CTF – wordpress

ENZO RIMBAULT

BTS SIO 1

02/02/2024

Sommaire

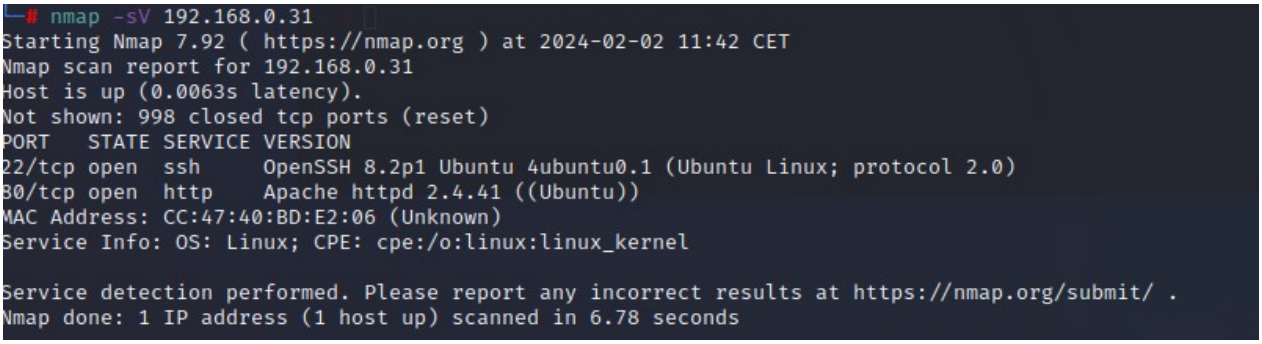
Wordpress

WordPress est un système de gestion de contenu gratuit, libre et open-source. Ce logiciel écrit en PHP repose sur une base de données MySQL et est distribué par la fondation WordPress.org.

Exploit Faille Wordpress

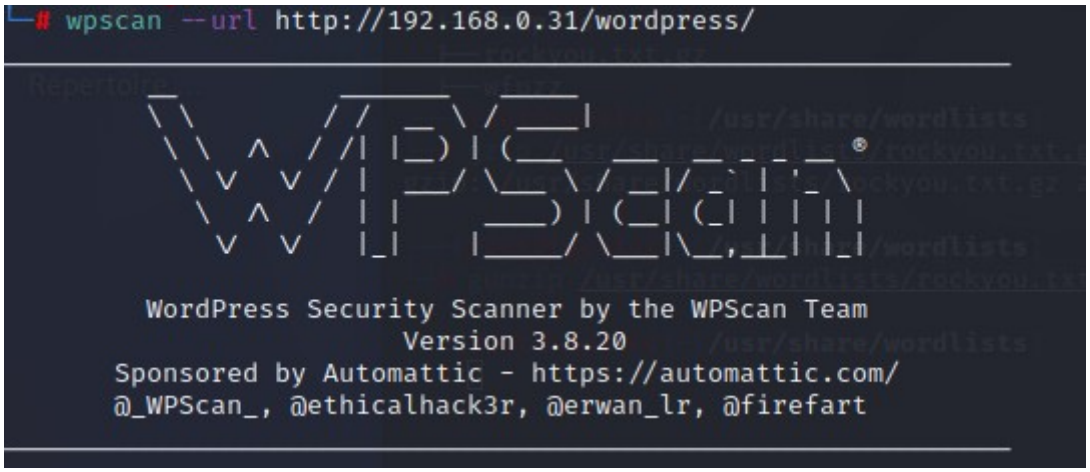
Pour exploiter cette faille on va utiliser un outil qu'on retrouve sur kali. Cet outils s'appelle WPSCAN.

Mais avant ça, on fait un nmap suivi de l'ip de la machine pour y voir ses ports ouverts.



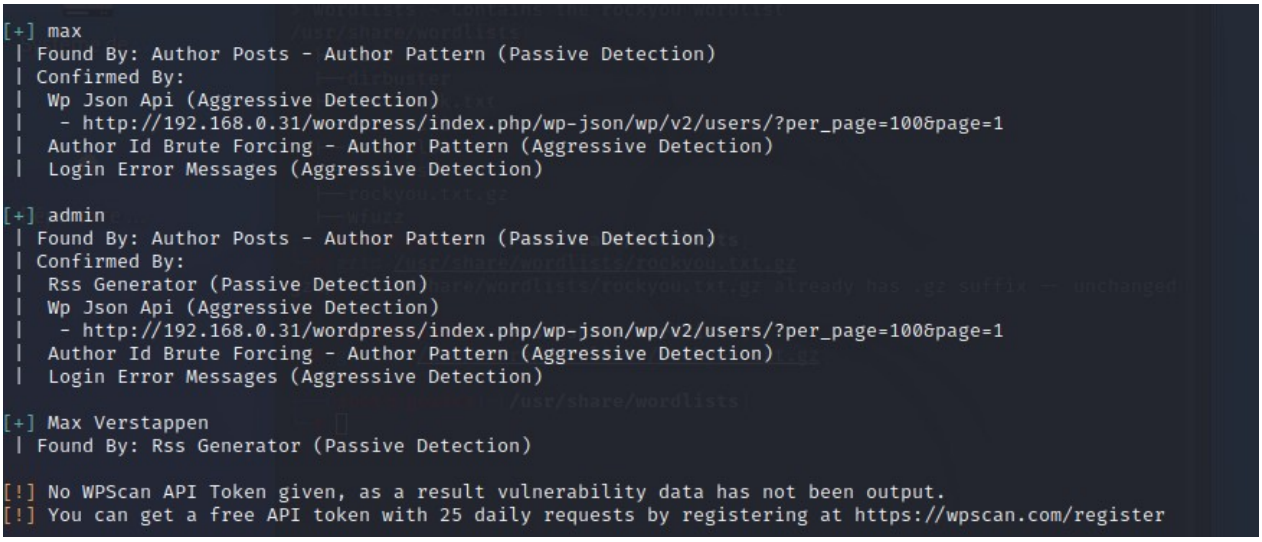
On peut voir que le port 80 est ouvert et quand on va sur le site de la machine, on tombe sur un wordpress.

On peut donc maintenant faire un wpscan de l'adresse du site.



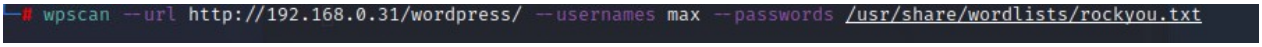
Ensuite on recherche les utilisateurs identifiés sur ce wordpress avec la commande

wpscan –-url (votre adrese url) –e u

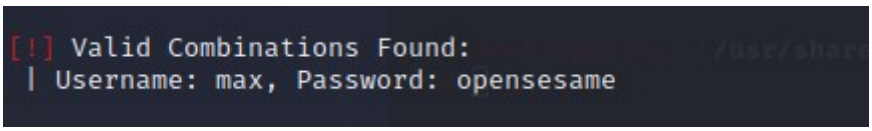


Avec cette commande on y retrouve 3 utilisateurs.

Maintenant on va utiliser un fichier texte contenant des mots de passes possible et essayer de trouver le bon mot de passe



On peut voir ci-dessous que le script a trouvé un mot de passe possible



On a plus qu’à l’utiliser pour se connecter sur le site.