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

La gestion de comptes à privilèges (PAM[2]) est une sous-section de la gestion d'identité et d'accès (IAM[3]). 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

2. Privileged Access Management
3. Identity and Access Management

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[4] 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 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[5].

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

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[6]. 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[7], 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.

4. Element permettant d'exploiter une faille de sécurité
5. 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
6. Attaque sur un serveur par exemple
7. A2A : Application To Application, littéralement d'application à application

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 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

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 [8].

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

Le serveur central a à sa charge de protéger les mots de passe dans un coffre-fort et de les renouveler régulièrement.

[Intégrer schéma USER <-> BASTION <-> RESSOURCE]

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 [9] : les ressources et les comptes d'utilisateurs sont séparés physiquement (ou logiquement [10]), 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

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 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

—

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

9. Toutes les communications transitent par un point de contrôle.
10. Redirection des paquet par port.

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 2 sous-sections : l'une traitant de la phase de recherche d'informations, avec ses problèmes rencontrés et solutions trouvée, puis une seconde décrivant le travail effectué pendant la phase de test des deux produits sur un environnement de test.

2.1 Recherche

N'étant pas spécialisé dans le domaine de la gestion d'identité car ayant une formation en réseau et système, le sujet des comptes à privilèges fut une découverte pour moi, et donc beaucoup de recherches à tatton

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.

[LPP] Rolland. *LaTeX par la pratique*. O'Reilly, 1999.

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.