

**Introduction**

Bounty est une machine Windows dont l’adresse IP est 10.10.10.93.

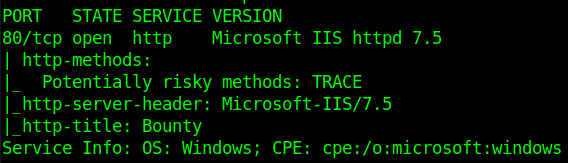
Compétences mises en œuvre :

* Enumération des ports et services d’une machine distante.

**Enumération initiale**

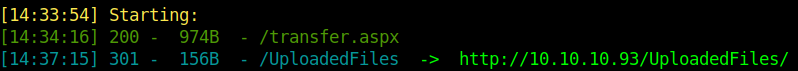
Nous commençons par l’énumération des ports et services avec nmap :

|  |
| --- |
| $ nmap -T4 -A 10.10.10.93 |



Seul le port 80 est ouvert, cela va nous simplifier la tâche. Nous allons faire une énumération des fichiers/dossiers avec dirsearch (on spécifie l’extension aspx en plus car il s’agit d’un serveur windows enface) :

|  |
| --- |
| $ dirsearch -w wordlist -e "php,txt,aspx" -x 404,400,403 -f -t 100 -u http://10.10.10.93/ |



Un dossier qui n’es pas accessible et un fichier transfer.aspx qui nous propose d’uploader des fichiers.

**Obtenir un accès utilisateur**

En recherchant sur google une RCE pour IIS 7.5, nous tombons sur un fichier web.config que nous pouvons uploader

**Obtenir un accès administrateur**

Bla