[info]

**Introduction**

Help est une machine Linux dont l’adresse IP est 10.10.10.121.

Compétences mises en œuvre :

* Enumération des ports et services.
* Enumération des dossiers/fichiers d’un site web.
* Recherche et exploitation d’exploit manuel (sans metasploit).
* Exploitation kernel.

**Enumération initiale**

Toujours la même, on commence avec une énumération des ports et services accessible depuis notre machine attaquante avec nmap :

|  |
| --- |
| $ nmap –T4 –A 10.10.10.121 |

[nmap]

Trois ports sont visibles :

* 22 pour un service ssh.
* 80 pour un serveur web.
* 3000 pour un ppp.

**Obtenir un accès utilisateur**

Nous allons aller inspecter manuellement le site web, mais avant, lançons une énumération des dossiers et fichiers du site web avec dirsearch :

|  |
| --- |
| $ dirsearch -w wordlist.txt -x 403 -e "php,html" -t 100 -f -u http://10.10.10.121/ |

[dirsearch]

**Obtenir un accès administrateur**

On fait une énumération de la version du noyau :

|  |
| --- |
| $ uname -a |

[uname]

Cette version est vulnerable, une petite recherche sur searchsploit permet de trouver une LPE :

|  |
| --- |
| $ searchsploit linux 4.4.0-116 |

[searchsploit2]

On récupère l’exploit, le rend exécutable et on devient root :

|  |
| --- |
| $ cp  $ chmod +x  $ ./exploit.py |