PROJET

RÉSEAUTIQUE ET SÉCURITÉ

1 Introduction

1.1 Objectif du projet

Ce projet a pour but de centraliser les journaux d'activité (logs) au sein de l'environnement virtualisé/conteneurisé présenté à la Figure 1, afin de renforcer la gestion de la sécurité.

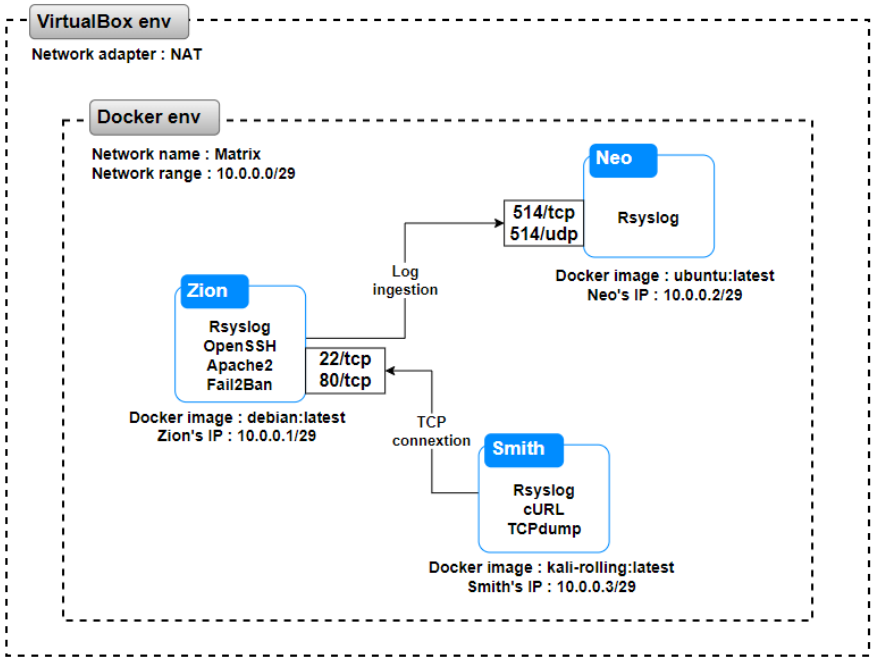

FIGURE 1 – Topologie de l'infrastructure cible

1.2 Description de l'infrastructure

Dans l'infrastructure cible dont la topologie est illustrée à la Figure 1, les noms des machines, serveurs et réseaux reflètent les personnages et les lieux clés de la série de films Matrix.

- `Zion` est le serveur contenant les actifs critiques de la `Matrix` à absolument protéger
- `Neo` est le serveur de centralisation des journaux d'activité (logs) générés dans la `Matrix`
- `Smith` est la machine de tests de connexion et de balayage (scan) de la `Matrix`

1.3 Etapes préliminaires

Plusieurs outils/technologies permettent la mise en place de la topologie illustrée à la Figure 1. Dans le cadre de ce projet, nous assumons les choix proposés.

1. Téléchargez et installez l'hyperviseur de type 2 VirtualBox (lien 1)
2. Téléchargez et décompressez la VM préconstruite Kali Linux (lien 2)
3. Importez Kali Linux à l'intérieur de VirtualBox (lien 3)
4. Installez Docker Engine dans Kali Linux (lien 4)

2 Mise en place de l'infrastructure [/10 pts]

1. En vos propres mots, expliquez le rôle et le fonctionnement de `rsyslog` et `Fail2Ban`.
2. En vos propres mots, expliquez le concept de « Infrastructure as a Code (IaaC) » .
3. Quels problèmes `Docker` et `Docker-compose` permettent-ils de résoudre dans le domaine du développement et du déploiement d'applications ?
4. Mettez en place l'infrastructure précédemment décrite en utilisant le principe de IaaC avec Docker et Docker-compose. Ci-après, quelques informations supplémentaires :
   — Toutes les configurations de filtrage réseau (parefeu/firewall) sont purgées par défaut.
   — Le serveur `Neo` est configuré pour recevoir uniquement les flux rsyslog du serveur `Zion`.
   — Les journaux d'activité (logs) générés par les services `OpenSSH` et `Apache2` sur le serveur `Zion` sont configurés pour être envoyés vers le serveur `Neo`.
   — Toute adresse IP qui échoue à établir une connexion SSH au serveur `Zion` plus de deux fois en l'espace de 5min est automatiquement bloquée pour une durée de 1h.
   — Le serveur web `Apache2` est configuré pour servir les pages web disponibles (ici).

