Mémoire de stage de fin d'études

État de l'art des systèmes de gestion des comptes à privilèges

Auteur :
Alexandre
Kervadec

Responsables :
M. Philippe Rolland
M. Damien Seiler
M. Mathieu Raffinot

2016

Remerciements

Je tiens tout particulièrement à remercier mes accompagnateurs chez SYNETIS : Damien Seiler et Philippe Rolland, qui m'ont aidé quotidiennement durant ce stage. Je remercie aussi tous les consultants de chez SYNETIS, qui ont, à des moments ponctuels, su m'enrichir de leur expertise. Il me semble aussi important de remercier Lionel Clément qui m'a suivi et aidé pour ma recherche de stage, lorsque j'avais un retard conséquent par rapport aux dates prédéfinies.

Table des matières

Introduction

Le choix de mon entreprise de stage s'est orientée vers SYNETIS, qui est une porte ouverte vers le monde de la sécurité, dans lequel je souhaite m'orienter malgré ma formation qui n'est pas spécialisée dans ce domaine.
SYNETIS est une PME [1] à taille humaine basée dans le centre de Paris. Une agence a été ouverte à Rennes en 2012 lors du recrutement de spécialistes en gestion des identités sur cette zone. Cette agence de Rennes compte 6 consultants et 2 managers (dont le chef d'agence). L'ambiance est très conviviale, tout le monde se connaît, des évènements de cohésion sont régulièrement organisés (afterwork, repas en groupe le vendredi midi). De même, une réunion trimestrielle est organisée sur le siège de Paris, qui regroupe tout le personnel de SYNETIS, afin de faire un bilan des projets, de rencontrer les nouveaux arrivants, et de partager les nouveaux objectifs visés par l'entreprise.
Le travail est réparti par équipe sur les différents projets en cours, chaque consultant pouvant travailler sur plusieurs projets en même temps. On peut distinguer deux types de projet : les gros projets s'étalant sur de longues périodes (plus de six mois) et les projets courts durant au maximum quatre mois. L'entreprise est spécialisée dans la gestion d'identité pour les grands groupes (conseils régionaux, grandes entreprises nationales et internationales), mais commence à développer une branche de pentest (test d'intrusion sur différentes structures, pour de plus amples informations, le guide de Rafay Baloch [1] est très complet).
J'étais intégré comme tous les autres consultants, avec un tuteur travaillant sur des projets correspondants au sujet de mon stage qui me guidait au travers de mes recherches et développements.
Ce stage concerne les systèmes de gestion de comptes à privilèges, qui sont les comptes avec des droits élevés, comme ceux des compte ROOT des systèmes d'exploitation Linux/UNIX et ADMINISTRATEUR sur Windows. Durant ce stage, il était question de comprendre ne profondeur les enjeux de la gestion de comptes à privilèges, les moyens existant pour établir cette gestion pour pouvoir mieux comparer l'ensemble des solutions disponibles sur le marché. Cette comparaison a permis de considérer 2 solutions à mettre en œuvre sur un environnement virtuel pour comprendre ces systèmes dans les moindres détails, et en faire une comparaison encore plus poussée. Toutes les informations récoltées nous auront finalement permis de comprendre comment les solutions répondent à la problématique de la gestion des comptes à privilèges, et de déterminer quelles solutions répondent le mieux à cette problématique, afin de pouvoir proposer de l'intégration avec de futurs clients.

Le plan adopté pour la suite de ce mémoire consiste en une première section décrivant la problématique à résoudre, et les origines de cette problématique. Une deuxième section expliquera les moyens et les méthodes mises

1. Petite à Moyenne Entreprise

en œuvre pour répondre à cette problématique et enfin une dernière partie expliquera les résultats obtenus.

1 Problématique : comment pallier le manque de contrôle des comptes privilégiés

L'objectif général est de résoudre le problème de manque de contrôle et de monitoring des comptes à privilèges. Afin de parvenir à ce résultat, plusieurs solutions ont été développées par des éditeurs, le but final de ce projet étant de déterminer quelle est, ou quelles sont, la ou les meilleures solutions permettant de résoudre ce problème.
Pour répondre à cette problématique, nous allons d'abord expliquer plus en détails ce qu'est un compte à privilèges, puis nous intéresser aux raisons pour lesquelles ces comptes sont des points clefs de la sécurité des systèmes d'information. Ensuite, nous allons expliquer un fonctionnement global et commun aux solutions du marché puis mettre en avant les limitations que peuvent avoir ces solutions de PAM.

1.1 Contexte

1.1.1 Les comptes à privilèges

Il semble important de définir clairement la différence entre un compte à privilèges et un compte d'utilisateur classique, et plus précisément les deux catégories de mot de passe qu'ils engendrent :

Les mots de passe utilisateur : basiquement, un mot de passe est un secret qui permet l'utilisation d'un compte. Un compte représente un utilisateur humain et son mot de passe justifie son identité, comme un compte Active Directory [2], qui représente digitalement un humain, et le mot de passe qui justifie l'identité de l'humain qui s'y connecte auprès du système. Ce type de mot de passe est connu par l'utilisateur humain qui est représenté par le compte, le but étant d'avoir un minimum de comptes par entité humaine, l'idéal étant une correspondance bijective [3]

Les mots de passe de compte à privilèges : ces mots de passe sont des mots de passe liés à un compte qui ne représente pas une entité humaine. Ce compte peut être un compte système comme `root` sur un système d'exploitation Linux ou un compte de service sur un système d'exploitation Windows. Ces mots de passe ne sont pas forcément fournis à un utilisateurs humain, et même idéalement, ne doivent pas l'être, ainsi, ils peuvent d'être d'une complexité élevée sans avoir un soucis d'apprentissage de ce dernier

2. Système d'annuaire électronique propriétaire de Microsoft, basé sur la norme LDAP (Lightweight Directory Access Protocol).

