جامعة مولاي إسماعيل
UNIVERSITÉ MOULAY ISMAÏL

المدرسة العليا للأساتذة
ÉCOLE NORMALE SUPÉRIEURE

Année 2023-2024

RAPPORT DE PROJET – LE INFORMATIQUE

OPERATING SYSTEM Linux « Secure Shell»

Projet réalisé par
Zakaria El Omari
Mohammed El Ouardi
Taha Yassine Taabani

Projet encadré par
Dr. Mehdi Moukhafi

,Nous tenons à vous remercier monsieur le professeur MOUKHAFI chaleureusement pour votre enseignement dédié au système d'exploitation Linux. Votre passion pour le sujet et votre soutien continu ont rendu le cours enrichissant.

Les opportunités que vous nous avez offertes pour présenter des exposés nous ont permis d'approfondir nos connaissances et de découvrir de nouvelles perspectives. Votre investissement dans notre formation n'est pas passé inaperçu, et nous sommes reconnaissants pour les compétences que nous avons acquises grâce à votre guidance.

Merci encore pour tout.

SOMMAIRE

1. INTRODUCTION

Le réseau informatique constitue un élément central dans l'infrastructure technologique contemporaine, fournissant la connectivité essentielle pour les systèmes et les utilisateurs. Cette étude explore divers aspects cruciaux des réseaux informatiques, en se concentrant sur les modèles TCP-IP/OSI, les protocoles de sécurité SSH/SSL, et l'outil d'automatisation ANSIBLE.

La première section offre une introduction détaillée aux réseaux informatiques, définissant leur nature et leurs objectifs fondamentaux. Elle examine également les modèles de référence TCP-IP/OSI qui sous-tendent le fonctionnement des réseaux modernes.

La deuxième section se penche sur la sécurité des communications en se concentrant sur les protocoles SSH et SSL. Elle explore l'historique du SSH, son positionnement dans les modèles TCP-IP/OSI, et souligne l'importance des clés SSH pour renforcer la sécurité des connexions.

ANSIBLE, l'outil d'automatisation de configuration, est ensuite abordé dans la troisième section. Cette partie décrit les principes fondamentaux d'ANSIBLE et met en lumière son utilisation synergique avec le protocole SSH, ainsi que l'utilisation du langage YAML dans la configuration.

La quatrième section détaille la configuration pratique du SSH et d'ANSIBLE, couvrant l'installation, la connexion des machines via SSH, la génération de clés SSH, et l'automatisation de tâches spécifiques à l'aide d'ANSIBLE.

Wireshark, un outil d'analyse réseau, est exploré dans la cinquième section, couvrant sa définition, son installation, et évoquant les menaces potentielles liées à son utilisation.

Enfin, la dernière section synthétise les résultats obtenus, tirant des conclusions significatives sur l'importance des protocoles de sécurité dans les réseaux informatiques, l'efficacité d'ANSIBLE dans la gestion des configurations, et les risques liés à l'utilisation de Wireshark.

2. Introduction au réseau informatique

a. Définition réseau informatique et ces objectifs

Un réseau informatique constitue une structure fondamentale permettant l'interconnexion de systèmes et de dispositifs. Son objectif principal est de faciliter le partage efficace de ressources et d'informations entre ces entités, favorisant ainsi la communication, la collaboration, et la mise en commun de données, de fichiers, ainsi que de périphériques.

b. Les modèles TCP-IP/OSI

Le Modèle OSI :

Le modèle OSI, ou Open Systems Interconnection, est une norme de référence internationale pour la conception et le fonctionnement des réseaux informatiques. Il se compose de sept couches, chacune remplissant un rôle distinct dans le processus de communication.

1.Couche Physique (1ère couche) :

Gère les aspects matériels de la transmission des données, définissant les caractéristiques électriques, mécaniques et fonctionnelles des interfaces physiques.

2.Couche de Liaison de Données (2ème couche) :

Responsable de la communication point à point entre deux dispositifs connectés directement. Elle assure également la détection et la correction d'erreurs au niveau de la liaison.

3. Couche Réseau (3ème couche) :

Gère la transmission de données à travers le réseau en déterminant le chemin optimal entre l'expéditeur et le destinataire. C'est la couche qui implémente le routage des paquets.

4. Couche Transport (4ème couche) :

Assure le transport fiable et efficace des données entre les applications des utilisateurs, en prenant en charge le contrôle de flux, la segmentation des données, et la gestion des erreurs.

5.Couche Session (5ème couche) :

Établit, maintient et termine les sessions de communication entre les applications sur différents dispositifs, permettant une gestion cohérente des échanges.

