Plan De Travail

Guenfaf Hicham

2020-06-06

Problématique:

La technologie de conteneurisation doit être déployée dans nos centres de données en raison du grand nombre de fonctionnalités et de capacités qu'aucune autre technologie ne le fera, mais en raison de son âge relativement jeune, elle n'est pas vraiment aussi répandue qu'elle devrait l'être et le principal facteur en est corrélé au manque de connaissances et de documentation nécessaires sur certaines fonctionnalités avancées ou même de base. L'autre aspect du problème est que la plupart des administrateurs des système ne veulent pas réellement quitter leur zone de confort, retombant vers la virtualisation afin de ne pas avoir à traiter les problèmes émergents de cette technologie, principalement l'aspect sécurité de celle-ci.

Dans la communauté de la cybersécurité d'aujourd'hui, il est un fait que les conteneurs et la conteneurisation en général ne sont pas encore assez mûrs dans un aspect cybersec pour être déployés directement en l'absence de tout type de mesures de sécurité externes, et même avec cela en place, les déployeurs de conteneurisation sont toujours vulnérable à une source externe de menace qui échappe totalement à son contrôle.

Le 25 avril 2019, une base de données d'images de conteneurisation appelée "Dockerhub"[1] a été violée par un attaquant inconnu comme indiqué dans un article de suivi de **hackernews**[2] juste après la divulgation,

> **"Docker Hub, l'une des plus grandes bibliothèques basées sur le cloud d'images de conteneurs Docker, a subi une violation de données après qu'un attaquant inconnu ait eu accès à la base de données Hub unique de l'entreprise."**

Après avoir surveillé l'incident, l'équipe Dockerhub a réagi le plus rapidement possible pour éviter d'autres pertes et a averti ses utilisateurs:

[1] Docker images https://hub.docker.com

[2] ycombinator @ https://news.ycombinator.com

> **"Le jeudi 25 avril 2019, nous avons découvert un accès non autorisé à une seule base de données Hub stockant un sous-ensemble de données utilisateur non financières. Lors de la découverte, nous avons agi rapidement pour intervenir et sécuriser le site."**

Et concernant les dommages causés, l'article indiquait:

> **"La violation aurait exposé des informations sensibles pour près de 190000 utilisateurs du Hub (soit moins de 5% du nombre total d'utilisateurs), y compris les noms d'utilisateur et les mots de passe hachés pour un petit pourcentage des utilisateurs concernés, ainsi que des jetons Github et Bitbucket pour les référentiels Docker ."**

La société n'a pas donné plus d'informations sur la manière dont sa base de données a été violée.

Ce type de *cyber attaques* est en général fatal car il cible un système de distribution de confiance publique, chargé de fournir des images de base partout dans le monde où il est utilisé dans une multitude d'applications pour les systèmes bancaires électroniques, les bases militaires, etc. Sera sous le contrôle du pirate informatique.

C'est l'un des nombreux cas qui montre à quel point l'infrastructure de conteneurisation est délicate.

Ce type de *cyber-attaques* est en général fatal car elles ciblent un système de distribution de confiance publique, chargé de fournir des images de base partout dans le monde où il est utilisé dans une multitude d'applications comme par exemple les systèmes bancaires, les bases militaires, etc. Être sous le contrôle du pirate informatique. C'est l'un des nombreux cas qui montre à quel point l'infrastructure de conteneurisation est délicate.

À ce stade, nous nous retrouvons avec quelques questions majeures:

- La conteneurisation est-elle vraiment aussi peu sécurisée?
- Comment l'utiliser correctement?
- Comment créer un environnement sans risque pour cette technologie relativement jeune?
- Quels sont les outils à notre portée en ce moment qui vont nous aider à atténuer ce genre d'événements malveillants à l'avenir?

Sur la base de ce que nous avons vu, nous pouvons conclure que la conteneurisation ne va pas vraiment contenir les cybermenaces, du moins pas aussi bonnes que la virtualisation. *ARES Algérie* a décidé de faire progresser la sécurité de la conteneurisation dans son infrastructure en mettant en œuvre une solution hybride où les deux technologies, notamment la virtualisation et la conteneurisation, travaillent côte à côte pour de meilleures normes de sécurité à tous les niveaux.

Objectifs :

Principale

1. Comprendre les concepts de base du sujet
    i. Virtualisation
    ii. Conteneurisation
2. Configuration de la virtualisation Qemu / kvm sur l'hôte
    i. Machine Virtuel de virtualisation Archlinux avec hyperviseur Qemu / kvm imbriqué avec interface utilisateur Web
    ii. Machine Virtuel de conteneurisation Fedora avec Docker & docker compose
3. Configuration de Docker dans un environnement virtualisé
4. Renforcement des VM[3] / hôtes de la conteneurisation
5. Configuration d'un environnement sécurisé pour les conteneurs Docker

Auxiliaire

1. Rendre Qemu plus facile à apprendre en utilisant une interface Web
2. Manipulation de l'image disque depuis la ligne de commande

[3]Virtual Machine

Plan De Travail

La topologie du réseau contient 3 machines au total, un seul *hôte* qui exécute **`Archlinux`** [Linux] comme système d'exploitation, et deux **VM** *invitées* au-dessus de l'*hôte*, l'une pour la **Conteneurisation** et l'autre pour la **Virtualisation**; Les deux exécutent respectivement **`Fedora`** et **`Archlinux`** .

I. La machine principale ou l'*hôte* exécute les programmes suivants

   - Qemu/KVM
   - Libvirt
   - VirtManager
   - Openvswitch (OVS)

II. La premier machine *invité* est une **VM** de conteneurisation **`Fedora`**

   - Docker
   - Docker Compose
     - Nextcloud
     - Syncthing
     - Duplicati
     - Perkeep
     - Jellyfin
   - SELinux
   - cgroups

III. La deuxième machine *invité* est une **VM** de virtualisation **`Archlinux`** exécutant

   - Qemu/KVMM
   - Apache Web Server
   - Custom Qemu/KVM Web UI