3. Un seul utilisateur humain pour un seul compte et vice-versa.

Le but de ce stage était de trouver la meilleure solution pour sécuriser les mots de passe de comptes à privilèges tout en supervisant les comptes liés à des utilisateurs.

1.1.2 La gestion de comptes à privilèges

La gestion de comptes à privilèges (PAM[4]) est une sous-section de la gestion d'identité et d'accès (IAM[5]). L'IAM est un large champ de contrôle d'accès qui se veut critique dans le domaine des technologies de l'information.
Il existe bien sûr une multitude de connexions spécifiques entre les utilisateurs et les dépendances technologiques. La PAM n'est que l'une d'entre elles.
La PAM est apparue au début des années 2000 à cause de l'impossibilité des solutions d'IAM de contrôler, gérer et faire des rapports sur les accès aux serveurs, aux bases de données, aux équipements réseau et tout autre application critique au sein d'une organisation. Cette solution entraîne une gestion d'un petit nombre d'utilisateurs, mais d'un grand nombre de dépendances technologiques ayant une importance clef dans le fonctionnement des infrastructures.
La fonctionnalité principale d'une solution de gestion d'identité privilégiée gravite autour de la sécurisation de l'accès aux ressources critiques par les administrateurs IT.
Plus précisément, des privilèges spécifiques peuvent être délivrés à des comptes d'utilisateur. Ces privilèges sont dépendants des systèmes et des applications impliqués, mais ils peuvent inclure la capacité à écrire des données, créer des comptes, exécuter une mission, pour ne citer que quelques exemples. En plus de contrôler l'accès avec un grand niveau de finesse, beaucoup de solutions fournissent aussi un package d'actions disponibles lors de l'utilisation d'un compte privilégié. Dans le but d'assurer la sécurité de ces comptes, les solutions exploitent un large éventail de mécanismes, comme par exemple, l'utilisation de clefs SSH, la rotation de mot de passe et l'ajout de multiples authentifications (authentification multi-facteur).
La gestion d'identités privilégiées est devenue de plus en plus importante, notamment avec la croissance des requis de sécurité et des règles de conformité (l'ISO 27001 qui est une norme de sécurité international sur la protection des actifs informationnels par exemple). Il est aussi important de noter que de nombreux exploits[6] compromettant des données sont liés à la compromission d'accréditations privilégiées. Avec la recrudescence des tentatives de hack et les contrecoups économiques de plus en plus

4. Privileged Access Management
5. Identity and Access Management
6. Element permettant d'exploiter une faille de sécurité

conséquents, les entreprises commencent à apporter de plus en plus d'intérêt à la gestion et au contrôle des comptes à privilèges. En effet, les tentatives de piratage sont de plus en plus variées : du social engineering, au vol de ces accréditations par une brèche dans la sécurité en passant par des *brute force* de mot de passe n'ayant pas une complexité suffisante [7] (dont traitent Weber *et coll.* [5]).

1.2 Un point clef de la sécurité des systèmes d'information

1.2.1 Une cible de choix pour les pirates

Un compte privilégié est un compte utilisé par les administrateurs système et réseau, ainsi que par les équipes de sécurité pour accéder aux ressources réseau comme les serveurs, les pare-feux, les switches, les routeurs, les ordinateurs, les applications ou les base de données avec des droits élevés. Ces comptes sont nécessaire à la maintenance d'une infrastructure, tout comme aux interventions de réparation, de diagnostique ou gestion de situations de crise [8]. Dans de grands groupes, il peut y avoir un grand nombre de ces comptes, de l'ordre de la centaine voir du millier d'entités, réparti sur plusieurs sites.
Ces comptes peuvent aussi être des comptes d'application communicant avec d'autres applications [9], comme par exemple un serveur faisant une sauvegarde régulière sur un autre serveur de récupération.
Tous ces comptes ne sont pas surveillés par les traditionnels gestionnaires d'identités, seul un mot de passe permet d'y accéder. De plus ces comptes sont très souvent des comptes partagés entre plusieurs administrateurs pour une question de facilité de gestion.
Ainsi, une personne mal intentionnée réussissant à voler les accès d'un tel compte verrait son pouvoir de destruction, voir de vol d'information sans limites, ce qui en fait une cible privilégiée par les pirates informatiques.

1.2.2 Un manque de visibilité d'actions

Comme abordé en introduction, il existe un grand manque de visibilité sur les actions des comptes à privilèges. En effet, ces comptes aux droits élevés, ne sont ni tracés, ni surveillés. Ceci peut avoir plusieurs mauvaises incidences, certaines intentionnelles et malveillantes, d'autre involontaires

7. L'utilisation de mots de passe faibles tels que `password`, `admin`, `1234`, `azerty1234` ou `Abcd1234` reste encore très fréquente. Pour trouver ces mots de passe faibles, la technique la plus employée est le brute force avec un dictionnaire de mots de passe
8. Attaque sur un serveur par exemple
9. A2A : Application To Application, littéralement d'application à application

mais tout de même paralysantes.
On peut classer ces incidences en deux catégories, l'une relevant d'une erreur accidentelle, et l'autre d'une volonté de nuire à une organisation :

— Erreur accidentelle :

→ Erreur de configuration, difficile à retrouver à cause du manque de supervision

— Volonté de nuire :

→ Sabotage d'une configuration, menant à un déni de service

→ Vol d'informations sensibles

Ce manque de visibilité crée aussi un point noir dans un audit de sécurité : il n'y a aucune détection de faille de sécurité concernant ces comptes.

