Cible de sécurité CSPN - SCB 4 LTS

Version	Date	Description	Rédacteurs
1	06-02-2014	Version initiale	Balabit
2	14-05-2014	Prise en compte des remarques de forme	Balabit
3	18-08-2014	Mise à jour des versions	Balabit
3.1	21-08-2014	Mise à jour des versions	Balabit
4.0	10-08-2015	Retrait des protocoles rdp et ica du périmètre Désactivation de l'accès SSH	Balabit
4.1	01-10-2015	Clarifications sur le périmètre de l'évaluation	Balabit
4.2	02-02-2016	Mise à jour pour la version 4.0.6.sec3	Balabit

Sommaire

1 Identification du produit

Cette cible de sécurité a été élaborée en vue d'une évaluation Certification Sécurité de Premier Niveau (CSPN).

Organisation éditrice	Balabit
Lien vers l'organisation	https://www.balabit.com/
Nom commercial du produit	Shell Control Box (SCB)
Numéro de la version évaluée	4 LTS (4.0.6.Sec3)
Catégorie de produit	Identification, authentification, contrôle d'accès, audit

Le produit SCB peut être vendu en appliance matérielle et en appliance virtuelle. Selon la demande du client final, trois plateformes matérielles sont disponibles :

- ***Balabit Shell Control Box T-1*** :
  - Processeur : Intel Xeon X3430 @ 2.40GHz,
  - Mémoire : 2 x 4GB,
  - Capacité : 2 x 931 GB,
  - RAID : RAID logiciel.

- ***Balabit Shell Control Box T-4*** :
  - Processeur : Intel Xeon E3-1275V2 @3.50GHz
  - Mémoire : 2 x 4GB,
  - Capacité : 4 x 2 TB,
  - RAID : LSI MegaRAID SAS 9271-4i SLG.

- ***Balabit Shell Control Box T-10*** :
  - Processeur : Intel Xeon E5-2630V2 @2.6GHz,
  - Mémoire : 8 x 4GB,
  - Capacité : 13 x 1 TB,
  - RAID : LSI 2208.

L'installation en appliance virtuelle a été retenue pour la configuration d'évaluation.

2 Argumentaire du produit

2.1 Description générale du produit

Shell Control Box (SCB) est un dispositif de surveillance d'activités qui permet de contrôler l'accès privilégié aux serveurs distants et aux périphériques réseaux et d'enregistrer les activités dans des pistes d'audit.

Figure 1: Description générale SCB

SCB fait office de passerelle. Les connexions et le trafic sont contrôlés au niveau applicatif (couche 7 dans le modèle OSI). Tout trafic en violation du protocole est rejeté.

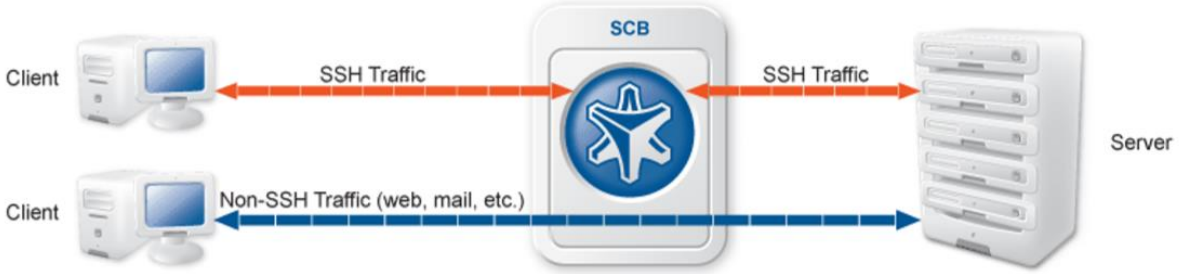

Figure 2: Fonctionnement global SCB

Dans la suite de ce document, le *client* est l'entité qui souhaite accéder à un serveur. Le *serveur cible* est la ressource à laquelle veut accéder le client comme le montre le schéma ci-dessus. Le *domaine Clients* correspond au domaine sur lequel se trouvent les clients SCB et le

domaine Serveurs Cibles correspond aux domaines sur lesquels se trouvent les serveurs cibles.

Si SCB supporte de très nombreux protocoles de communication entre le domaine Client et le domaine Serveurs Cibles (SSHv2, RDP v8, HTTP/HTTPS, …) seul le protocole SSHv2 est activé dans la configuration évaluée.

