Station Blanche

Lien du projet (pour la version PDF) : https://gitlab.com/thibaultfeugere/station-blanche

Objectif

Après quelques mois d'alternance en sécurité informatique, je me rends compte que les failles humaines sont plus difficiles à remédier que les failles techniques. Malgré la mise en place de nombreuses mesures basées sur le principe de Pareto, certaines surfaces d'attaques subsistent telle que l'attaque par média amovible.

J'ai entendu plusieurs fois parler de station blanche (aussi appelé station de désinfection) sans jamais approfondir le sujet.

De ce fait, la mise en place de ma première station blanche pendant le laboratoire de cybersécurité d'Ynov, lors des Ydays, me semblait appropriée.

Feuille de route

1. Définir ce qu'est une station blanche, faire des recherches sur internet, lire le rapport de l'ANSSI
2. Faire des recherches sur des antivirus gratuits et open source si possible
3. Choisir un système d'exploitation
4. Mettre en place du durcissement (hardening)
5. Rédaction de la documentation
6. Prise de recul sur les choses à améliorer

Problèmes rencontrés

Le projet s'étant déroulé sur 5 mois, il y a eu plusieurs petits problèmes qui ont été résolus sans trop de difficultés.

Le plus gros problème auquel j'ai dû faire face était le manque de contenu sur internet. Finalement, il n'y a pas beaucoup de projets similaires sur internet ou, du moins, il n'y a pas beaucoup de projets open source. Les rares stations blanches sont des produits finis et payants comme Kub Cleaner par exemple. J'ai donc seulement regardé les fonctionnalités proposées.

Les zones de flou ont donc été sujettes à mon interprétation.

Définitions

Station blanche : Poste de travail isolé du réseau opérationnel dédié à l'analyse des médias amovibles afin de déterminer si elle peut être utilisée sur ledit réseau.

Constat

Enormément de piratage passent par les médias amovibles. Les attaquants joue sur un maillon faible, l'humain qui a un défaut : la curiosité.

Il est très simple de laisser une clé usb infectée par terre, en plein milieu d'un couloir ou devant les bureaux d'une entreprise que vous ciblez.

La curiosité de l'humain va alors le pousser à brancher la clé usb sur son poste et il n'y a pas énormément de moyen de s'assurer de la légitimité des données avant de l'avoir branchée. Si l'antivirus prévient l'utilisateur, il y a de grandes chance pour qu'il accepte le risque. Tout un réseau peut alors être compromis.

Une solution peut être de mettre en place une station blanche.

Respect du DICT

Logiciels du produit : Les logiciels du produit (système d'exploitation, application, base de signatures virales, etc.) sont considérés comme des biens sensibles. Ils doivent être protégés en disponibilité, intégrité et authenticité.

Journaux d'évènements : Les évènements de sécurité sont journalisés localement et de façon déportée. Ce bien est à protéger en disponibilité et intégrité. Les journaux doivent être également authentifiés lorsqu'ils sont déportés

Journaux de transfert de fichiers : Les informations liées au transfert de fichier(s) sont journalisées localement et de façon déportée. Ce bien est à protéger en disponibilité et intégrité. Les journaux doivent être également authentifiés lorsqu'ils sont déportés.

Données des fichiers à analyser : Le fichier à analyser doit être protégé en intégrité

Résultat d'analyse : Les données issues de l'analyse du fichier par le produit doivent être protégées en confidentialité.

Source : rapport de l'ANSSI.

Menaces à prendre en compte sur une Station Blanche

Les menaces peuvent provenir de différents horizons :

- Utilisateur légitime : insertion d'un média compromis ou réalisation d'une erreur de manipulation.
- Utilisateur non autorisé : accès physique à la station blanche.
- Attaquant avec droits administrateurs : l'attaquant a réussi à compromettre le compte d'un administrateur.

Système d'exploitation de station blanche

OS

Le système d'exploitation choisit est Q4OS qui utilise un base Debian. C'est une distribution relativement stable, légère et qui a fait ses preuves au cours des années. Cela va donc dans le sens de la station blanche qui devra être, potentiellement, réinstallée plusieurs fois.

De plus, le budget sécurité informatique est souvent très faible. Il faut donc que l'OS tourne sur n'importe quel ordinateur.

Le système d'exploitation a été durcît (hardening) grâce aux recommandations de l'ANSSI ainsi que l'outil `lynis`.