1.3 Objectifs d'un système de PAM

D'après les points précédents, on peut en déduire les spécificités que nous voudrions améliorer vis-à-vis des comptes à privilèges :

— Centraliser l'accès aux données de l'entreprise

— Sécuriser les comptes à privilèges (duo identifiants et mot de passse)

— Gérer de manière forte des mots de passe et établir une politique d'authentification forte

— Journaliser et superviser les activités des comptes à privilèges

1.4 Fonctionnement d'un système de gestion de comptes à privilèges

1.4.1 Cas général

Le principe commun à toutes les solutions des éditeurs est la présence d'une identification sur un serveur central. On peut considérer 2 groupes : les comptes à privilèges et les ressources à protéger. Entre ces 2 entités vient s'intercaler le serveur d'identification, qui fait la passerelle entre les comptes et les ressources.
L'identification d'un utilisateur sur un compte à privilèges se fait sur le serveur central, et l'identification de ce compte à privilèges sur une ressource protégée est déléguée au serveur central. Ainsi, les utilisateurs n'ont plus à gérer et connaître les mots de de passe d'accès au ressources protégées ; c'est le serveur central qui détient tous les secrets [10].
Le serveur central a à sa charge de protéger les mots de passe dans un coffre-fort et de les renouveler régulièrement.

10. Les logins et mot de passe, aussi appelés « credrentials » en anglais.

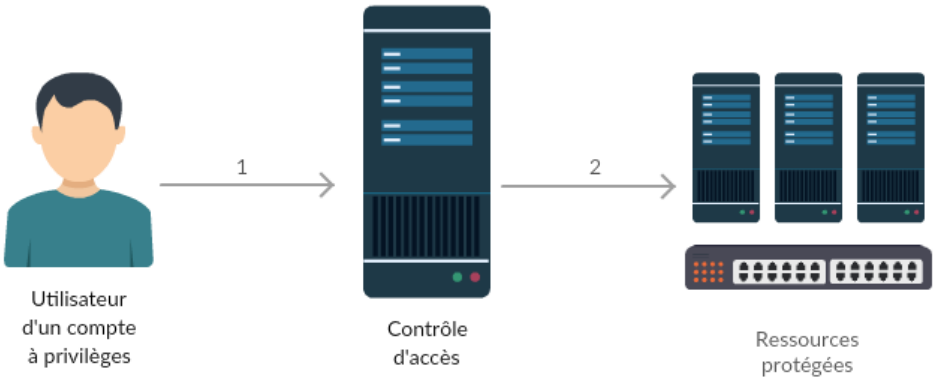

FIGURE 1 – Fonctionnement général d'un système de PAM

1.4.2 Deux types d'architecture

Malgré le principe de fonctionnement identique pour quasiment toutes les solutions de PAM, il existe cependant des différences au niveau de l'architecture de ces dernières solutions, on distingue 2 grandes familles :

— Architecture proxy [11] : les ressources et les comptes d'utilisateurs sont séparés physiquement (ou logiquement [12]), le serveur central gère tout seul les accès aux applications

— Architecture avec agents : les accès aux ressources et la supervision sont gérés par des agents sur les ressources cibles (application installée sur la ressource)

Nous pouvons rapidement nous rendre compte qu'une architecture avec des agents est beaucoup plus intrusive et longue ou difficile à mettre en place qu'une architecture en proxy, où seul l'adressage est à modifier.

1.5 Les limitations des solutions PAM

1.5.1 Le facteur humain

Il faut noter que même avec un système de PAM éprouvé et efficace, nous ne pouvons pas mettre de côté le risque le plus exploitable dans le domaine de la sécurité qu'est le facteur humain. En effet, il est souvent plus facile de tromper un élément du personnel pour une compromission de données. Il sera donc important lors d'un déploiement d'une solution de PAM, d'éduquer le personnel de l'organisation concernée, afin que ces

11. Toutes les communications transitent par un point de contrôle.
12. Redirection des paquet par port.

derniers mettent correctement en œuvre les règles de base de la sécurité informatique comme par exemple :

— Totalement prohiber « l'effet *post-it* » : notation de mot de passe sur un *post-it* collé sur l'écran

— Toujours remplacer les mots de passe d'usine dans les logiciels utilisés

— Forcer le changement régulier (au minimum une fois par mois) de mot de passe des utilisateurs

1.5.2 La détection de comportements anormaux

Très peu de solutions de PAM proposent un système de détection de comportements anormaux, comme par exemple un conseiller commercial qui aurait accès aux informations des comptes client, qui abuserait de ce droit. En effet, même avec une restriction des droits, une supervision et journalisation des activités, une solution de PAM n'est pas une intelligence artificielle qui peut détecter des comportements suspect. Cependant, il est toujours possible de détecter des comportements prédéfinis avec des successions de commandes qui lèveraient une alerte.

2 Méthodes et moyens mis en œuvre

Comme le titre l'indique, nous allons expliquer les méthodes et les moyens utilisés pour répondre à la problématique posée. Cette section sera séparée en 3 sous-sections : la première décrivant mon cheminement en matière de gestion de projet, la deuxième traitant de la phase de recherche d'informations, avec ses problèmes rencontrés et solutions trouvée, puis une troisième partie décrivant le travail effectué pendant la phase de test des deux produits sur un environnement de test, ainsi que toutes les différentes technologies utilisées.

