Infra Chapril - Demande #5515

ssh ForwardAgent

31/07/2021 18:05 - Christian P. Momon

Statut:	En cours de traitement	**Début:**	31/07/2021
Priorité:	Élevée	**Echéance:**	
Assigné à:	Romain H.	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Backlog		

Description

Le 30/07/2021 sur #april-chapril :

```
20:05 < Pilou> À propos de https://admin.chapril.org/doku.php?id=admin:procedures:ajouter-animateur-service#acces_ssh,
est-il recommandé d'utiliser une clef SSH dédiée pour le Chapril étant donné l'utilisation de ForwardAgent ?
20:08 < PoluX__> ha oui perso je fais pas de forward
[…]
22:02 < PoluX__> cpm_screen: si tu fw ton agent, un root sur la machine concernée peut avoir accès à ta clé iirc
22:03 < PoluX__>      ForwardAgent
                              Agent forwarding should be enabled with caution.  Users with the ability to bypass file permissions
                              on the remote host (for the agent's Unix-domain socket) can access the local agent through
22:03 < PoluX__>              the forwarded connection.  An attacker cannot obtain key material from the agent, however they can
                              perform operations on the keys that enable them to authenticate using the identities loaded into the agent.
22:04 < PoluX__> man ssh_config
22:05 < PoluX__> donc c'est la dernière partie qui est intéressante :)
```

Pour rappel, la configuration actuellement suggérée :

```
Host *.cluster.chapril.org
  User root
  ProxyCommand ssh -W %h:22 april@fip.chapril.org -A
  ForwardAgent yes
  SendEnv GIT_AUTHOR_NAME GIT_AUTHOR_EMAIL
```

Actuellement, le « ForwardAgent Yes » est utilisé pour pouvoir pusher sur les dépôts de la forge April.

Techniquement, puisque root alors il est certainement possible de pirater le ForwardAgent d'un autre.
Dans le cas nominal, il n'y a aucun problème car confiance de l'équipe et actions locales au SI Chapril.

Par contre, dans le cas d'une **compromission de compte animsys, ça donne potentiellement accès à des machines externes au SI Chapril des autres animsys.**

Demande : évaluer la problématique et envisager une solution.

Solutions envisageables :
1) dans la doc admin, mettre un message d'avertissement sur le « ForwardAgent Yes » ;
2) retirer « ForwardAgent Yes » de la doc (implique de faire un git pull chez soi avant de pusher sur la forge April) ;
3) conserver le « ForwardAgent Yes » et rajouter une injonction à utiliser une clé spécifique au Chapril, et donc ajouter dans la documentation comment indiquer la clé spécifique.

Historique

#1 - 01/08/2021 11:24 - Pierre-Louis Bonicoli

Exemple de documentation

La doc de GitHub contient un avertissement relatif à l'utilisation de ForwardAgent, la première solution pourrait s'en inspirer.

Exploitation

Un exemple d'exploitation (en français):

```
SSH_AUTH_SOCK=/tmp/ssh-haqzR16816/agent.16816 ssh bob@host
```

Autres solutions

L'utilisation de l'option SSH AddKeysToAgent=confirm pourrait être ajoutée aux solutions envisageables, à l'usage elle pourrait être considérée comme pas pratique (popups trop fréquentes).

D'autres alternatives sont mentionnées dans la dernière note de cet article.

Ce post cité précédemment mentionne la 3ème solution (une clef dédiée) et l'utilisation de plusieurs agents.

Conséquences

> Par contre, dans le cas d'une compromission de compte animsys, ça donne potentiellement accès à des machines externes au SI Chapril des autres animsys.

Les documentations Chapril concernant la configuration du client SSH pour les animsys et pour les adminsys mentionnent toutes les deux l'utilisation de ForwardAgent et tous les animys ne gèrent pas les même services, je propose:

```
Par contre, dans le cas d'une compromission de compte, ça donne potentiellement:
    * accès aux machines auxquelles un adminsys a accès, dans le cas d'une compromission d'un compte animsys (
si un adminsys est connecté simultanément)
    * accès aux machines auxquelles un animsys a accès, dans le cas d'une compromission d'un compte animsys (s
i un adminsys de plusieurs services est connecté simultanément)
    * et accès à des machines externes au SI Chapril.
```

Modèle de menace

Loic suggère d'établir un modèle de menace avant de changer les recommandations relatives à la configuration SSH:

```
<dachary> Pilou: c'est possible de renforcer cet aspect particulier du système d'information de Chapril. Et ça
 vaut le coup de faire un ticket sur ce point. Dans la mesure ou ça impose a tous de changer ses habitudes, la
 question se pose de savoir quelle priorité donner à ce ticket. Je n'imagine pas qu'il existe un modèle de men
ace pour Chapril: ce serait une première étape. Très utile d'ailleurs et c'est un projet en soi. A défaut de m
odèle de menace, il est vraiment difficile de savoir si ce problème mérite d'être corrigé.

<pilou> pour le modèle de menace, il y a une méthode recommandée ?
<dachary> Pilou: c'est une question compliquée. Il faut se faire accompagner de quelqu'un qui a de l'expérienc
e sinon ça devient vite n'importe quoi (top ou pas assez de détails). Mon conseil serait de commencer par cher
cher une personne avec qui le faire.
```

#2 - 04/12/2021 20:53 - Romain H.

- Statut changé de Nouveau à En cours de traitement

- Assigné à mis à Romain H.

J'ai remplacé la commande *ProxyCommand* par *ProxyJump* dans la documentation.

Avez-vous des exemples d'utilisation légitime du *ForwardAgent* dans l'infra actuelle ? Je pense qu'on pourrait simplement l'interdire au niveau de la configuration du serveur.

Pour les personnes qui veulent cloner un dépôt de la forge sur les serveurs, je pense qu'on peut simplement utiliser le système de clés de déploiement intégré dans Gitea.