[info]

**Introduction**

La machine distante est un linux dont l’adresse IP est 10.10.10.60.

Compétences mises en œuvre :

* Enumération des ports et services.
* Identification puis énumération des dossiers et fichiers du pare-feu.
* Exploitation manuelle d’un exploit.

**Enumération**

On commence l’énumération de la machine avec le binaire **nmap** pour connaitre les ports ouverts et les services qui y sont reliés :

|  |
| --- |
| $ nmap -T4 -A 10.10.10.60 |

[nmap]

Les ports **80** et **443** sont ouverts avec un serveur web **lighttpd** en version **1.4.35**, nous allons faire un petit tour sur les interfaces avec Firefox pour voir les différentes pages accessibles et trouver des informations en plus (les pages contacts ou informations peuvent donner des indications sur un username ou sur la technologie mise en place), nous nous rendons compte que les sites web repose sur un firewall connu : **pfsense**.

Une rapide recherche d’exploit/CVE sur google concernant **pfsense** résulte sur un exploit en RCE mais nécessite un identifiant et un mot de passe. Donc nous allons continuer l’énumération sur les sites web.

Le port **80** n’ayant rien d’intéressant, nous allons décider d’énumérer les dossiers et fichiers que peut contenir le site web sur le port **443** avec le binaire **dirsearch** :

|  |
| --- |
| $ dirsearch -w wordlist -e ".txt,.php" -r 2 -f -u https://10.10.10.60:443/ |

[dirsearch]

Le fichier **changelog.txt** est à lire puisqu’il contient tous les derniers changements qui ont été effectués. On peut voir qu’il contient juste des patchs contre des vulnérabilités :

[changelog]

Les différents fichiers sont bons à lire, ne serait-ce que pour jeter un coup d’œil s’il n’y a pas d’informations supplémentaires dedans. Le fichier **system-user.txt** contient un identifiant et son mot de passe pour pfsense :

[system-user.txt]

**Exploitation**

Bla