2.1 Gestion de projet

La première chose que j'ai dû faire en arrivant dans l'entreprise, fut ce qu'on appelle chez SYNETIS une note de cadrage. Cette note de cadrage correspond, par rapport à ce qu'on a pu faire à l'université durant divers projets, à l'analyse des besoins et les résultats attendus, l'organisation en tâches de l'intégrité du stage. Cette répartition des tâches dans le temps a permis de scinder l'ensemble du projet en de multiples étapes simples, courte, qui m'a permis de segmenter mon stage pour ne pas me retrouver perdu ou submergé par le travail. En dernière partie furent explicités les contraintes et exigences de rendus pour l'entreprise ainsi que les éventuels risques à rencontrer.

2.1.1 Analyse des besoins

Le besoin général était de réaliser un état de l'art des solutions de gestion des comptes à privilèges, de mettre en place 2 preuves de concept sur un environnement de test virtualisé afin de pouvoir définir le ou les solutions les plus adaptés à la gestion des comptes privilégiés. Ces solutions pouvaient (à l'époque de la réalisation de l'état de l'art) et sont (à ce jour) déployés chez un gros client. Je suis notamment intégré à l'équipe travaillant sur cette intégration dans l'infrastructure, car ayant réalisé une mise en place dans un environnement de test de la solution en question, je fais parti des personnes les plus compétentes de SYNETIS pour répondre aux différents problèmes qui pourraient se présenter.
Cet état de l'art devait aboutir à un document présentant le principe de gestion de comptes à privilèges, premièrement de façon théorique, puis de façon technique. Ensuite, ce document devait faire une analyse d'une liste de solutions d'éditeurs étant des acteurs majeurs sur le marché de la gestion de comptes à privilèges. Enfin, ce document a aura permis de créer un tableau comparatif de toutes les solutions étudiées, selon des critères pointus qui ont été définis comme répondant à la problématique du stage.

2.1.2 Planning prévisionnel

Afin d'avoir une vue d'ensemble du projet, un planning a été réalisé à partir d'un découpage journalier des tâches à effectuer. Ce planning a permis d'avoir une vue marcoscopique du stage, et de répartir le travail sur la durée du stage, pour éviter d'avoir un retard qui pourrait surprendre à quelques semaines de la date buttoir. Ce découpage a aussi permis d'avoir des étapes, et de savoir à n'importe quel moment si j'avais de l'avance, ou surtout du retard, chose à proscrire pour arriver à un résultat convenable.

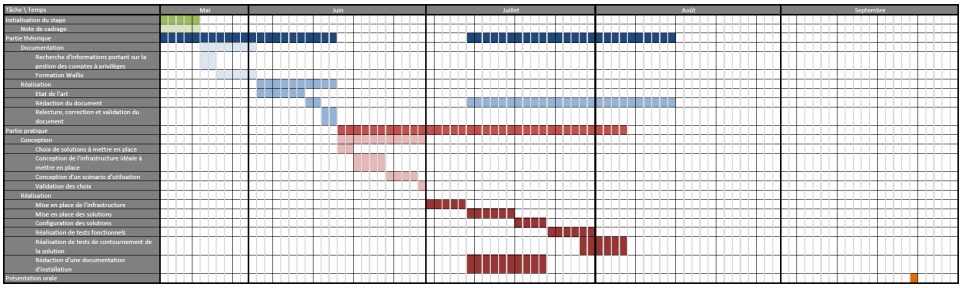

FIGURE 2 – Calendrier prévisionnel

Bien sûr, le calendrier est une estimation et la réalité s'est avérée différente, ce point est abordé en section 3. : la durée de recherche sur la gestion de comptes à privilèges et sur les différentes solutions a pris presque 2 fois plus de temps que prévu, tout comme le déploiement des solutions et le test de ces dernières. Cependant, le calendrier prévisionnel étant vu avec une large marge d'erreur, le stage tout de même pu être complété dans la durée impartie.

2.2 Recherche

La première étape a été la recherche d'informations sur le sujet. N'ayant pas de notions sur le sujet, j'ai d'abord commencé par me renseigner auprès des consultants de l'agence de Rennes, notamment mes tuteurs, Damien Seiler et Philippe Rolland, ainsi que le manager de l'agence, David Geffroy, ayant une base d'expertise dans le domaine. Grâce à ces premières lignes directrices fournis par ceux qui sont devenus mes collègues, j'ai pu orienter mes recherches internet vers la bonne direction, afin de trouver un maximum de résultats.

2.2.1 Recherche du fonctionnement des solutions

La meilleure façon de trouver des informations concernant le fonctionnement d'une solution de PAM s'est d'abord orientée vers la recherche d'informations génériques, comme des tutoriels ou des articles traitant du sujet. Cependant, j'ai fini par réaliser qu'il y avait très peu de ces ressources. La solution fut donc de directement s'orienter vers les solutions des éditeurs, et de tenter de comprendre leur fonctionnement, pour en tirer moi-même un fonctionnement général des solutions. Cette étape resta tout de même laborieuse, les éditeurs ne partageant pas énormément d'information quant à l'architecture ou le fonctionnement technique de leurs solutions, mais plutôt des caractéristiques de leur solution. Ceci ne m'empêcha pas de pouvoir trouver assez de solutions pour pouvoir en déduire une architecture assez claire, qui me donnait une vision d'ensemble du fonctionnement [13] d'une solution de PAM.
INCLURE L'EXPLICATION DE FONCTIONNEMENT EN DÉTAIL ICI ?

