aDvens

Security for the greater good

Intrusion sous Unix/Linux

Méthodologie de réponse à incident

IRM-03 | 2022-11-30 | **TLP-CLEAR** | CERT aDvens - CSIRT
Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

Introduction

Cette méthodologie de réponse à incident est une feuille de route dédiée aux gestionnaires et aux cellules de crise menant une investigation sur un problème de sécurité précis.

→ La fiche IRM s'adresse aux personnes ou fonctions suivantes :
- Les **RSSI et leurs adjoints**
- Le **CERT**
- Le **SOC**
- Les **administrateurs**

Dans le cas d'un incident : Lire l'IRM et prendre des notes.
Rester calme et contacter immédiatement l'équipe de réponse à incident du secteur d'activité ou un CERT si nécessaire.

Étapes de traitement des incidents

6 étapes sont définies pour gérer les incidents de sécurité :

1. **Préparation** : Se préparer à gérer l'incident,
2. **Identification** : Détecter l'incident,
3. **Confinement** : Limiter l'impact de l'incident,
4. **Remédiation** : Supprimer la menace,
5. **Récupération** : Revenir à un état normal,
6. **Capitalisation et apprentissage** : Élaborer et améliorer les processus.

Cette IRM fournit des informations détaillées pour chaque étape. Les étapes sont issues du NIST.

Cette fiche est issue du travail collaboratif avec le **CERT-SG** de modification et de mise à jour de leurs fiches de méthodologie de réponse à incident.

Références

→ IRM CERT-SG
→ IRM CERT-aDvens

1. Préparation

Objectif : Établir la liste de contact des personnes concernées et impliquées dans la résolution de l'incident, définir les procédures, recueillir les informations pertinentes pour ne pas perdre de temps durant la réponse à incident.

- Déployer une solution logicielle de type EDR, de détection et de réponse sur les terminaux, les postes de travail et les serveurs :
  - Cet outil est devenu l'une des pierres angulaires en réponse à incident dans la gestion d'un incident de type rançongiciel ou sur un système d'information compromis sur un large périmètre, facilitant les étapes d'identification, de confinement et de remédiation,
  - Lancer des recherches à l'aide de l'EDR et des analyses antivirales, en spécifiant des indicateurs de compromission ciblés (IOC), et suivre la progression de la compromission et de sa remédiation,
  - Configurer les stratégies de l'EDR sur le mode Prévention.

En l'absence de solution logicielle EDR, un accès physique au système suspect doit être accordé à l'analyste forensique.
Un accès physique est préférable à un accès à distance, l'attaquant pouvant détecter les investigations effectuées à distance sur le système (à l'aide d'un logiciel d'analyse réseau par exemple).

- Un **accès physique sur le système suspect** doit être procuré à l'enquêteur forensique.
- Une **copie physique (binaire) du disque de données ou support de stockage** peut être nécessaire pour les investigations forensiques et à titre de preuve. Une intervention en local sur le système suspect doit être envisagée pour le déconnecter de tous les réseaux.
- Il est nécessaire de **disposer d'une base de connaissance sur l'activité réseau usuelle et normale du système compromis**. Le fichier stocké dans un endroit sûr doit décrire l'activité habituelle des ports réseau afin d'être comparer à l'état actuel lors de l'incident.
- Il est nécessaire de **disposer d'une base de connaissance sur les services habituellement utilisés** sur les systèmes. Demander au besoin l'aide d'un expert en Unix/Linux :
  - Utiliser les journaux d'événements d'Auditd et du système Linux comme les journaux "system", "message" et les journaux d'événements des applications (Apache, NGINX,…)
  - Utiliser le logiciel "AppArmor" par exemple
- Il est nécessaire de disposer d'une **liste régulièrement mise à à jour de tous les fichiers critiques** (notamment les fichiers avec les permissions SUID et/ou GUID positionnées), la liste devra être stockée dans un endroit sûr déconnecté du réseau ou même imprimée sur du papier. A l'aide de cette liste, il est possible d'écarter les fichiers SUID usuels et de détecter les fichiers inhabituels.
- Il est nécessaire de disposer d'une **matrice de l'activité normale du réseau et des ports utilisés** par les services et applications sur le système d'information.

2. Identification

Objectif : Détecter l'incident, déterminer son ampleur et impliquer les acteurs appropriés.

