Effacement de traces

Introduction

On accorde beaucoup d'attention lors des attaques aux modes d'intrusions l'identification des victimes ou même le craquage des mots de passe de ceux derniers mais l'étape de suppression de traces reste aussi importante qu'eux car une attaque n'est considérée réussite qu'après l'effacement de tout empreinte pouvant mettre en péril l'intrusion et démasquer par la suite son auteur

Présentation de l'atelier

Afin d'effacer les traces le pentesteur doit essentiellement penser à masquer son identité ainsi qu'à nettoyer les logs sans oublier la manipulation des programmes de sécurité

1- Masquer l'identité :

Pour masquer son identité le pentesteur recourt en premier lieu au cryptage de ses propres données et ce à l'aide des crypteurs de fichiers, crypteurs de disques durs ou crypteurs de sessions telnet ….

Tout comme il peut utiliser un serveur d'attaque intermédiaire qui est situé en général à l'étranger sachant que ce serveur n'est pas le même lors de deux attaques successives.

2- Nettoyer les fichiers log

Manipuler les logs sous format texte :

Ce sont les fichiers d'historique de lancement du Shell Unix qui sont selon la version d'unix : *.sh_history* ou *.bash_history* ou tout simplement *.history*

Il y aussi les fichiers de sauvegarde (backup) Unix *dead.letter, *.bak, *~*

Ces fichiers peuvent être manipulés en utilisant la commande grep –wc, ou ls- altr qui liste tous les éléments modifiés.

On peut aussi utiliser des scripts comme le suivant pour vider le .logout :

```
mv .logout save.1
   echo rm .history>.logout
   echo rm .logout>>.logout
   echo mv save.1 .logout>>.logout
```

En effet le contenu du .logout va être recopié au début de l'attaque dans un fichier save.1 puis on y écrit les commandes qui suppriment .history, puis .logout et on récupère l'ancien contenu de .logout et finalement on le ré-exécute.

Manipuler les logs sous format données

Les 3 fichiers les plus importants sont :

- **WTMP** : chaque connexion/déconnexion avec l'heure, le serveur et le terminal concerné
  UTMP : la liste de tous les utilisateurs connectés à un moment donné
  LASTLOG : origine des connexions

Ces fichiers ne doivent pas être supprimés car sinon l'administrateur de la machine cible saura immédiatement qu'il y a eu une intrusion.

Par contre il est possible d'utiliser des outils ou des programmes de modification de ces fichiers logs.

- ZAP (ou ZAP2) : remplacement de la dernière donnée de connexion par des zéros.
- CLOAK2 : modification des données.
- CLEAR : effacement des données.

3- Manipuler les programmes de sécurité :

Sur les serveurs sécurisés, les programmes de sécurité sont lancés à des intervalles périodiques par cron. Donc pour connaitre les programmes de sécurité actifs il suffit donc d'accéder aux paramètres cron et de savoir ce qu'ils enregistrent et pour mettre à jour les fichiers de données du programme et le modifier.

On va par exemple tester deux IDS à savoir A.I.D.E et Tripwire :

AIDE

L'AIDE (Advanced Intrusion Detection Environment) est un contrôleur d'intégrité de dossier.il construit une base de signature des fichiers qu'on désire surveiller avec des dossiers spécifiques dans AIDE.conf. Il est très utile dans la découverte et la détection des changements au niveau des journaux, les fichiers surtout les fichiers de configurations.

Sa configuration est comme suit:

Pour initialiser la base de signature on utilise la commande: **/usr/sbin/aide --init**

Suite à cette initialisation un fichier sera créé, c'est un fichier accessible en lecture afin de vérifier la prise en compte des fichiers qu'on veut surveiller.

Avec la commande **# /usr/sbin/aide --check**

On vérifie l'intégrité des fichiers si elle détecte une anomalie dans les fichiers elle permet soit de recréer la base entièrement ou bien de modifier la base en incluant les changements trouvés et cela avec la commande **#aide --update**

Et on obtiendra à la fin un fichier contenant une nouvelle base de signature qui va remplacer l'ancien.

Malgré qu'AIDE soit très utile dans la détection des intrusions, il est possible de supprimer des traces de cet IDE puisqu'il suffit que le pentesteur sache l'emplacement exact des rapports et ensuite il effectuera les mises à jour et ainsi il n'y aura pas de trace de son intrusion.

Tripwire :

Tripwire est un autre IDS qui a les mêmes principes qu'AIDE sauf que la base de données qu'il crée est protégée par un mot de passe.

Etapes de configuration :

Pour l'initialiser on utilise la commande suivante : **/usr/sbin/tripwire –init**

Lors d'une vérification d'intégrité, Tripwire compare les objets actuels du système de fichiers avec leurs propriétés à l'aide de la commande suivante : **/usr/sbin/tripwire –check**

Une commande **twprint** pour imprimer des rapports Tripwire ressemble à ce qui suit:

/usr/sbin/twprint -m r –twrfile /var/lib/tripwire/report/<*nomdufichier*>.twr

Pour mettre à jour votre base de données Tripwire, afin qu'elle accepte les violations trouvées dans un rapport, on doit spécifier quel rapport on désire utiliser pour la mise à jour de la base de données :

/usr/sbin/tripwire --update –twrfile /var/lib/tripwire/report/<*nomdufichier*>.twr

Mais la protection de tripwire n'est pas infaillible puisque le mot de passe peut être trouvé avec le phishing ou le social engineering.