2.2.2 Recherche des solutions existantes sur le marché

La recherche des solutions existantes sur le marché fut assez simple, compte tenu de la précédente recherche, s'appuyant sur ces solutions en question. Néanmoins, étant parti sur une base de 6 solutions trouvées pour réaliser un descriptif du fonctionnement général d'une solution de PAM, j'ai réussi à trouver plus du double de solutions par la suite, en navigant de lien en lien et en m'inscrivant à des newsletter m'envoyant des rapports tels que celui de l'éditeur FORRESTER écrit par Cser [2].

Nous avons ainsi pu nous retrouver avec une liste de solutions satisfaisante pour pouvoir commencer à faire un comparatif *réaliste* (terme à revoir). Nous avons alors orienté mes recherches vers les spécificités des solutions, en parcourant toute la documentation disponible, en participant à des vision-conférences avec les commerciaux et ingénieurs des maisons d'édition ou en contactant le support. Cette étape a été celle qui a pris le plus de temps dans la période de recherche, qui parfois s'est avérée infructueuse au vu du manque d'informations disponibles et de l'absence de réponse du support (ou plus précisément des réponses me redirigeant vers des documents en ligne ne contenant pas les réponses demandées). C'est par ailleurs une des étapes qui a complètement décalé le calendrier prévisionnel, prenant sur la marge prévue à cet effet.
Cette étape a conduit à éditer un tableau comparatif des solutions, dont nous pouvons trouver un aperçu à la FIGURE 2.2.2. Ce tableau comparatif n'est

13. Fonctionnement décrit dans un schéma en ANNEXE

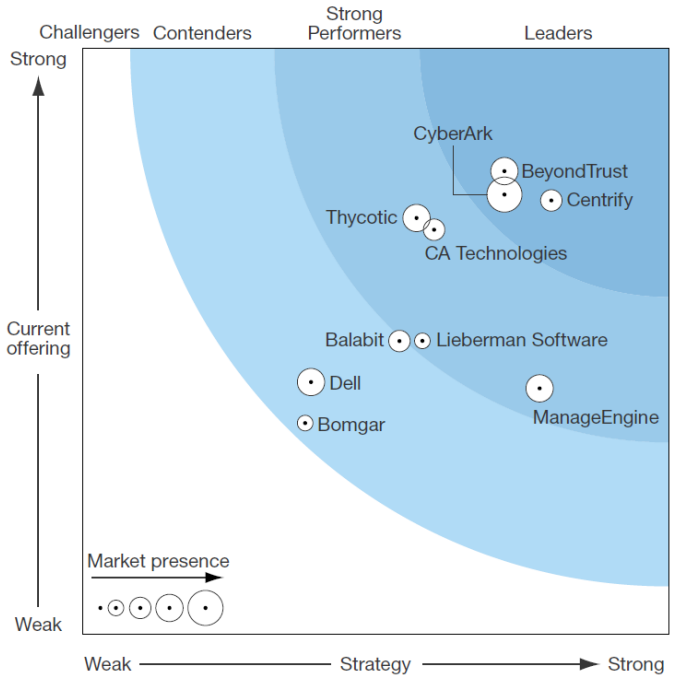

FIGURE 3 – Quadrant mettant en évidence les acteurs du marché de PAM selon le rapport offre/stratégie et l'indice de présence sur le marché

pas disponible en annexe, à cause de sa taille impossible à imprimer, mais il reste tout de même disponible sur demande en format *Microsoft Excel*.

2.3 Proof of Concept

La phase de conception d'environnement de test s'est déroulée en plusieurs étapes :

- Conception architecture idéale
- Validation de l'architecture avec le tuteur, et remaniement de cette dernière pour s'adapter aux ressources matériels disponibles chez SYNETIS, ressources assez limitées car nous étions en saturation de ressources mémoire et processeur sur le serveur interne. Un nouveau serveur est arrivé en fin de stage, mais malheureusement quelques semaines trop tard
- Installation de l'infrastructure et déploiement des solutions à tester

	A	L	M	N
1	Solutions / Caractéristiques	Secret Server	Vormetric Data Security Platform	AdminBastion
26	Condition de montée en privilèges	- Autorisations basées sur les rôles (role-based) - Approbation d'un supérieur (ou autre personne désignée)	Role LDAP	Basée sur un ensemble de règles prédéfinies
27	Check-out et check-in	- OTP		N/A
28	Session limitée dans le temps			+ plage horaire
29	**Monitoring**			
30	Enregistrement vidéo	Uniquement pour l'édition Enterprise plus		
31	Reconnaissance OCR			
32	Enregistrement des logs			
33	Contenu des logs	N/A	Protocole Syslog RFC5424	L'ensemble des sessions
34	Monitoring en direct			
35	Remonté d'alerte en direct			
36	Edition de rapports	- via un SIEM	- via compatibilité avec un SIEM	
37	**Aspect Financier**			
38	Modes de licensing	3 modes de licences : - Professional - Enterprise - Enterprise Plus - Version d'essai (Enterprise Plus) de 30 jours L'achat de la licence Professional se fait en ligne, les deux autres licences sont juste des upgrades de clef qui permettent l'accès à la licence supérieure. Chaque utilisateur doit avoir une adresse email liée à une clef de licence valide.	3 appliances : - VM (machine virtuelle) : le client doit fournir le serveur dédié - V6000 : serveur hébergeant l'application fourni - V6100 : serveur avec HSM hébergeant l'application fourni	5 Appliances physiques disponibles : - **WAP 50** : CPU : Pentium 1403 (2,6 GHz) - Dual Core RAM : 4 Go SAS : RAID 1 - 500 Go utile - Hot-plug Alim : Rendondante - Hot-plug - **WAP 200** : CPU : Xeon E5-2620 (2,4 GHz) - Hexa Core RAM : 8 Go SAS : RAID 1 - 1,2 To utile - Hot-plug Alim : Rendondante - Hot-plug - **WAP 600** : CPU : Xeon E5-2640 (2,6 GHz) - Octo Core RAM : 16 Go SAS : RAID 1 - 2,4 To utile - Hot-plug Alim : Rendondante - Hot-plug - **WAP 1000** : CPU : 2 * Xeon E5-2640 (2,6 GHz) - Octo Core RAM : 32 Go SAS : RAID 1 - 3,6 To utile - Hot-plug Alim : Rendondante - Hot-plug - **WAP 2000** : CPU : 2 * Xeon E5-2667 (3,2 Ghz) - Octo Core RAM : 64 Go SAS : RAID 1 - 1,8 To utile - Hot-plug Alim : Rendondante - Hot-plug
39	Coût des licences	Contacter les revendeurs (Thycotic n'est pas en France) : Vendeurs certifiés : - ADINES - Acternet - Nellsoft Revendeurs autorisés : - Atlantis		N/A
40	Légende :			
41	Condition remplie			
42	Condition non-remplie			