2.1. Activités Système

→ Comptes inhabituels
- Rechercher toute entrée suspecte dans le fichier "/etc/passwd", en particulier avec l'UID 0. Vérifier également les fichiers "/etc/group" et "/etc/shadow".
- Rechercher les fichiers orphelins ayant pu être oubliés par un compte supprimé utilisé dans l'attaque :

```
# find / \( --nouser -o --nogroup \) --print
```

→ Fichiers non conventionnels
- Rechercher tous les fichiers SUID et GUID :

```
# find / -uid 0 \( --perm -4000 -o --perm 2000 \) --print
```

- Rechercher des noms de fichiers étranges, commençant par ". " ou ".. " ou " " :

```
# find / --name ". *" --print
```

```
# find / --name ".. *" --print
```

```
# find / --name " *" --print
```

- Rechercher les fichiers de grand taille (ici : De plus de 10 Mo) :

```
# find / -size +10MB --print
```

- Rechercher les processus exécutés depuis ou vers des fichiers qui ont été dissociés :

```
# lsof +L1
```

- Rechercher les fichiers inhabituels dans les dossiers "/proc" et "/tmp". Ce dernier répertoire est un lieu de prédilection pour les pirates pour stocker des données ou des binaires malveillants.

→ Services inconnus
- Exécuter la commande chkconfig (si installé) pour vérifier tous les services présents sur le système :

```
# chkconfig --list
```

- Vérifier la légitimité des processus en cours d'exécution (il est rappelé qu'un rootkit peut modifier les résultats obtenus, notamment pour toutes les commandes mentionnées dans ce document !) :

```
# ps -aux
```

- Utiliser la commande `lsof -p [pid]` sur les processus inconnus.

Il est nécessaire de connaître les processus habituellement présents sur un système pour être capable d'identifier les processus ajoutés par un attaquant.
Porter une attention particulière sur les processus exécutés depuis l'UID 0

2.2. Activité réseau inhabituelle

→ Essayer de détecter les logiciels d'analyse réseau de plusieurs manières :
- rechercher dans les fichiers journaux du noyau Linux les interfaces réseau basculées en mode promiscuité, mode utilisée pour écouter tout le trafic réseau comme le message suivant :
  → "kernel: device eth0 entered promiscuous mode"
- Utiliser la commande # ip link pour identifier les interfaces réseau ayant présentant un attribut "PROMISC".

→ Rechercher l'utilisation inhabituelle de ports réseau :

```
# netstat -nap
```

```
# lsof -i
```

→ Rechercher la présence d'entrée d'adresse MAC inhabituelles sur le réseau :

```
# arp -a
```

→ Rechercher la présence d'adresses IP inhabituelles ou nouvelles sur le réseau :

```
# netstat -ntaupe
```

```
# netstat -ant
```

```
# watch ss -tt
```

2.3. Tâches planifiées inhabituelles

→ Rechercher la présence de tâches inhabituelles qui auraient pu être planifiées par les utilisateurs dans le fichier /etc/cron.allow. Porter une attention particulière aux tâches cron planifiées par les comptes ayant l'UID 0 (root) :

```
# crontab -u root -l
```

→ Rechercher les tâches cron inhabituelles à l'échelle du système :

```
# cat /etc/crontab
```

```
# ls -la /etc/cron.*
```

2.4. Événements inhabituelles dans les journaux

→ Rechercher dans les fichiers journaux du système la présence d'événements suspects, notamment les suivants :
- Nombre important d'échecs d'authentification/de connexion effectuées par des logiciels d'accès en local ou à distance (sshd, ftpd, etc.),
- Programmes d'appel de procédure à distance (RPC) présentant un événement dans un journal comprenant un grand nombre de caractères non conventionnels …,
- Nombre important d'événements dans les journaux Apache mentionnant "erreur",
- Événements de redémarrage (redémarrage matériel),
- Redémarrage d'applications (redémarrage logiciel).

La majorité des fichiers journaux se trouvent sous le répertoire /var/log dans la plupart des distributions Linux.

→ Les principaux journaux sont (les chemins d'accès peuvent varier selon les distributions) :
- /var/log/message : Messages généraux et éléments liés au système
- /var/log/auth.log : Journaux d'authentification
- /var/log/kern.log : Journaux du noyau
- /var/log/cron.log : Journaux du processus Crond (tâches cron)
- /var/log/maillog : Journaux du serveur de messagerie
- /var/log/httpd/ : Répertoire des journaux d'accès et d'erreurs d'Apache
- /var/log/boot.log : Journal de démarrage du système
- /var/log/mysqld.log : Fichier journal du serveur de base de données MySQL
- /var/log/secure : Journal d'authentification
- /var/log/utmp ou /var/log/wtmp : Fichier d'enregistrements de connexion
- /var/log/syslog : Messages cron, activité samba et plus
- /root/.*history : Historique des commandes de l'utilisateur root
- /home/*/.*history : Historique des commandes des utilisateurs

Pour parcourir les fichiers journaux, des outils comme cat et grep peuvent être utiles :

```
cat /var/log/httpd/access.log | grep "GET /signup.jsp"
```

→ Entrées inhabituelles dans le journal du noyau :
- Rechercher la présence d'événements suspects dans les fichiers journaux du noyau du système :

```
# dmesg
```

- Répertorier toutes les informations importantes sur le noyau et le système :

```
# lsmod
```

```
# lspci
```

- Rechercher la présence de rootkit connu (en utilisant des logiciels comme rkhunter et d'autres outils)

2.5. Empreintes numériques de fichiers

→ Vérifier toutes les empreintes numériques MD5 des fichiers binaires présents dans les répertoires /bin, /sbin, /usr/bin, /usr/sbin ou tout autre emplacement connu de fichiers binaires (utiliser AIDE ou équivalent)

Cette opération modifiera probablement tous les horodatages des fichiers. Cela ne devrait être mise en oeuvre qu'à l'issue de toutes les autres investigations sur le système et que cette opération peut altérer les données.

