[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 autre serveur web.

**Obtenir un accès utilisateur**

Nous allons aller inspecter les sites web, mais avant, lançons une énumération des dossiers et fichiers des sites web avec dirsearch :

|  |
| --- |
| $ dirsearch -w wordlist.txt -x 403 -e "php,html" -t 100 -f -u http://10.10.10.121/ |
| $ dirsearch -w wordlist.txt -x 403 -e "php,html" -t 100 -f -u http://10.10.10.121:3000/ |

[dirsearch]

Rien de vraiment suspect, rien de detecté sur le port 3000, avant de lancer une nouvelle recherche avec une meilleure wordlist et plus d’extension, nous allons donc aller manuellement sur les deux sites pour voir des liens suspects ou des versions de logiciels ou encore des indices. Sur le port 80, la page support indique un logo de HelpDeskz, nous allons faire une recherche avec searchsploit :

|  |
| --- |
| $ searchsploit helpdeskz |

[searchsploit]

Apparemment, il y a un exploit pour uploader des fichiers sur le site, très intéressant pour upload un reverse shell.

**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 |