Durcissement du systeme Linux

Assigné

FR

LM **Laurent MATHIEU**
créé : 25/…

Durcissement du systeme Linux

Référentiels

Administr Cloud

Ressource(s)

ANSSI - REC OMMANDA…

Contexte du projet

En tant que administrateur système DevOps, en tant qu'Administrateur Cloud, vous êtes responsable de plusieurs infrastructures. On vous demande de mettre en conformité les machines virtuelles en vue d'un futur audit. Dans une démarche qualité/traçabilité on vous demande d'industrialiser le processus qui

appliquera les recommandations de sécurité de l’ANSSI sur l’ensemble des machines Linux.

Modalités pédagogiques

Important : vous allez travailler sur une plateforme RedHat 8.8 pour ce brief

++**Partie 1 : durcissement système**++

A l’aide du document suivant https://www.ssi.gouv.fr/uploads/2019/02/fr_np_linux_configuration-v2.0.pdf traduire les recommendations de securite dans un role ansible que vous nommerez ANSSI-RECOM. (Dans un premier temps ne faites que les niveaux de durcissement Minimum et Intermédiaires, ne faites pas les protections BIOS/UEFI ou matériel, ce n’est pas nécessaire sur des VM).
Afin de s’y retrouver facilement, faites un fichier de task par recommendation.
Vous devrez importer ces fichiers de tasks dans le fichier main.yml
Envoyer votre role Ansible sur Github
Créer un nouveau dossier dans lequel vous allez créer le fichier playbook.yml, requirements.txt et votre fichier d’inventaire
Dans le fichier requirements.txt faites reference au repo github de votre role Ansible puis installer votre rôle avec la ligne de commande ansible-galaxy

A l’aide des briefs précédents et dans le même dossier que votre fichier playbook.yml, déployer un resource group sur azure avec le vnet et ses subnets avec terraform.
Ajoutez la création d’une azurerm_virtual_machine, idéalement utilisez une clé ssh que vous avez généré ca sera plus simple pour les autres opérations.
Dans votre resource azurerm_virtual_machine ajouter un block provisionner local-exec qui exécutera les commandes Ansible galaxy pour installer les dépendances, puis ansible playbook pour appliquer les différentes tasks. Attention veillez à bien configurer votre playbook.
Au terraform Apply, l’infrastructure doit se deployer tel que décrite et votre role Ansible doit être appliqué

++**Partie 2 : auditer le durcicement**++

Vous allez a present scanner vos machines Linux pour verifier que les differentes mesures de durcissement soient bien en place
Utilisez l’outil SCAP avec le profil ANSSI pour cela
Verifiez que votre durcissement est bien en place, corrigez les eventuels ecarts, et relancez un nouveau scan pour confirmer

++**Partie 3 : bonus**++

(BONUS 1): Utiliser un inventaire dynamique en utilisant la collection azure pour Ansible. Ainsi vous pourrez appliquer les mise a jour sur l’ensemble des machines virtuelles

(BONUS 2): Déployer une Azure Image Gallery et utiliser Packer avec Ansible pour déployer une image custom qui intègre toute les recommandations ANSSI de base
(BONUS 3): Uniquement si le bonus précédent est fait. Ecrire les pipelines Github pour deployer votre image custom s'il y a eu des modifications sur le repo de votre rôle Ansible (Indice: Webhooks)

Modalités d'évaluation

Travail individuel.

Livrables

1/ Repo Github contenant le role Ansible
2/ Repo Github contenant vos fichier terraform et ansible
3/ Rapport SCAP avec le profil ANSSI donnant le resultat de l'audit de vos machines Linux

Critères de performance

Achèvement des objectifs.