2.2 Utilisation du produit

2.2.1 Connexion aux serveurs cibles

Les connexions aux serveurs cibles se font en utilisant les outils de connexion habituels via les ports standards de chaque protocole.

Si SCB peut être déployé selon plusieurs modes, le mode de déploiement retenu pour l'évaluation est le **mode Bastion**.

Dans ce mode, les clients ne peuvent contacter que le SCB. Les serveurs administrés ne sont pas accessibles directement. Le pare-feu du réseau doit être configuré de telle sorte que seules les connexions en provenance du SCB puissent accéder aux serveurs. Dans ce mode, SCB n'a besoin que d'une interface physique.

Dans le mode Bastion, l'accès est réalisé de manière non-transparente : SCB extrait l'adresse du serveur cible du protocole inspecté. Ce mode simplifie l'intégration de la solution SCB à l'infrastructure réseau.

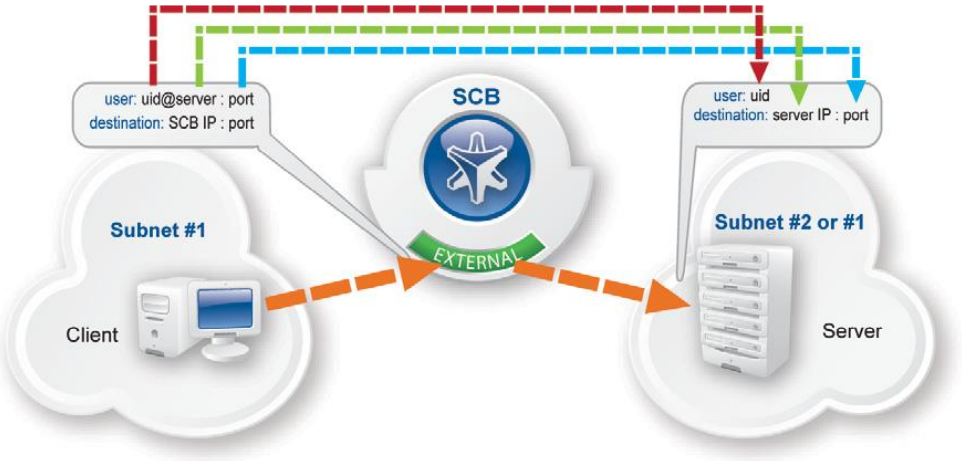

Figure 3: Mode non-transparent

Dans la configuration retenue pour l'évaluation (SSHv2), l'authentification est réalisée par mots de passe. La base contenant les données d'authentification est stockée localement.

2.2.2 Administration du SCB

SCB s'administre grâce à une interface Web qui est accessible en HTTPS sur le port 443. Dans la configuration évaluée, l'administration via le protocole SSH est désactivée.

2.3 Environnement d'utilisation

SCB s'intègre dans un réseau IPv4. Les clients standards pour accéder aux équipements restent identiques à ceux utilisés avant la mise en place du SCB (par exemple : openssh, putty, client RDP mstsc, navigateurs web, …).

2.4 Dépendances du produit à des matériels, logiciels et/ou des microprogrammes du système

Dans le mode de distribution Appliance virtuelle, SCB nécessite une plateforme VMware ESXi version 4.0 ou supérieure. Le système d'exploitation est Ubuntu Precise version 12.04.

2.5 Utilisateurs typiques du produit

Il existe deux types d'utilisateurs :

- Clients : entités (personne ou machine) souhaitant accéder à un serveur cible,
- Administrateurs du SCB.

SCB permet de créer des groupes d'administrateurs partageant un profil d'actions possibles. Ces actions sont appliquées à des objets détaillés dans le guide administrateur qui peuvent être, par exemple, le contrôle d'accès, l'accès aux pistes d'audit, la création ou la suppression d'administrateurs SCB etc.

