Lab 3 : Sécurité de KVM sur Ubuntu

Objectif du Lab

Dans ce laboratoire, nous allons explorer la sécurisation de KVM (Kernel-based Virtual Machine) sur une machine Ubuntu. Vous apprendrez à configurer KVM pour garantir une isolation et une sécurité accrues des machines virtuelles. Nous allons aussi examiner des techniques pour sécuriser les communications entre les hôtes et les machines virtuelles et protéger les ressources critiques.

Prérequis

Avant de commencer ce laboratoire, assurez-vous que vous avez les éléments suivants :
- Une machine Ubuntu (Ubuntu 20.04 ou version plus récente)
- Accès root ou sudo pour installer des paquets
- KVM et les outils associés installés sur votre machine Ubuntu.

Installation de KVM sur Ubuntu

1. Mettez à jour les paquets de votre système Ubuntu :
```
$ sudo apt update && sudo apt upgrade -y
```

2. Installez KVM, QEMU et libvirt :
```
$ sudo apt install qemu-kvm libvirt-daemon-system libvirt-clients bridge-utils virt-manager
```

3. Vérifiez que KVM est installé correctement en exécutant :
```
$ kvm-ok
```

Cela devrait vous indiquer si votre système prend en charge KVM.

Création d'une Machine Virtuelle Sécurisée

Une fois KVM installé, nous allons créer une machine virtuelle sécurisée en utilisant 'virt-manager'.

1. Lancez Virt-Manager :
```
$ sudo virt-manager
```

2. Créez une nouvelle machine virtuelle en choisissant l'ISO d'un système d'exploitation léger comme Ubuntu Server.

- Suivez les étapes pour allouer des ressources CPU, mémoire et disque.
- Lors de la création, sélectionnez 'Utiliser un réseau privé' pour limiter l'accès réseau.
- Configurez le système pour qu'il ne soit accessible que par SSH sécurisé.

3. Avant de démarrer la machine virtuelle, configurez les paramètres de sécurité dans 'virt-manager' :
- Activer la virtualisation avec TPM (Trusted Platform Module) et Secure Boot si pris en charge.
- Désactiver les périphériques inutiles dans la configuration de la machine virtuelle pour minimiser la surface d'attaque.

Note : Le **TPM** est une puce de sécurité intégrée dans certains ordinateurs, serveurs et autres dispositifs électroniques. Elle est conçue pour renforcer la sécurité matérielle en stockant des informations sensibles, comme des clés de chiffrement, de manière isolée du reste du système.

Sécurisation des Communications Réseau

Les communications réseau sont un vecteur d'attaque majeur. Il est donc essentiel de sécuriser les échanges réseau.Voici quelques bonnes pratiques :

1. Utilisez des réseaux virtuels isolés (VLAN) pour chaque machine virtuelle.
2. Activez le chiffrement pour les connexions SSH en modifiant les paramètres du fichier '/etc/ssh/sshd_config'.
3. Déployez des firewalls au niveau de l'hôte et des machines virtuelles pour limiter les connexions non autorisées.

Sécurisation de l'Accès à l'Hôte KVM

L'accès à l'hôte KVM lui-même doit être soigneusement protégé :

1. Assurez-vous que l'accès SSH est configuré de manière sécurisée sur l'hôte KVM.
   - Désactivez l'authentification par mot de passe dans '/etc/ssh/sshd_config'.
   - Utilisez des clés SSH pour l'authentification et restreignez l'accès aux utilisateurs nécessaires.

2. Configurez SELinux ou AppArmor pour ajouter des contrôles d'accès obligatoires sur les processus KVM.
3. Désactivez les services inutiles et mettez à jour régulièrement tous les logiciels pour corriger les vulnérabilités.

Audit et Surveillance

Il est important de suivre les activités sur votre hôte KVM et dans vos machines virtuelles :

1. Installez et configurez des outils de surveillance tels que 'auditd' pour suivre les actions des utilisateurs.
2. Configurez des journaux d'événements système et réseaux pour détecter des comportements anormaux.
3. Utilisez des outils comme 'fail2ban' pour prévenir les attaques par force brute sur SSH.

Conclusion

Ce laboratoire vous a guidé à travers les étapes essentielles pour sécuriser un environnement KVM sur Ubuntu. Il est essentiel de toujours suivre les meilleures pratiques en matière de sécurité afin de protéger vos ressources et de prévenir les attaques potentielles. La gestion de la sécurité dans un environnement virtuel est un travail continu, et les étapes présentées ici ne sont qu'un début pour garantir la sécurité à long terme de votre infrastructure.