La langue de la station blanche est le français afin qu'elle soit compréhensible par tous.

Configuration minimale requise

- RAM: 128 MB
- CPU: 300 MHz
- Espace de stockage : 3 Gb

Chiffrement

Le système d'exploitation est chiffré.

Compte utilisateur

Pour la preuve de concept, l'identifiant et le mot de passe sont simples. Dans une utilisation en entreprise, il est conseillé de changer ce mot de passe et mettre une politique de changement de mots de passe. L'ANSSI recommande de changer tous les 90 jours.

Le mot de passe de l'utilisateur `root` est uniquement connu du gestionnaire de la station blanche et le changement fréquent du mot de passe est aussi conseillé.

Nom d'utilisateur : `statioblanche`

Mot de passe : `statioblanche`

Fonctions de la station blanche

Pour les utilisateurs qui souhaitent utiliser la station blanche, il suffit de brancher la clé USB à scanner et d'exécuter le fichier `scan.sh`.

Celui-ci va lancer l'outil `ClamAV` et `VirusTotal`. Les détails des arguments utilisés avec l'outil `Clamav` par le script `scan.sh` sont disponibles ici.

Mise à jour de la station blanche

Régulièrement, il faut faire des mises à jour du système d'exploitation de la station blanche ainsi que de la base de données de signature de ClamAV. Pour cela il faut la brancher au réseau. L'utilisation d'un pare-feu est donc recommandé.

Pare-feu

Le pare-feu choisit est UFW. Il est simple d'utilisation et efficace. Ce pare-feu est utile lorsque l'administrateur de la machine va la connecter au réseau pour faire des mises à jour du système d'exploitation, de la base de données des signatures, etc.

Sont autorisés : - DNS - HTTP / HTTPS

Le firewall est configuré afin de stocker des logs qui sont stockés dans `/var/log/ufw.log`.

Automatisation de l'installation de la station blanche

Création d'une OVA

Lien vers l'OVA (8Gb) : https://drive.google.com/file/d/1Ge5rGOlfr10B0fTT5qmDuAExrGmnSKzv/view?usp=sharing

Création d'une ISO

Lors de la création et du pentest, il est fréquent que la station blanche devienne compromise. La création d'un image peut alors être intéressant.

Scan régulier de tout l'OS

Grace à une CRON, l'entièreté de l'OS est scannée toutes les semaines. La ligne de commande est stockée dans `/etc/cron.weekly/`.

Le scan de tout l'OS est effectué avec l'outil `ClamAV` : `clamscan -i -r -z / > /root/global-scan-$(date "+%A-%B-%d-%T-%y").txt` et est uniquement accessible pour l'administrateur.

Post création de la station blanche

Il est indispensable de pentester la station blanche.

Maintien de la station blanche à jour

Même si nous nous efforçons à diminuer les surfaces d'attaques de la station blanche à un instant donné, celle-ci verra ses vulnérabilités augmenter avec le temps. De ce fait, il faut la mettre à jour de temps en temps. Pour cela, il y a le script `update.sh`.

Ce script a pour mission de mettre à jour la station blanche, de scanner les paquets qui possèdent des failles de sécurité et d'installer la version corrigée si elle existe. De même, nous mettons à jour la base de signatures de ClamAV et nous exécutons à nouveau `lynis` pour vérifier que l'état de la machine ne se dégrade pas.

`update.sh` est à exécute en tant qu'administrateur et il faudra lui fournir un accès internet exceptionnelement le temps de faire les mises à jour.

Aboutissement du projet

Il est acceptable de dire que le projet est à un stade suffisant pour être deployé en entreprise. Cependant, il est encore nécessaire d'effectuer de l'hardening, même si c'est un chantier en constante évolution.

Les scripts ne sont pas facilement utilisables pour tous les utilisateurs, or l'objectif de la station blanche est quelle soit accessible. Si la solution n'est pas facilement utilisable, alors les utilisateurs ne passeront pas par cette étape pouvant mettre tout ou partie des postes d'un réseau en danger et par conséquent l'entreprise.

Le repertoire Docs contenant la documentation des outils à utiliser devrait être exhaustif. Actuellement, l'administrateur devra utiliser les scripts fournis ou faire ses propres recherches.

Facultatif

Pour les personnes qui ne souhaiteraient pas utiliser l'image ou le fichier ova mais qui voudrait utiliser certains outils ou exécuter le script sur une autre machine, il vous suffit de cloner se repository et d'exécuter en administrateur le script `install-all.sh`. Celui-ci va venir exécuter tous les scripts qui se trouvent dans le répertoire `installs`.