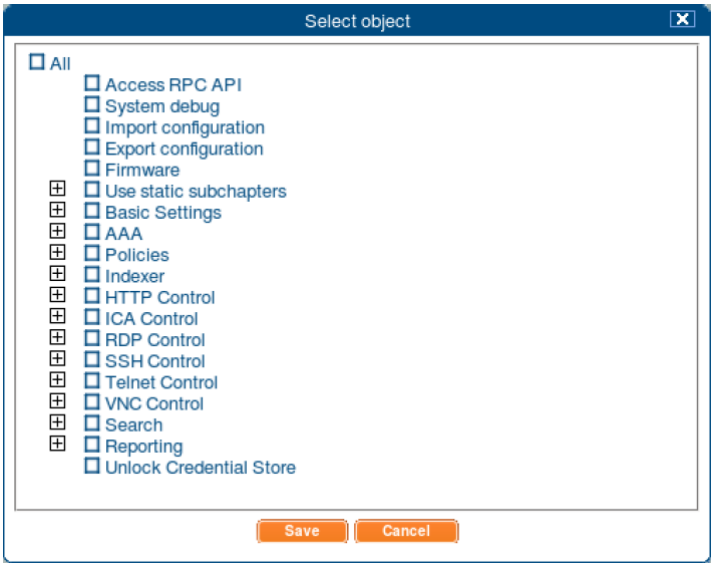

Figure 4 : Objets présents dans l'interface SCB

Un administrateur peut avoir ses propres privilèges sans faire partie d'un groupe.

Un profil Super administrateur est présent. Ce dernier est un administrateur avec tous les privilèges et ne peut être supprimé. Il permet de créer les premiers administrateurs lors de la première utilisation de SCB.

2.6 Hypothèses sur l'environnement

2.6.1 Hypothèses sur l'environnement physique du produit

- L'accès physique au serveur SCB et à sa console est restreint aux seuls administrateurs du produit SCB.

2.6.2 Hypothèses sur les utilisateurs du produit

- Le produit est installé et configuré par des personnes compétentes, formées et non hostiles.
- Les administrateurs de l'infrastructure réseau des domaines Clients et Serveurs cibles sont compétents, formés et non hostiles.
- Les administrateurs du produit SCB sont compétents, formés et non hostiles.

2.6.3 Hypothèses sur l'environnement technique du produit

- Les accès aux équipements du domaine Serveur Cible sont contrôlés de manière à obliger le passage par SCB.
- L'environnement virtuel de déploiement (ESXi) est considéré comme sécurisé et de confiance.

2.7 Périmètre de l'évaluation

Tous les logiciels intégrés dans l'appliance SCB font partie du périmètre de l'évaluation.

Dans la configuration évaluée, seuls les protocoles suivants sont supportés :

- Administration du SCB :
  - HTTPS
- Flux utilisateurs :
  - SSH v2

3 Environnement technique dans lequel le produit doit fonctionner

La configuration retenue pour l'évaluation est la suivante :

- Appliance virtuelle SCB version 4.0.6.Sec2,
- Mode : bastion,
- Méthode d'authentification : base de données de mots de passe,
- Base de données utilisateurs : locale.

4 Biens sensibles que le produit doit protéger

Les services offerts par SCB doivent être disponibles et intègres et SCB doit protéger les données suivantes :

4.1 Données utilisateur

4.1.1 Flux Utilisateurs

Les flux transitant par SCB doivent être protégés en Disponibilité, Intégrité et Confidentialité. SCB ne doit pas altérer de manière illicite ces flux et ne doit pas permettre à une personne non explicitement autorisée de les consulter.

4.1.2 Pistes d'audit

Les pistes d'audit doivent être protégées en Intégrité et Confidentialité. SCB ne doit pas permettre à une personne de supprimer, modifier ou même consulter des pistes d'audit s'il n'en a pas explicitement les droits.

4.2 Données internes

4.2.1 Base des utilisateurs

Cette base contient les identifiants et les moyens d'assurer l'authentification des utilisateurs du SI sur le SCB. Une personne non explicitement autorisée à le faire ne doit pas pouvoir consulter, modifier ou supprimer des données dans cette base.

4.2.2 Base des serveurs cibles et droits d'accès

Cette base contient les données permettant de se connecter aux serveurs cibles, ainsi que les associations autorisées entre les clients et les serveurs cibles. Une personne non explicitement autorisée à le faire ne doit pas pouvoir consulter, modifier ou supprimer des données dans cette base.

4.2.3 Journaux

Outre générer des pistes d'audit des flux utilisateurs, SCB génère des journaux des opérations effectuées par elle-même. Une personne non explicitement autorisée à le faire ne doit pas pouvoir modifier, supprimer ou même simplement consulter ces données.

