"Cap ?"

Jean-Marc Pouchoulon

Mai 2022

Vous travaillerez de préférence dans une VM Debian à la dernière version sur `http://store.iutbeziers.fr`.

1 Définition des capabilities

Après les "NameSpaces" et les "CGROUPS" c'est la troisième brique de la "containairisation".

Les "capabilities" s'appliquent aux THREAD(Processus légers Linux) et aux fichiers binaires.

Un processus ou un ensemble de processus doit avoir ce qu'il lui faut comme "capabilities" afin de fonctionner mais pas plus sous peine de servir de passerelle à un attaquant.

Les "capabilities" peuvent aussi servir afin de donner des capacités à un programme sans avoir besoin de l'ensemble des droits du compte "root" ou d'avoir à positionner le "bit SUID".

Les systèmes de fichiers les plus courants implémentent les "capabilities" dans les inodes.

Il existe deux "library" pour travailler avec les "capabilities". Installez donc aussi le package "libpcap-ng-utils".

Ces packages vous donneront accès aux commandes pour afficher ou modifier les "capabilities" :

- capsh
- getcap
- filecap
- setcap

2 Lecture des capabilities

1. Quelles sont les pouvoirs des "capabilities" suivantes : CAP_NET_ADMIN,CAP_NET_RAW, CAP_NET_BIND_SERVICE, CAP_SYS_ADMIN.
2. Retrouvez les capabilities de votre kernel à l'aide la commande "firejail –debug-caps".
3. Listez tous les programmes de votre machine avec "capabilities" avec la commande suivante :

```
getcap -r / 2>/dev/null
```

4. A l'aide de la commande getcaps retrouvez les capabilities attachées au programme ping.

5. Sous l'utilisateur "test" visualisez les capabilities de votre processus bash dans /proc à l'aide de la commande suivante :

```
cat /proc/$$/status | egrep "^Cap"
```

6. A quoi correspondent CapInh,CapPrm,CapEff ?
7. Que donne la commande précédente avec un processus bash sous root ?
8. Utilisez capsh –decode=valeur pour décoder les "effective capabilities" ?
9. Sous un utilisateur non privilégié refaites les opérations précédentes. Rassuré ?

3 Modifications des capabilities

1. Lancez la commande "python3 -m http.server port" avec comme port 9000 puis 80. Que se passe-t-il avec le port 80 ?
2. Donnez la "capability" permettant de se binder sur le port 80 avec setcap.
3. Vérifiez avec getcap que la capability a bien été acquise.
4. Sous root enlevez toutes les capabilities à votre processus bash et verifiez que vous ne pouvez plus rien faire (ping, tcpdump...).

```
capsh --drop=all --secbits=1 --
```