FIGURE 4 – Extrait du tableau comparatif de solutions édité au terme de la phase de recherche

2.3.1 Architecture

L'architecture idéale sur laquelle les solutions devaient être intégrée nous semblait être celle qui se rapprochait le plus d'une situation réelle d'entreprise, comprenant des séparations logiques pour les différents corps de métier (

En effet, les ressources limitées ont réduit notre infrastructure de test au strict minimum, donc une machine de chaque type :

— MS WINDOWS SERVER 2012 R2 : serveur de test de connexion RDP [14], de configuration des solutions de PAM (base de données *MySQL* et *SQL Server*), de mail (avec le logiciel *hMailServer* [3] et contrôleur de domaine *Active Directory*

14. Remote Desktop Protocol : contrôle à distance d'un serveur.

— MS Windows Server 2012 : serveur TSE[15] permettant de tester une connexion sur une application distante (*VMWare vSphere Client*[16] dans notre cas)

— Linux Debian 8.4.0 Jessie : serveur Linux permettant de tester une connexion SSH[17]

Cette architecture limitée nous a permis de tester et d'éprouver 2 des solutions choisies, tout en respectant les contraintes de ressources établies. Bien plus que les solutions en elles-même, le déploiement de l'infrastructure de base a nécessité d'autres technologies, que l'ont peut lister en tâches suivantes :

— Sur Microsoft Windows Server 2012 et 2012 R2 :
  → Installation du rôle contrôleur de domaine[18]
  → Création et configuration d'un domaine, d'une forêt et de toutes ses dépendances assurant le bon fonctionnement de l'infrastructure
  → Création d'utilisateurs de domaine[19] avec les droits nécessaires et suffisant à leur fonctionnement, grâce aux groupes de sécurité Windows (consulter le livre de Minasi *et al.* [4] pour plus d'informations sur Active Directory et la sécurité de Windows Server 2012 R2)
  → Création de comptes de service de domaine (MSA[20]) sous *Powershell*[21]
  → Installation de système de gestion de base de données relationnelle *MySQL* et *SqlServer* et création de bases de données pour les solutions de PAM
  → Installation et configuration d'un serveur de mail local *hMailServer* pour récupérer les mails envoyés par les solutions de PAM
  → Installation du rôle TSE et configuration de ce dernier avec l'application *VMWare vSphere Client*

— Sur Debian 8.4.0 :
  → Installation du serveur SSH
  → Configuration réseau

15. Terminal SErvice : permet d'utiliser le serveur pour faire tourner des applications utilisées en bureau distant.

16. Programme Windows permettant de configurer un hôte de virtualisation et de faire tourner des machines virtuelles.

17. Secure SHell : protocole de connexion à distance à une machine Linux/Unix.

18. gestionnaire d'un domaine sous le système d'exploitation Windows.

19. Utilisateurs créés dans un annuaire Active Directory, disponible pour toute machine du domaine.

20. Managed Service Account : compte Active Directory dédié aux service, le système gère lui-même les mots de passe.

21. Interface en ligne de commande et langage de scripting dédié à Windows.

2.3.2 Choix des solutions de PAM à tester

Nous avions fait, au terme de la phase de recherche, une sélection de 3 potentielles solutions à déployer sur nos environnements de test. Ce choix s'était fait en prenant en compte les données présentées dans le tableaux comparatif des solutions dont on a un aperçu dans la FIGURE 2.2.2. Ces 3 solutions étaient :

— WALLIX ADMINBASTION

— CYBERARK PRIVILEGED ACCOUNT SECURITY SUITE

— THYCOTIC SECRETSERVER

Nous étions déjà en contact avec *Wallix*, car partenaires et mon tuteur était en train de passer une formation avec eux, pour la solution en question. Nous avons donc pu avoir facilement une installation de leur solution. En revanche, étant partenaire de *Wallix*, *CyberArk* a refusé de nous fournir une version d'évaluation tant que nous n'abandonnions pas notre partenariat, afin qu'il devienne notre partenaire exclusif. Ce choix de *CyberArk* venant du fait que *Wallix* est leur plus gros concurrent en France, car *Wallix* est une entreprise Française et que beaucoup d'entreprises jouent le jeu de faire fonctionner une entreprise locale[22]. Nous avons donc déclineé la solution de *CyberArk* et sommes entrés en contact avec *Thycotic*, avec qui nous n'avons pas eu de soucis et qui nous ont offert un suivi remarquable (une communication omniprésente à toutes les étapes de test).