6.Couche Présentation (6ème couche) :

Gère la traduction, la compression et le chiffrement des données, assurant la compatibilité entre les différents systèmes.

7.Couche Application (7ème couche) :

Fournit des interfaces pour les applications réseau, offrant des services directs aux utilisateurs.

Le Modèle TCP/IP :

Le modèle TCP/IP, ou Transmission Control Protocol/Internet Protocol, est un ensemble de protocoles largement utilisé pour les communications sur Internet. Il se divise en quatre couches, regroupées en deux catégories : la couche hôte et la couche réseau.

1.Couche Application (Hôte) :

Fournit des interfaces pour les applications réseau, similaire à la couche Application du modèle OSI.

2.Couche Transport (Hôte) :

Gère le transport de données de bout en bout, assurant la fiabilité de la communication, correspondant à la couche Transport du modèle OSI.

3.Couche Internet (Réseau) :

Responsable du routage des paquets à travers le réseau, correspondant à la couche Réseau du modèle OSI.

4.Couche Accès Réseau (Réseau) :

Gère l'accès au support physique, la détection d'erreurs, et le contrôle de flux, regroupant les fonctions des couches Physique et de Liaison de Données du modèle OSI.

Cette comparaison met en lumière les similitudes et les différences entre les deux modèles, offrant une compréhension approfondie des couches et de leurs rôles respectifs dans le fonctionnement des réseaux informatiques.

3. SSH/SSL

a. Définition SSH et son but

SSH, acronyme de "Secure Shell," est un protocole de communication sécurisé conçu pour permettre un accès sécurisé à des systèmes distants sur un réseau non sécurisé. Il établit un canal sécurisé sur une connexion typiquement non sécurisée, comme l'Internet, en utilisant des techniques de chiffrement pour protéger les données transitant entre le client et le serveur.

b. L'histoire du SSH

Début (années 1990) :Tatu Ylönen crée SSH comme une alternative sécurisée pour l'accès à distance.

Évolution (milieu à fin des années 1990) : SSH-2 est introduit, devenant un standard de facto pour la sécurité dans les communications.

Défis (années 2000) : Découverte de vulnérabilités, nécessitant des mises à jour régulières pour maintenir la sécurité.

Intégration moderne (années 2010 à aujourd'hui) : SSH devient essentiel dans la sécurité informatique, utilisé pour l'accès distant, le transfert de fichiers sécurisé et la gestion des identités.

c. Positionnement du SSH dans TCP-IP/OSI

OSI: SSH (Secure Shell) se positionne principalement au niveau de la couche application du modèle OSI.

- Il opère au-dessus des couches de transport (par exemple, TCP) et de réseau (par exemple, IP), assurant ainsi une sécurisation des données à un niveau élevé dans la pile de protocoles.

TCP/IP: Dans le modèle TCP/IP, SSH s'insère également au niveau de la couche application, correspondant à la couche d'application du modèle OSI.

- Il utilise des protocoles de transport sous-jacents tels que TCP pour assurer la fiabilité de la communication.

d. SSL en résumé

Le SSL (Secure Sockets Layer) est une technologie standard de sécurisation des connexions Internet. Il assure le chiffrement des données transitant entre un navigateur et un site web (ou entre deux serveurs), protégeant ainsi les informations personnelles, financières, etc., contre les hackers.

e. SSH keys et Hashage pour sécuriser la connexion

Les clés SSH, ou clés de chiffrement Secure Shell, sont une méthode de sécurisation des connexions réseau, notamment utilisée pour l'accès à distance à des serveurs. Le principe de base est le chiffrement asymétrique, impliquant l'utilisation de deux clés distinctes : **une clé privée et une clé publique.**

Clé Privée: C'est la clé secrète utilisée pour signer numériquement les données et déchiffrer les informations chiffrées par la clé publique correspondante.

Clé Publique: C'est la clé partagée publiquement, utilisée pour vérifier la signature numérique créée par la clé privée et pour chiffrer les données.

Hashage en Relation avec les SSH Keys:

Le hashage renforce la sécurité des SSH Keys en ajoutant une couche de protection supplémentaire. Lorsque les clés SSH sont générées, leurs empreintes, également appelées fingerprints, sont obtenues via des fonctions de hachage cryptographique. Ces empreintes servent de "résumé" unique et fixe des clés.

Fonctionnement du Hashage en SSH Keys:

1.Génération de Paires de Clés: Un utilisateur génère une paire de clés (publique et privée) sur son ordinateur.

2.Établissement d'une Connexion SSH:Lorsqu'une connexion SSH est établie, le serveur utilise la clé publique pour chiffrer un message.

3.Chiffrement et Signature: Le chiffrement asymétrique permet au serveur de créer un hash du message chiffré.