Sur les systèmes ayant RPM installé :

```
# rpm -Va | sort
```

Sur certains systèmes Linux, un script nommé check-packages peut être utilisé.

Sur Solaris :

```
# pkg_chk -vn
```

Sur Debian :

```
# debsums -ac
```

Sur OpenBSD (exemple de commande possible) :

```
# pkg_delete -vnx
```

3. Confinement

Objectif : Atténuer les effets de l'attaque sur l'environnement ciblé.

- → Sauvegarder en toute sécurité les données importantes de la machine compromise, si possible, en effectuant une copie physique bit à bit (binaire) de l'intégralité du disque dur sur un support externe. Faire également une copie de la mémoire volatile (RAM) du système, qui pourra être examinée par la suite si nécessaire,
- → Isoler le système à l'aide de l'EDR et vérifier les autres ordinateurs et les réseaux.

Ou

- → Isoler le système depuis le pare-feu ou les commutateurs réseau.

Si la machine n'est pas considérée comme critique pour l'entreprise et qu'elle peut être déconnectée du réseau, l'éteindre brutalement en retirant sa prise d'alimentation.
S'il s'agit d'un ordinateur portable avec une batterie intégrée, appuyer simplement sur le bouton "off" pendant quelques secondes jusqu'à ce que l'ordinateur s'éteigne.

Des investigations hors ligne doivent être lancées immédiatement si l'étape d'identification n'a donné aucun résultat, mais que le système est toujours suspecté d'être compromis.

- → Tenter de trouver des preuves de chaque action de l'attaquant (en utilisant des outils d'investigation comme The Sleuth Kit/Autopsy par exemple) :
  - Identifier tous les fichiers utilisés par l'attaquant, y compris les fichiers supprimés et élucider leurs utilisations ou au moins leurs fonctionnalités pour évaluer la menace,
  - Vérifier tous les fichiers consultés récemment,
  - Vérifier les fichiers journaux.
  - Plus généralement, essayer de trouver comment l'attaquant a pu accédé au système. Toutes les pistes doivent être prises en compte. Si aucune trace d'intrusion n'est visible, ne jamais oublier que l'attaquant peut être en interne de l'entreprise.
  - Si possible, appliquer les correctifs, pour empêcher le même type d'intrusion, au cas où l'attaquant utiliserait une vulnérabilité corrigée connue.

4. Remédiation

Objectif : Prendre des mesures pour arrêter l'attaque et éviter d'être de nouveau attaquer.

Ne commencer à corriger que lorsque l'intégralité du périmètre délimité est contenu ou isolé afin d'empêcher l'attaquant de prendre des mesures de répression.

Retirer temporairement tous les accès aux comptes incriminés dans l'incident et supprimer tous les fichiers malveillants.

5. Récupération

Objectif : Restaurer le fonctionnement normal du système.

Peu importe jusqu'où l'attaquant a pu accéder sur le système et la connaissance apprises sur l'attaque mise en oeuvre, à partir du moment où un système a été compromis, la meilleure pratique consiste à réinstaller complètement le système et à appliquer toutes les mises à jour de sécurité.

→ Dans le cas où cette solution ne peut pas être appliquée :
- Modifier tous les mots de passe des comptes du système et faire en sorte que les utilisateurs le fassent de manière sécurisée,
- Vérifier l'intégrité de l'ensemble des données présentes sur le système, en utilisant leurs empreintes numériques (par exemple SHA256)
- Restaurer tous les fichiers binaires ayant pu être modifiés (par exemple : /bin/su)
- Remplacer tous les paquets logiciels compromis par des paquets sains.

6. Capitalisation et apprentissage

Objectif : Documenter les détails de l'incident, discuter des leçons apprises et ajuster/améliorer les dispositifs et stratégies de défense.

Le rapport d'incident

Il doit être rédigé et mis à la disposition de toutes les parties prenantes.

Le retour d'expérience

Les thèmes du retour d'expérience doivent être décrits avec les éléments suivants :

→ Cause initiale de l'infection,
→ Actions et chronologies de chaque événement important,
→ Ce qui s'est bien passé,
→ Ce qui ne s'est pas bien passé,
→ Coût de l'incident,
→ Indicateurs de compromission.

La capitalisation

Des actions d'amélioration des processus de détection des logiciels malveillants et des intrusions sur le réseau doivent être définies pour capitaliser sur cette expérience.