2.3.3 Déploiement : Wallix AdminBastion

La version d'essai de *Wallix AdminBastion* se présente sous forme d'une machine virtuelle (fichier `vmdk`[23]).
Cette machine virtuelle est un Debian 8 personnalisé par Wallix, avec leur propre configuration d'usine. Cette machine doit utiliser une base de données *MySQL* externe afin de stocker ses données (logs et accréditations). Nous avons donc créé une base de données sur le serveur *MySQL*

22. Information fournie par le troisième éditeur, *Thycotic* durant des échanges de mails.
23. VMWare Virtual Disk : format de disque virtuel créé par *VMWare*

3 Résultats et discussion

Corps de texte.

Conclusion

Une page tout au plus, résumé du travail accompli, faire apparaître si les objectifs ont été atteints, si de nouvelles difficultés ont été soulevées, propositions de solution et futur développement.

Références

[1] R.Baloch *Ethical Hacking Penetration Testing Guide*, Auerbach Publications ; 1 edition, 531 pages, 2014.

[2] Andreas Cser *The Forrester Wave^{TM} : Privileged Identity Management*, Forrester®, Q3 2016.

[3] hMailServer. Page consultée le : 02/08/2016. *Functionality - hMailServer - Free open source email server for Microsoft Windows*, Site web. URL : https ://www.hmailserver.com/functionality

[4] Minasi, Mark, et al. *Mastering Windows Server 2012 R2*, John Wiley & Sons, 2013.

[5] James E. Weber, Dennis Guster, Paul Safonov & Mark B. Schmidt, *Weak Password Security : An Empirical Study*, Information Security Journal : A Global Perspective, 17 :1, 45-54, DOI :10.1080/10658980701824432, 2008.

Annexe A

3.1 Fonctionnement détaillé des solutions de PAM

Nous détaillerons dans cette annexe, le fonctionnement détaillé d'une solution de PAM. Afin d'illustrer les propos tenus, nous nous appuierons sur des schémas et digrammes de séquences.
Avant d'expliquer le fonctionnement d'une solution de PAM, nous allons voir comment les systèmes fonctionnent en temps normal.

3.1.1 Sans solution de PAM

Dans ce scénario, les utilisateurs finaux possèdent le mot de passe d'accès direct à la ressource protégée, comme on peut le voir sur la FIGURE 5.

FIGURE 5 – Connexion à une ressource protégée sans solution de PAM

On remarque qu'ici, les utilisateurs accèdent directement aux ressources protégées avec des mots de passe dédiés à chaque service/application/matériel. Il est donc très fréquent car inévitable que des utilisateurs partagent le même mot de passe. De plus, n'ayant aucune fédération (pas de supervision, ni de traçage), l'utilisateur est apte à effacer ses traces, par exemple en vidant les logs des applications et de ses actions[24].
On ne peut donc pas savoir ce que l'utilisateur a fait, ni quel utilisateur a fait des actions sur la ressource cible.
Le diagramme de séquence en FIGURE 6 décrit en détail les action qui se déroulent lors d'une telle connexion. Il permet de ausi de mettre en évidence l'absence de contrôle des utilisateurs : aucun registre d'évènements ne prend en compte les actions des utilisateurs. Les utilisaterus se partageant le même mot de passe pour chaque ressource cible, le contrôle n'est ainsi plus mis sur

24. Par exemple sous Debian 8, la commande `cat /dev/null > /.bash_history && history -c && exit` supprime toute action effectuée sur la machine avec le compte courant.

les utilisateurs, mais sur les ressources cibles, ce qui est l'opposé de ce que nous cherchons à faire. La Figure 7 schématise cette inversion du contrôle.

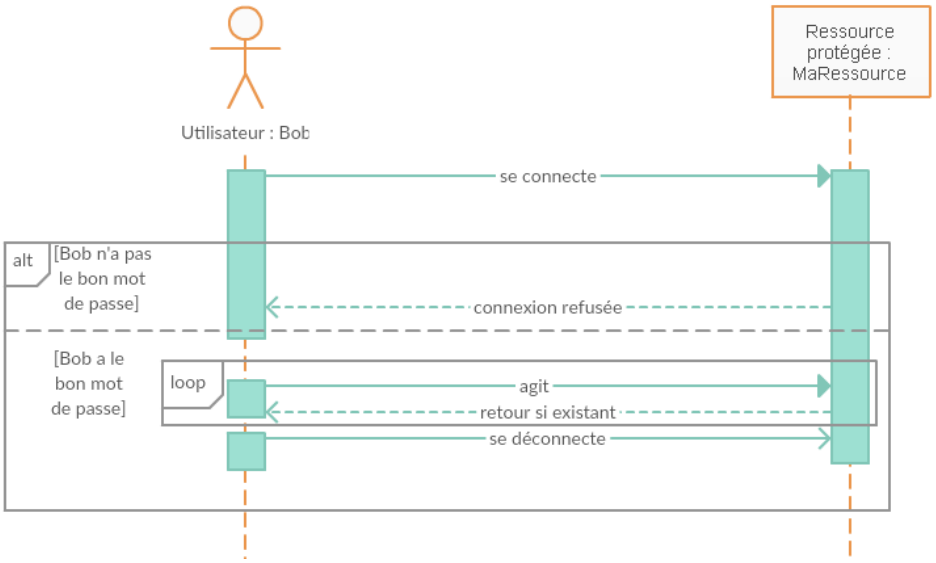

FIGURE 6 – Diagramme de séquence détaillant les actions effectuées lors d'une connexion à une ressource sans solution de PAM

