/push_check_result - ws-arbiter

Sommaire

Contexte

Le check Security SSH lire les fichiers de configuration de votre serveur SSH et vous les afficher dans un tableau.

- Ce qui vous permet de consulter accès simplement la configuration de votre serveur SSH, sans devoir vous connecter dessus (*dans ce cas le check sera toujours en* ***OK***).
- En plus, si vous le souhaitez, vous pouvez détecter si la configuration correspond à vos standards de sécurité en fournissant les valeurs des paramètres comme référence.
    - Par exemple, le standard sur le nombre maximum de clients connectés simultanément au serveur pourra être de 2, et le check sera en CRITIQUE, si un de vos serveurs est paramétré à 4.

Paramétrage

Le check utilise la ligne de commande suivante :

```
$USERPLUGINSDIR$/linux_by_ssh/check_ssh_security_rust -H "$HOSTADDRESS$" -u "$_HOSTSSH_USER$" -p "$_HOSTSSH_PORT$" -i "$_HOSTSSH_KEY$" -P "$_HOSTSSH_KEY_PASSPHRASE$" -w "$_HOSTSSH_SECURITY_WARN$" -v "$_HOSTSSH_PROTOCOL$","$_HOSTSSH_ROOT_LOGIN$","$_HOSTSSH_EMPTY_PASS$","$_HOSTSSH_PASS_AUTH$","$_HOSTSSH_USER_ENV$","$_HOSTSSH_MAX_AUTH$","$_HOSTSSH_ALIVE_INTERVAL$","$_HOSTSSH_ALIVE_MAX$"
```

Données utilisées provenant du modèle

Donnée	Nom dans la configuration sshd	Description	Valeur par défaut
SSH_ALIVE_MAX	clientalivecountmax	Nombre maximum de clients connectés simultanément au serveur	2
SSH_ALIVE_INTERVAL	clientaliveinterval	Secondes avant que le client soit déconnecté pour inactivité	60
SSH_MAX_AUTH	maxauthtries	Maximum de tentatives de connexion autorisées	2
SSH_PASS_AUTH	passwordauthentication	Autorisation ou non d'accès au serveur par mot de passe	no
SSH_EMPTY_PASS	permitemptypasswords	Autorisation ou non d'accéder au serveur par des comptes sans mot de passe	no
SSH_ROOT_LOGIN	permitrootlogin	Autorisation ou non d'accéder au serveur par le compte root	no
SSH_USER_ENV	permituserenvironment	Autorisation ou non au client connecté de modifier l'environnement	no
SSH_PROTOCOL	protocol	Version du protocole SSH utilisée	2
SSH_WARN		Active/désactive les alertes dues au check	False

Remarque

Dans l'optique de proposer une sécurité stricte nos valeurs par défaut ont été choisies pour une installation basique d'un serveur linux, nous vous conseillons fortement de les modifier pour les adapter à la sécurité que vous souhaitez fixer sur votre/vos serveur(s).

Comme expliqué précédemment, ces données sont utilisées uniquement si la donnée SSH_SECURITY_WARN est à **True**.

Données utilisées provenant du check

Pas de données spécifiques pour ce check

Résultat

Dans ce premier résultat le paramètre SSH_WARN est défini à False, le check passe donc en OK, car il a réussi à trouver le fichier de configuration :

? Unknown Attachment

Dans ce résultat, nous avons passé SSH_SECURITY_WARN à True et le check change d'état pour nous avertir que notre configuration n'est pas idéale pour la sécurité de la machine :

? Unknown Attachment

Interprétation des données

- Statut :
  Le statut peut prendre 3 valeurs différentes (***OK*** / ***CRITICAL*** / ***UNKNOWN***).

- Résultat :
  Le résultat contient un message donnant des informations sur le statut du check ainsi qu'une liste des paramètres à modifier si le statut passe en **CRITIQUE**.

- Résultat Long :
  Le résultat long contient un tableau listant les paramètres sensibles de votre configuration SSH. Si le statut passe en **CRITIQUE**, une troisième colonne apparaît pour lister les valeurs recommandées.

Métriques

Aucune métrique n'est renvoyée pour ce check