Si un outil ne vous intéresse pas, vous pouvez le supprimer du répertoire.

Pour vérifier le bon fonctionnement de la station blanche, vous trouverez le fichier de test antimalware Eicar. Il est inoffenssif mais permet de lever des alertes.

Voici le résultat de ce fichier sur VirusTotal par exemple :

Ressources

- https://askubuntu.com/questions/4508/how-do-i-safely-use-a-virus-infected-usb-drive-in-ubuntu
- https://askubuntu.com/questions/134874/how-to-auto-scan-any-plugged-in-usb-storage-device-with-clamav
- https://jpwils.ch/git/jpwilsch/station-blanche
- https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-un-systeme-gnulinux/
- https://cisofy.com/lynis/
- https://www.ssi.gouv.fr/guide/profil-de-fonctionnalites-et-de-securite-sas-et-station-blanche-reseaux-non-classifies/

Hardening du système

L'hardening va se baser sur les recommandations de l'ANSSI : https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-un-systeme-gnulinux/

Le fichier : Rapport de l'ANSSI

Outils disponibles pour le gestionnaire de la station blance

Apt-listbugs

`apt-listbugs` est un utilitaire qui se lance automatiquement à l'installation d'un nouveau paquet, et va chercher les rapports de bug (s'ils existent). En cas de bug, il vous prévient et vous demande si vous souhaitez installer, annuler ou figer le paquet en question..

Apt-listchanges

(Pas fonctionnel pour l'instant)

ClamAV

ClamAV est un antivirus avec une base de données. Les commandes de base sont expliquées dans ./clamav.md.

Debsums

Cet outil permet de vérifier la signature MD5 du paquet associé à sa vraie valeur.

Pour l'utiliser : `debsums`.

Résultat :

```
/usr/share/man/man1/b2sum.1.gz                                      OK
/usr/share/man/man1/base32.1.gz                                     OK
/usr/share/man/man1/base64.1.gz                                     OK
/usr/share/man/man1/basename.1.gz                                   OK
...
```

Debsecan

Cet outil permet de lister les CVE associés aux outils que la station blanche possède.

Pour l'utiliser : `debsecan --suite buster --format detail` .

Pour obtenir seulement ceux qui possèdent un fix : `debsecan --suite buster --only-fixed` .

Résultat :

```
CVE-2020-27170 linux-headers-4.19.0-14-amd64 (fixed)
CVE-2020-27171 linux-headers-4.19.0-14-amd64 (fixed)
CVE-2021-26930 linux-headers-4.19.0-14-amd64 (fixed)
...
```

Pour fixer les paquets : `apt install $(debsecan --suite buster --only-fixed --format packages)` .

Debian-goodies

`Debian-goodies` est un ensemble de petits utilitaires avec notamment `checkrestart` qui permet de voir les processus ou programmes qui ont besoin de redémarrer.

```
sudo checkrestart
Found 2 processes using old versions of upgraded files
(2 distinct programs)
(2 distinct packages)
These processes (2) do not seem to have an associated init script to restart them:
pulseaudio:
        2282    /usr/bin/pulseaudio
kmix-trinity:
        2653    /opt/trinity/bin/kmix
```

Needrestart

Cet outil permet de définir si le redemarrage d'un daemon ou de la machine est nécessaire. Il s'exécute automatiquement lorsque c'est nécessaire.

Cependant, nous pouvons forcer son exécution via la commande : `sudo needrestart`.

Résultat :

```
 root@q4os-desktop:~# sudo needrestart
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.
```

Le résultat en version graphique ressemble à ça :

Lynis

Lynis est un outil qui permet d'auditer rapidement son système avec la commande `sudo lynis audit system`.

Avant

Voici le résultat au début :

```
-[ Lynis 3.0.3 Results ]-

  Warnings (3):
  ----------------------------
  ! grpck binary found errors in one or more group files [AUTH-9216]
      https://cisofy.com/lynis/controls/AUTH-9216/

  ! No AIDE database was found, needed for AIDE functionality [FINT-4316]
      https://cisofy.com/lynis/controls/FINT-4316/

  Suggestions (35):
  ----------------------------
  * Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT
      https://cisofy.com/lynis/controls/BOOT-5122/


...
```