http://clx.asso.fr/spip/?Creer-des-cocons-a-l-epreuve-des

Créer des cocons à l'épreuve des root-kits

- Documentations - Technique -

Date de mise en ligne : lundi 4 novembre 2002

L'article initial de Jonathan A. Zdiarski est disponible sur cette page :
http://www.networkdweebs.com/saferoom.html.

Apportez toutes suggestions d'ajouts et/ou corrections à Jonathan A. Zdziarski.

Nous venons de voir comment chrooter un service. En cas d'attaque, il est toujours bon de détecter une attaque. Pour cela, une technique consiste à se préparer un petit cocon (ou *saferoom*) bien à l'abri.

Table des matières

Partie I : Introduction aux *Saferooms*

Si vous souhaitez permettre à quelqu'un de pénétrer votre système pour le détruire, mâchez-lui le travail.

1.1 Qu'est ce qu'un root-kit ?

Un root-kit est un outil utilisé par des intrus pour manipuler votre machine tout en rendant la détection de l'effraction du système beaucoup plus difficile. Les root-kits incluent généralement des programmes créant des portes d'entrée (*back-doors*). Elles permettent à de nouveaux intrus de pénétrer le système. La plupart des sites internet consacrés aux attaques fournissent des root-kits en téléchargement libre.
Une fois qu'un intrus a réussi à pénétrer dans un système, il compile et installe son root-kit, tout simplement. Le root-kit contient généralement plusieurs programmes semblables aux outils système tels que `find, netstat, ps`, etc. Les versions modifiées de ces outils cachent volontairement l'activité de l'intrus, ainsi ses activités ne sont pas

détectés tout de suite par l'administrateur système. Le plus dangereux, c'est que l'administrateur système n'a souvent aucune raison de suspecter l'effraction du système, et ne tente pas d'examiner attentivement ce dernier.

1.2 Comment puis-je me protéger ?

Il existe plusieurs logiciels pour détecter des root-kits. Une recherche sur Internet vous en suggérera quelques-uns. Une autre manière de se protéger contre un root-kit est de garder une trace des résumés (*checksum*) de tous les binaires du système. Pour cela, utilisez des outils comme **tripwire** ou **md5sum**. Les deux paquetages sont à disposition du grand public, et créent des "empreintes digitales" de chaque fichier, permettant à un administrateur système de détecter tout changement des empreintes initiales. Ils sont très utiles pour détecter si le système est compromis et notamment plus tard, lors de la récupération de celui-ci, sans devoir tout réinstaller. Le sujet de cet article, cependant, est de détailler une méthode non conventionnelle de protection appelée un cocon.

Qu'est ce qu'un cocon (*saferoom*) ?

Si vous avez déjà fait installer un système de sécurité à votre domicile, vous avez remarqué que le technicien (s'il n'est pas mauvais) a mis en place un ensemble de verrous et a renforcé un point d'entrée (à un endroit bien particulier). En cas de problème, toute la famille se rend dans cette pièce pour empêcher l'accès au cambrioleur.

Un cocon, en termes de sécurité, est un 'emplacement' impénétrable sur votre système contenant les outils critiques nécessaires pour vos administrateurs systèmes avec toutes les fonctions indispensables. Les cocons sont généralement prioritaires sur le chemin conventionnel déclaré dans le `.login` ou le `.profile` de l'administrateur système. On y trouve les outils de maintenance quotidienne. Un cocon, utilisé efficacement, fournit un ensemble d'outils pour détecter des
compromissions, essentiellement grâce des fonctions de traçage.

Un cocon est-il inviolable ?

Cela dépend du type de cocon que vous créez. Si vous réussissez à mettre en place un cocon en lecture seule stricte, même pour root, vous devez continuer à vous méfier de certains intrus capables de modifier votre chemin (*path*) et qui par la suite pourront démonter complètement le cocon. Bonne nouvelle, les intrus ne les "cherchent" pas systématiquement. Quand un intrus pénètre par effraction dans votre système, ils réalisent qu'ils n'ont que très peu de temps pour sécuriser leur propre accès et donc encore moins pour y installer leur root-kit. Pour qu'un intrus puisse neutraliser un cocon, il doit déjà en connaître son existence. Par ailleurs, en le démontant, il risque d'être détecté, un peu comme s'il se jetait dans la gueule du loup.

Ce qu'il faut savoir pour créer un cocon.

Il existe deux types de 'saferooms : les cocons physiques, ou logiques. Le cocon idéal est situé sur un disque séparé,
physiquement protégé en écriture grace à un cavalier matériel. Face à des contraintes de coût, certains choisissent cependant de simplement créer un répertoire caché sur une partition accessible en écriture (il s'agit d'un cocon logique). Ceci rend très facile la neutralisation du cocon, mais est encore efficace car psychologiquement l'intrus moyen ne va pas rechercher un répertoire caché. Cela a quelques avantages, car le *saferoom* n'apparaîtra pas dans l'affichage de points de montages du système. L'intrus devra rechercher des binaires systèmes dans le système tout entier, ou trouver les comptes d'administrateurs, en examiner leur .profile ou leur .login afin de repérer une éventuelle *saferoom* dans un répertoire caché. En supposant qu'il la trouve malgré tout, il doit toujours se méfier de ne pas signaler sa présence (et donc révéler l'intrusion). Si je me suis "logué" avec mon compte et qu'un cocon est

déclaré dans mon chemin de base et que quelqu'un le supprime, j'obtiendrai soudainement des erreurs de "fichier non trouvé". De même, il y a bien d'autres choses à prendre en compte. Un bon administrateur pourrait écrire une tâche automatique qui vérifierait l'état du cocon et enverrait un courriel en cas de changement ou de disparition. Toutes ces différentes protections non standardisées du système prennent un
intrus par surprise, et augmentent de manière significative le risque de détection.

