authentication funkció?
4. Mire való az Inband Destination Selection funkció?

A. Jegyzőkönyv

A jegyzőkönyvet a mérés után egy héten belül el kell küldeni a mérésvezetőnek pdf formátumban. A jegyzőkönyvnek az alábbiakat kell tartalmaznia:

- Hallgató(k) neve és Neptun kódja
- Mérés neve
- Mérés időpontja
- Feladatok megoldása

A megoldások leírásánál törekedni kell a tömör, de érthető válaszra. A leírásból a megoldásnak reprodukálhatónak kell lennie (hosszabb kód mellékelhető a pdf-hez, nem feltétlenül kell beírakni)!