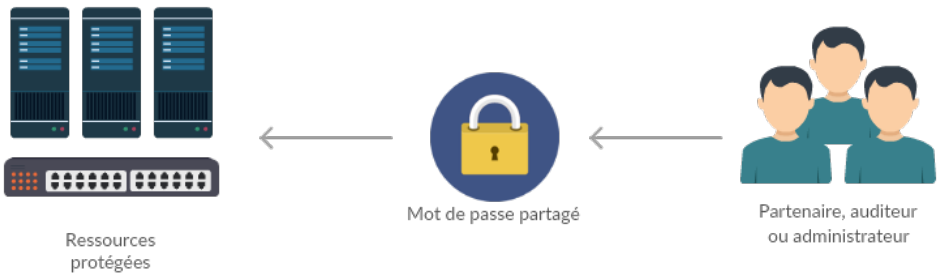

FIGURE 7 – Schéma mettant en évidence l'inversion du contrôle de sécurité, mis sur les ressources plutôt que sur les utilisateurs

3.1.2 Avec solution de PAM

Dans ce scénario, une solution de PAM est en place. Ainsi les utilisateurs n'ont pas d'accès direct aux ressources cible. Toute l'architecture s'articule autour d'un composant central : le contrôleur d'accès appelé **bastion**. Tout accès à une ressource cible se fait via ce bastion. Cette architecture centralisée est schématisée dans la FIGURE 8. Nous allons reprendre point par point un

scénarion de connexion réussie à une ressource cible (en correspondance avec les étapes de la FIGURE 8).

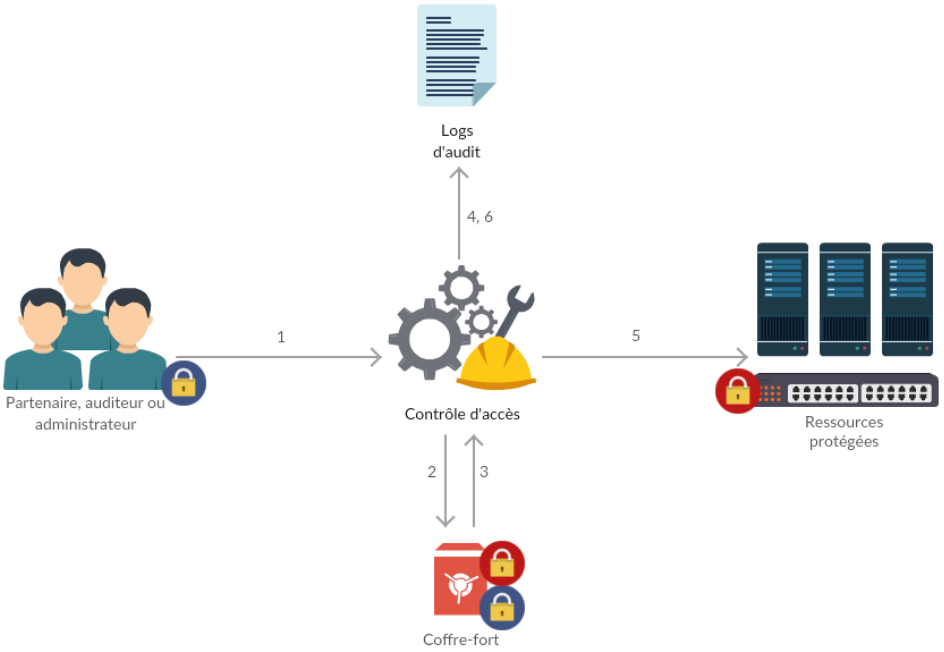

FIGURE 8 – Schéma décrivant l'architecture d'une solution de PAM intégrée dans une infrastructure

1. L'utilisateur se connecte au bastion avec ses crédentiels

Résumé La gestion des comptes à privilèges est un domaine clef de la gestion d'accès et d'identité. Elle permet de suivre et journaliser les activités des comptes ayant des droits élevés comme `root` sur Linux/UNIX ou `Administrateur` sur Windows. Cette gestion permet ainsi de retrouver une erreur de configuration ayant entrainé une perturbation des services, de prévenir les intrusions par escalade de privilèges sur les système et de suivre d'éventuels prestataires de service dans un grand groupe (sous-traitance de la maintenance d'un service). Les solutions commerciales offrent différentes approches de la problématique des comptes à privilèges. Ce stage a donc fait l'objet d'une étude de ces différentes solutions, de leurs fonctionnalités et de leur fonctionnement. Cette étude a permis de faire ressortir 3 produits, Wallix AdminBastion, CyberArk Privileged Access Security Solution et Thycotic Secret Server, pour finalement en déployer 2 dans un environnement de test virtualisé. Cette mise en situation nous a permis d'aller plus en profondeur dans la compréhension du fonctionnement de la gestion des comptes à privilèges, des points traités et des points nécessitant des traitement supplémentaires à la diminution des risques des comptes à privilèges.

Abstract The management of privileged accounts is a key area of access and identity management. It can track and log activity of accounts with elevated privileges such as `root` on Linux/UNIX or Windows `Administrator`. This allows to recover a misconfiguration that caused a disruption of services, prevent intrusions by escalating privileges on the system, and monitor potential service providers in a large groups (outsourcing of maintenance service). Commercial solutions offer different approaches to the problem of privileged accounts. This internship has been the subject of a study of these different solutions, their functionalities and operation. This study allowed us to highlight three products : Wallix AdminBastion, CyberArk Privileged Access Security Solution and Thycotic Secret Server, to finally deploy in 2 proof of concept. This development has allowed us to go further in understanding the operation of the management of privileged accounts, treaties points and points requiring additional treatment to lower risk on privileges accounts.