Si vous voulez vraiment assurer la sécurité de vos systèmes, nous recommendons l'utilisation des deux cocons (un de chaque type). Si un intrus recherche un cocon et en neutralise un, il y a une chance très mince qu'il en recherche un second. Et, si toutefois il prenait le temps de la trouver tout de même, il augmenterait énormément les risques de détection.

Les étapes de base pour créer un cocon sont :
– Préparer un disque (ou un répertoire) à agir en tant que tel,
– Y ajouter les binaires critiques,
– Ajouter les cocons dans les chemins de base des administrateurs (ou celui par défaut),
– Verrouiller le cocon.

Partie II : Créer un cocon

Configuration du disque du cocon

Si vous créez un cocon physique, vous devrez trouver un disque avec un cavalier pour permettre la position en lecture seule. Ils sont
assez fréquents. Comme la taille du cocon sera particulièrement petite (à moins que vous souhaitiez quelque chose de mieux), plus le disque est petit, mieux c'est. Une fois le disque installé et branché en lecture et écriture, choisissez un point de montage (pas trop évident) et installez-y les
fichiers souhaités. Si vous créez un cocon logique, trouvez un endroit pour y créer le répertoire. Beaucoup de gens choisissent quelque chose du genre `/usr/local/lib/perl5` ou `/usr/include/sys`. Quelque soit l'endroit, essayez de ne pas choisir un nom de fichier trop évident ("saferoom" est par exemple un mauvais choix).

Remplir le cocon

Une fois que vous avez créé votre cocon initial, vous voudrez y créer un répertoire `bin` et y copier les fichiers critiques. On pourrait y mettre :

```
crontab du find finger kill killall ls netstat passwd ps top
```

Tout autre outil fréquemment utilisé par les administrateurs peut y prendre place. Une fois que vous les avez copiés, la prochaine chose que vous devrez faire est d'y copier les bibliothèques dynamiques afin d'utiliser ces fichiers critiques. Si un intrus parvenait à déposer ses propres bibliothèques, vous pourrez utiliser les originales. Créez un répertoire `/lib` dans votre cocon, puis faites un 'ldd' sur tous les binaires que vous y avez copiés. Par exemple :

```
ldd /moncocon/bin/* | awk '{print $3}'|sort|uniq
```

Le résultat devrait être utile. Copiez toutes les librairies énumérées dans le répertoire lib.

Installation du chemin

Une fois que vous avez créé votre cocon, vous voudrez rendre ces outils et bibliothèques disponibles par défaut pour les administrateurs système. En quoi le cocon est intéressant si vous continuez à utiliser les outils originaux et que l'intrus pénètre malgré tout dans le système ? Vous ne le détecterez jamais si vous n'utilisez pas les programmes du cocon. Certains administrateurs préfèrent utiliser les nouvelles bibliothèques mais pas les nouveaux outils. L'intrus a encore plus de mal à découvrir l'existence du cocon puisqu'aucune mention n'en est faite dans le .login ou le .profile. Cela force cependant les administrateurs à taper le chemin complet de la bibliothèque lorsqu'ils lancent le programme. Quelle que soit la méthode, `/usr/lib` devra passer après le nouveau répertoire lib. Sur quelques systèmes d'exploitation, on peut modifier le fichier `ld.so.conf` pour inclure le chemin des nouvelles bibliothèques, d'autres préfèrent positionner manuellement les variables d'environnement correctes. La variable `LD_LIBRARY_PATH` est généralement employée à cette fin, bien que quelques administrateurs systèmes aient choisi de modifier le chemin complet. Consultez la documentation pour trouver la solution la plus élégante.

Verrouiller votre cocon

Une fois que vous avez créé et analysé votre cocon, vous êtes prêt à le verrouiller. Si vous avez un disque physique, placez le cavalier sur la position lecture seule. Personne ne sera plus en mesure d'écrire dessus.

Surveiller votre cocon

Les cocons pouvant être détruits, en surveiller l'activité est une bonne idée, par exemple par des contrôles périodiques en regardant les points de montage, ou en examinant le répertoire. Cela est déjà un bon début. La meilleure manière de surveiller votre cocon, cependant, est d'écrire un script pour toutes ces tâches. Les différentes actions à prévoir :

– produire des sommes md5 sur les socons accessibles en lecture et écriture,
– vérifier les points de montages inaltérables, tout cela de façon scriptés le tout accompagné
– d'un envoi d'avertissement en cas d'intrusion et de démontage de votre cocon.

Mais comme nous l'avons dit, tous les intrus ne recherchent pas systématiquement les cocons.

Post-scriptum :

La version originale de cet article est consultable en ligne : http://www.networkdweebs.com/saferoom.html.