5 Description des menaces

5.1 Agents menaçants

Les agents de menace considérés pour l'évaluation sont:

- les personnes malveillantes ayant un accès logique ou physique à des équipements pouvant se connecter au SCB mais ne disposant pas de compte client, ci-après « attaquant externe »;
- les clients malveillants.

5.2 Liste des menaces retenues

5.2.1 Menaces sur les flux Utilisateurs

- ***Écoute des flux utilisateurs :*** Un attaquant externe écoute les flux utilisateurs pour compromettre la confidentialité des données transmises.

  Données impactées : Confidentialité des flux utilisateurs.

- ***Altération des flux utilisateurs :*** Un attaquant externe intercepte et modifie les flux utilisateurs.

  Données impactées : Intégrité des flux utilisateurs.

5.2.2 Menaces liées aux opérations réalisées par les Clients

- ***Abus des droits clients :*** Un client malveillant abuse de ses privilèges pour commettre des actions illicites sur un serveur cible.

  Données impactées : Intégrité des flux clients.

- ***Répudiation client:*** Un client malveillant nie avoir réalisé une opération (ou a contrario certifie avoir réalisé une opération).

Données impactées : Intégrité des flux Utilisateurs.

- ***Accès illicite client aux serveurs cibles*** : Un client malveillant tente d'accéder à un serveur cible auquel il n'est pas autorisé à accéder.

  Données impactées : Intégrité des flux Utilisateurs.

5.2.3 Menaces sur SCB

- ***Usurpation d'identité SCB:*** Un attaquant externe tente d'usurper l'identité d'un client légitime ou d'un administrateur de SCB pour utiliser ses privilèges (accès aux serveurs cibles ou accès à l'interface d'administration de SCB).

  Données impactées : Intégrité et confidentialité des biens sensibles accessibles avec le compte usurpé.

- ***Accès illicite SCB*** **:** Un attaquant externe ou un client malveillant réussit par une attaque à s'introduire dans le système et à accéder et/ou à modifier illicitement les données sensibles stockées dans SCB (données d'authentification, pistes d'audit).

  Données impactées : Intégrité et confidentialité des biens sensibles stockés (pistes d'audit, secrets d'authentification, ACL, ...)

6 Description des fonctions de sécurité du produit

6.1 Liste des fonctions de sécurité

Le périmètre d'évaluation couvre les fonctions de sécurité suivantes du SCB:

- ***Contrôle des accès aux serveurs cibles*** : SCB permet de mettre en œuvre une politique d'accès aux ressources cibles ;

- ***Traçabilité des accès aux serveurs cibles*** : placé en coupure entre l'utilisateur et la ressource cible, SCB permet d'enregistrer toutes les opérations réalisées, et ceci pour tous les protocoles supportés ;

- ***Protection des pistes d'audit*** : Les activités réalisées par l'utilisateur dans et au travers du SCB sont enregistrées dans les pistes d'audit. Ces pistes sont protégées en intégrité, confidentialité et sont horodatées et signées pour en garantir l'authenticité;

- ***Authentification des clients*** : le client s'authentifie avec un mot de passe sur SCB avant d'accéder aux serveurs cibles ;

- ***Authentification des administrateurs*** : pour accéder à l'interface d'administration SCB, les administrateurs SCB s'authentifient en tant qu'administrateur grâce à un mot de passe ;

- ***Protocoles sécurisés*** : Les communications avec SCB sont protégées en confidentialité et en intégrité.

Dans la configuration évaluée, seuls les protocoles suivants sont supportés : HTTPS pour la connexion des administrateurs, SSHv2 pour les flux clients.

6.2 Argumentaire des fonctions de sécurité

Le tableau ci-dessous indique comment chaque menace identifiée est couverte par les fonctions de sécurité évaluées.

Menaces	**Fonctions de sécurité permettant de contrer les menaces**
Écoute des flux	Protocoles sécurisés
Altération des flux	Protocoles sécurisés
Abus des droits clients	Traçabilité des accès aux serveurs cibles Protection des pistes d'audit
Répudiation	Traçabilité des accès aux serveurs cibles Protection des pistes d'audit
Accès illicite aux serveurs cibles	Contrôle des accès aux serveurs cibles
Usurpation d'identité	Authentification des clients Authentification des administrateurs
Accès illicite	Authentification des administrateurs

Tableau 1 : Tableau de couverture des menaces par les fonctions de sécurité