La clé privée de l'utilisateur est utilisée pour signer numériquement ce hash.

4.Comparaison des Empreintes: Le serveur compare l'empreinte de la clé publique reçue avec l'empreinte générée localementl. La correspondance vérifie l'identité de l'utilisateur.

L'utilisation du hashage avec les SSH Keys renforce la sécurité en permettant la vérification d'identité, en garantissant l'intégrité des données échangées, et en résistant aux attaques potentielles. Cette méthode robuste assure des connexions sécurisées dans les environnements réseau, contribuant à la protection fiable des données sensibles.

4. ANSIBLE

a. C’est quoi ANSIBLE L’utilisation du SSH dans l’ANSIBLE

C’est quoi ANSIBLE et l’utilisation du SSH dans l’ANSIBLE:

Ansible est une plateforme open source d'automatisation des configurations et du déploiement d'infrastructures informatiques. Elle simplifie les tâches répétitives liées à la gestion de configuration, au déploiement d'applications, et à l'orchestration des infrastructures. Ansible, développé par Red Hat, est écrit en Python et repose sur un modèle déclaratif. Dans ce modèle, les utilisateurs décrivent simplement l'état souhaité du système, et Ansible se charge d'appliquer ces états sur les machines cibles.

b. YAML

En Ansible, YAML (YAML Ain't Markup Language) est un langage de sérialisation de données utilisé pour décrire les configurations. Il est employé dans les fichiers de configuration Ansible tels que les playbooks, les fichiers de variables et les inventaires. La syntaxe YAML est basée sur l'indentation, favorisant la lisibilité, et permet de définir des tâches, des rôles, et d'autres éléments nécessaires à l'automatisation des infrastructures de manière concise. Son utilisation simplifie la rédaction et la lecture des fichiers de configuration Ansible.

Utilisation du SSH dans Ansible:

Ansible utilise le protocole SSH pour établir des connexions sécurisées avec les machines cibles. Cette approche offre plusieurs avantages, notamment la simplicité, la sécurité, et la capacité à fonctionner sans agent sur les machines cibles. Lorsqu'une tâche est exécutée via Ansible, le protocole SSH est utilisé pour établir une connexion avec la machine distante, permettant ainsi le déploiement des configurations et l'exécution des opérations automatisées de manière sécurisée.

En résumé, Ansible, en conjonction avec le protocole SSH, offre une solution puissante pour automatiser les opérations de configuration et de déploiement, garantissant une gestion efficace des infrastructures informatiques. L'utilisation du langage YAML contribue également à rendre les configurations plus compréhensibles et maintenables.

5. Configuration du SSH et ANSIBLE

A voire le readme file pour plus d'informations sur la configuration et l'installation.

6. Wireshark

a. C’est quoi Wireshark

Wireshark est un outil open- source d'analyse de paquets réseau qui permet de capturer, visualiser, et inspecter le trafic sur un réseau. Il offre une compréhension approfondie du fonctionnement des communications réseau en examinant les paquets de données qui transitent entre les différents points du réseau.

b. Installation du Wireshark

A voire le readme file pour plus d'informations sur l’installation.

7. Analyse des résultats (conclusion)

En examinant les résultats de la simulation avec SSH, on peut montrer que les données échangées entre le client et le serveur sont sécurisées. Le chiffrement des données par SSH garantit que même si un attaquant intercepte les paquets, il ne peut pas comprendre le contenu, car il est chiffré.

La comparaison visuelle des données capturées avec Wireshark dans les deux scénarios soulignera la sécurité renforcée offerte par SSH. Les informations sensibles, telles que les identifiants de connexion, les commandes, ou les données confidentielles, restent confidentielles et ne peuvent pas être exploitées par un tiers non autorisé.

On peut également mettre en avant le mécanisme d'authentification forte de SSH, qui ajoute une couche supplémentaire de sécurité en vérifiant l'identité des parties impliquées dans la communication.

Intégrant Ansible, une plateforme d'automatisation s'appuyant sur SSH, renforce la cohérence et la sécurité des opérations informatiques, permettant des processus automatisés fiables. En résumé, la combinaison de SSH et Ansible offre une solution complète pour des communications sécurisées et une gestion automatisée des infrastructures.

Annexes

Readme file pour plus d'information sur la configuration.

Les ressources :

- https://wiki.archlinux.org/title/Secure_Shell
- https://wiki.archlinux.org/title/Ansible
- https://wiki.archlinux.org/title/Wireshark
- https://www.geeksforgeeks.org/tcp-ip-model/
- https://www.digicert.com/fr/what-is-ssl-tls-and-https
- https://docs.ansible.com