Challenge2 : Chessboard CTF

Pour la catégorie des challenges moyenne/difficile nous avons choisi CTF qui se fait en deux machines Debian. Pour parvenir à nos fins, il vous faudra capturer 7 flags à différents niveaux au cours de la résolution du challenge. En vous aidant par des hints qui permettent de vous aider afin de trouver les flags. Pour la première machine héberge un site web avec base de données et un site wordpress (un système de gestion de contenus (CMS)) que le développeur a oublié à l'héberger. Un autre site web est vulnérable au SQL Injection et le site de blog partage le mot de passe de admin login avec le site, qui peut être piraté par SQLi. Dans cette machine, nous cachons les flags de 1 à 3, et aussi l'information nécessaire pour accéder à la deuxième machine.

Pour la machine 2, vous pouvez obtenir dans le fichier known_hosts de la première machine mot de passe haché. Dans cette machine, il existe plusieurs utilisateurs, respectivement existe le flag.

Les étapes de la création :

La création de ce challenge s'est basée sur un ensemble des étapes cohérent :

1. Création de deux machines Debian avec une adresse privée et une autre flottante qui sont disponibles sur open Stack.

2. Création d'un site Web hébergé par python dans le port 8000 contenants une fail de SQL injection qui permet l'accès à la base de donne et récupérer les logins et les mots de passe ainsi que le deuxième flag (flag2 comme nom de l'utilisateur et son contenu comme mot de passer).

3. Création d'un blog Wordpress hébergé dans apache à l'aide de Docker dont le login est le mot de passe est celle trouvée dans l'attaque SQL Injection précédente. Pour pouvoir se connecter, le hacker doit aller à /login. Par suite, l'attaquant doit aller à la corbeille du site pour trouver le 3e flag.

5. Dans machine 1 : Création de hint login – mdp hashé SHA1 et IP de la 2eme machine

6. Dans machine 2 : Création de 4 utilisateurs pour chaque niveau de privilege escalation

7. Utilisateur Rook : Création de backup.sh et cronjob pour backup.sh

8. Utilisateur Queen : Création d'un fichier binaire vulnerable au PATH Variable Vulnerable

9. Utilisateur Pawn : Création d'un fichier 32 bits mount_pawn qui est SUID permettre les autres a mount avec privilege de root, buffer-overflow vulnerable