Note importante : Assurez-vous de fournir l'ensemble des fichiers de configuration utilisés dans la mise en place de votre infrastructure (.yml, .conf, .sh, etc.), ainsi qu'un fichier `README.md` qui détaille les étapes à suivre pour la reconstituer.

3 Tests de journalisation et IDS/IPS [/6 pts]

1. Effectuez 4 tentatives de connexion SSH au serveur `Zion` à partir de la machine `Smith`, en réussissant 2 fois et échouant 2 fois. Que constatez-vous dans les journaux d'activité (log) du serveur `Neo` ?
2. Accédez aux pages web `/Oracle.html` et `/Trinity.html` de votre serveur web à partir de la machine `Smith`, en utilisant la commande curl. Que constatez-vous dans les journaux d'activité (log) du serveur `Neo` ? Que contient la page web `/Oracle.html` ?
3. Effectuez une capture réseau en utilisant la commande tcpdump pendant que vous refaites les questions 3.1 et 3.2. Utilisez Wireshark pour identifier le port et le protocole de la couche de transport utilisés pour le service rsyslog.
4. Purgez les règles de parefeu sur le serveur `Zion` et `Neo`. Quels constats faites-vous concernant les règles de pare-feu après avoir refait les questions 3.1 et 3.2 ?

Utilisez scp pour le transfert de fichiers de vos conteneurs vers votre machine virtuelle.

4 Sécurité des journaux d'activités (logs) [/2 pts]

1. Comment configureriez-vous rsyslog pour prendre en charge les adresses IPv6 ?
2. Quels sont les avantages de centraliser les journaux d'activité (log) ? Faut-il préférer un serveur de centralisation local ou distant, et pourquoi ?
3. L'une des étapes de la post-exploitation lors d'une cyberattaque est la couverture des traces. Lorsque les logs sont stockés en local, ils peuvent subir des altérations de la part des attaquants, les rendant ainsi inexploitables pour les analystes.

   (a) Expliquez le principe de l'attaque par injection de log « log injection ».

(b) Est-ce que la suppression d'un fichier log crée une entrée log ? Justifiez votre réponse.

(c) Il est de bonne habitude de garantir la suppression automatique des logs au-delà de leur durée de retention. Pour cela, une « politique de rotation des journaux » est mise en œuvre au sein du système de journalisation. Quel commentaire pouvez-vous faire ?

5 Consignes et livrables [/2 pts]

— La date de remise du projet est configurée sur Moodle
— La formation des équipes se déroule sur Moodle avant le 04 mars 2024 à 12h00 EDT
— Veuillez conserver le nom des machines, des réseaux et les adresses IPs spécifiés.
— Veuillez conserver la numérotation des questions dans votre rapport.
— Veuillez fournir en un seul fichier compressé les livrables ci-dessous :
  — Section 2 : tous les fichiers de configuration utilisés (.yml, .conf, .sh, etc.)
  — Section 3 et 4 : un rapport ne dépassant pas 3 pages, y compris la page de garde. Ce rapport devra contenir des réponses précises et succinctes aux questions posées. Aucune introduction ni conclusion n'est requise. Pas de commentaire superflux !

6 Pénalités

Des pénalités seront appliquées pour les éléments suivants, sans être exhaustifs :
— Incapacité à travailler en équipe
— Non respect du nombre de page(s) indiqué
— Absence de soumission ou soumission tardive des livrables
— Absence de mention des membres de l'équipe dans les livrables

7 utilisation des SIAG (Systèmes d'Intelligence Artificielle Générative)

Veuillez consulter l'avis à la communauté de Polytechnique Montréal à ce sujet.

8 Ressources utiles

1. Docker
2. Docker-compose
3. Rsyslog
4. OpenSSH
5. Apache2
6. Fail2Ban