# **PROJET PRO – TOOLBOX**

par

Christophe GUZIK

**Sup de VINCI – Pôle Universitaire Léonard de Vinci**

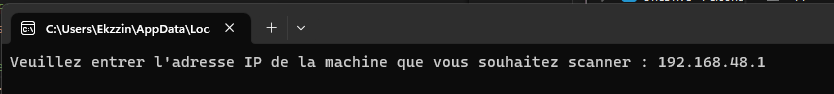
*CNIT - 2 Place de La Défense 92800 PUTEAUX*

## Scan de vulnérabilité

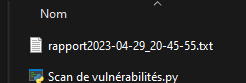
Le scan de vulnérabilité se fait au travers un script écrit en Python. Il utilise le logiciel NMAP et les libraires OS et DATETIME de Python. NMAP va nous permettre d’effectuer le scan mais à celui-ci été ajouté un script en plus qui se nomme « vulners ». Il va nous permettre d’indiquer les vulnérabilités sur les protocoles détectés. Vulners est une base de données qui est installé avec NMAP par défaut.

Après avoir effectué le scan, il nous créé un rapport dans un fichier texte qui s’affichera dans la console. On peut retrouver ce rapport dans le dossier où se situe le script et est nommé.

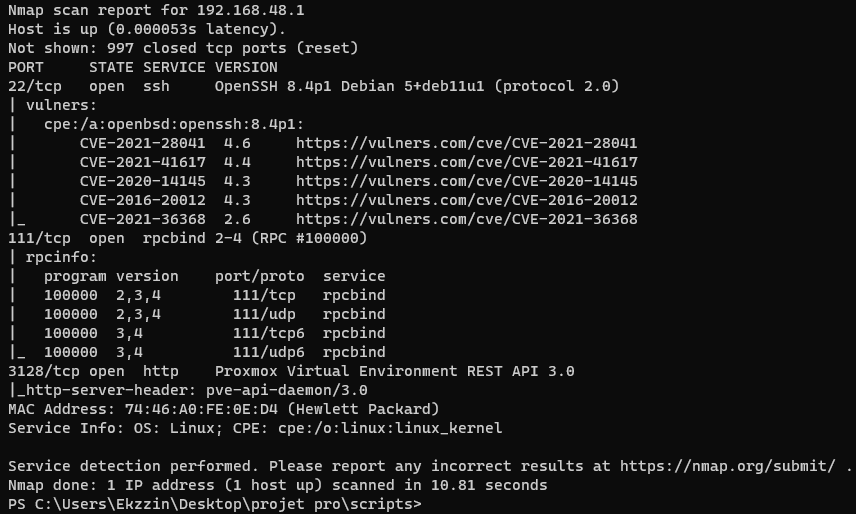
Lorsque l’on lance le script, il nous demande la machine que l’on souhaite scanner :



On insère donc l’IP que l’on souhaite et on laisse le script faire son travail. Une fois le scan terminé on remarque qu’un fichier texte à bien été créé :

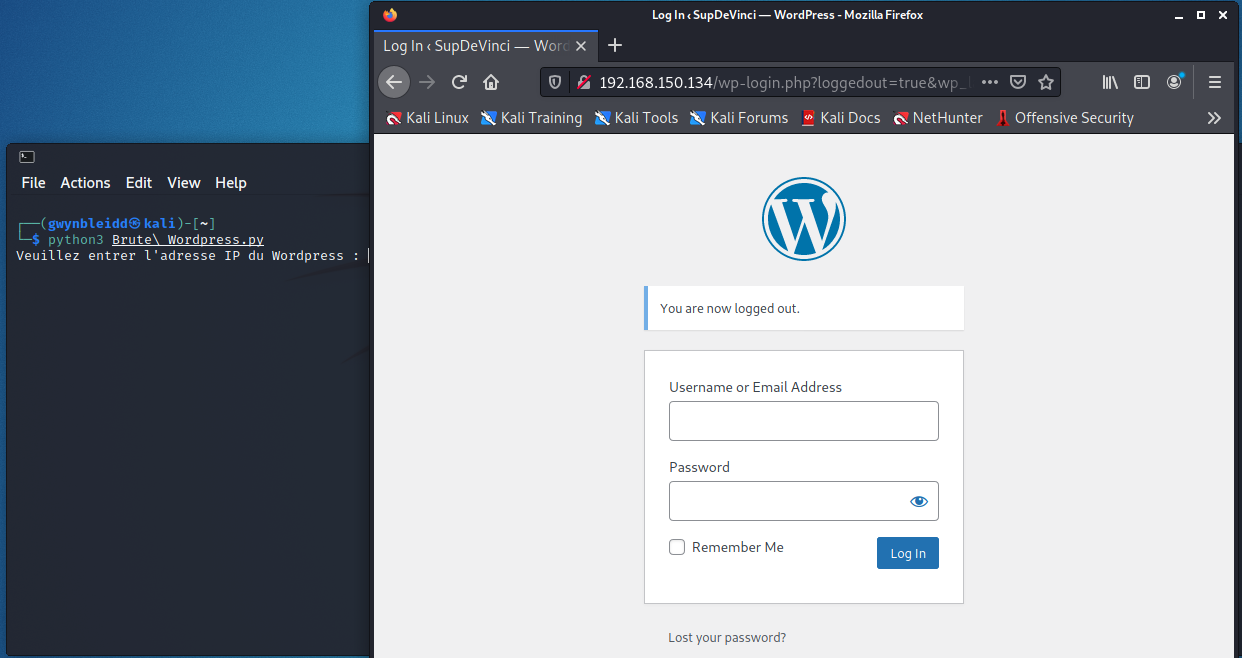


Et dans la console où le script a été exécuté on voit bien le résultat de la commande NMAP :



## Brute de Wordpress

Une nouvelle fois avec un script Python et NMAP nous avons la possibilité de faire une brute force sur un site Wordpress afin d’avoir les crédenciales du compte administrateur. C’est un script installé avec NMAP qui se nomme « http-wordpress-brute ». On peut utiliser des wordlists qui sont déjà préinstallés avec kali ou on peut les télécharger sur des GitHub, ce que j’ai fait afin d’avoir une liste à jour. Ce que le script va faire c’est tenter de se connecter en boucle avec tous les mots qui se trouvent dans ces wordlists jusqu’à qu’une combinaison fonctionne. Mon script Python est assez basique car la commande est déjà écrite il nous faut tout simplement indiquer la cible (qui est un Wordpress bien évidemment).



L’IP de notre cible est 192.168.150.134 avec un port en 80. Lorsque l’on lance le script avec la commande « python3 Brute\ Wordpress.py » il nous demande l’IP de la cible et ensuite le port de celle-ci.



Le NMAP va tenter de trouver s’il y a bien un Wordpress actif sur le port indiqué. Après avoir brute force il nous donne les informations nécessaires :

