

**Introduction**

Postman est une machine linux dont l’adresse IP est 10.10.10.160.

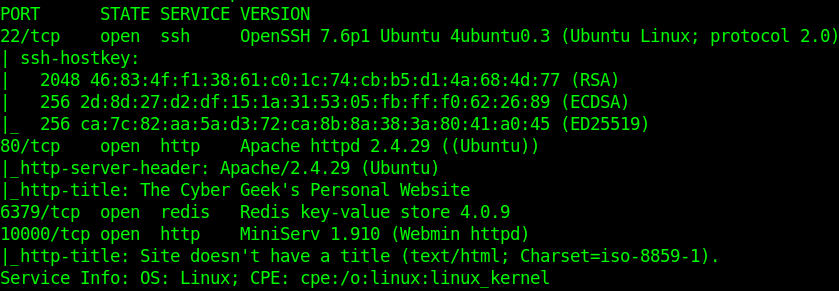
Compétences mises en œuvre :

* Enumération des ports et services d’un ordinateur.

**Enumération initiale**

Nous commençons comme d’habitude avec un scan nmap pour découvrir les ports et services ouverts :

|  |
| --- |
| $ nmap -T4 -A 10.10.10.160 |



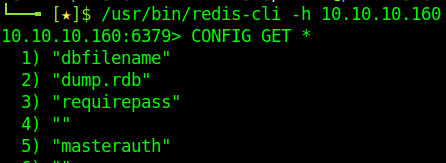
Plusieurs ports sont ouverts :

* 22 pour un serveur ssh
* 80 pour un serveur web
* 6379 pour un serveur de données structurées
* 10000 pour un serveur web

**Obtenir un accès utilisateur**

Le port 6979 n’est pas commun donc en faisant des recherches sur le service qui tourne derrière. Apparemment les versions entre Redis 4.0 et 5.0 sont vulnérables aux RCE. Un script redis-cli est disponible pour vérifier si la vulnérabilité est présente :

|  |
| --- |
| $ locate redis-cli  $ /usr/bin/redis-cli -h 10.10.10.160 |



170 lignes sont présentes sur la configuration. En regardant la configuration, nous trouvons que le dossier par défaut est /var/lib/redis. Nous allons donc fouiller par là-bas :



Il faut apparemment tester si chaque dossier existe en faisant une requête..

**Obtenir un accès administrateur**

Bla