Une image contenant cadenas, verrouiller

Le contenu généré par l’IA peut être incorrect.

|  |
| --- |
| TryHackMe  Capture the Flag  Room : Silver Platter (easy) |
| TryHackMe | Cyber Security TrainingUne image contenant oiseau, Graphique, conception  Description générée automatiquement |
| Réalisé par : CHARPEIL Romain |

## Scanning

Pour ce CTF là, j’ai recherché comment effectuer un scan disons ‘réaliste’ :

Nmap -sS -p- -sV --version-light -O --osscan-limit @ip

-sS : SYN scan (demi-connexion, plus discret qu'un TCP connect -sT)

-p- : Scanne tous les ports (1-65535) au lieu des 1000 par défaut

-sV --version-light : Détecte les versions des services mais en mode léger

-O --osscan-limit : Essaie d’identifier l’OS mais uniquement si les conditions sont bonnes

Une image contenant texte, capture d’écran, Police, document

Le contenu généré par l’IA peut être incorrect.

Port 80 et 8080 ouverts, on va dans un premier temps regarder depuis le port 80 ce que l’on pourrait énumérer puis dans un second temps le port 8080.

## Enumération

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Le contenu généré par l’IA peut être incorrect.

Une image contenant texte, Police, capture d’écran

Le contenu généré par l’IA peut être incorrect.

Une image contenant texte, capture d’écran, logiciel, Police

Le contenu généré par l’IA peut être incorrect.

On a un nom ’Silverpeas’

On a un username déjà nommé : ‘scr1ptkiddy’ sensé être le manager.

Enumérant avec Fuzz :

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Rien d’intéressant sur le port 80 à part les 2 indices donnés, on passe maintenant au port 8080.

Une image contenant capture d’écran, texte, logiciel, Logiciel multimédia

Le contenu généré par l’IA peut être incorrect.

Donc sans préciser de chemin, nous avons une erreur 404 not Found.

Personnellement, je pense j’ai eu un peu de chance, j’ai tenté de rentrer le nom donné dans le port 80 ‘Silverpeas’ :

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Le contenu généré par l’IA peut être incorrect.

Nous avons une interface, et je le rappel, également un nom d’utilisateur ‘scr1ptkiddy’

J’ai regardé s’il y avait possiblement une vulnérabilté SQLi mais ce n’est pas le cas ;

J’ai également regardé s’il y avait des exploits possibles avec des recherches google :

Une image contenant texte, capture d’écran, logiciel, Police

Le contenu généré par l’IA peut être incorrect.

Comment fonctionne l’exploit :

Voici la traduction en français du texte technique concernant la vulnérabilité CVE-2024-36042 dans Silverpeas :

Silverpeas jusqu'à la version 6.3.4 incluse est vulnérable à un contournement simpliste de l'authentification. Lors de l'authentification, si l'expéditeur omet le champ de formulaire du mot de passe, l'application connecte l'utilisateur spécifié sans aucune vérification.

Exemple de requête de connexion standard :

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Login=SilverAdmin&Password=SilverAdmin&DomainId=0

Cette tentative échouera (sauf si le mot de passe par défaut n'a pas été modifié), et vous serez redirigé vers la page de connexion avec un code d'erreur.

En revanche, si vous supprimez le champ du mot de passe :

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

La connexion réussira généralement et vous redirigera vers la page principale, maintenant connecté en tant que super admin.

Fonctionnement :  
Ce bug fonctionne avec tout utilisateur valide, mais *SilverAdmin* est le super admin par défaut.

## Exploitation

Je vais donc tester l’exploit en question, avec Burp Suit ,

Il est indiqué qu’il faut comme condition de fonctionnement, un utilisateur valide, comme trouvé précédemment, on a le ‘scr1ptkiddy’ :

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Le contenu généré par l’IA peut être incorrect.

J’ai intercepté la requête pendant la connexion sans indiquer de mots de passes,

Comme précisé dans la CVE, si j’enlève le champ ‘password’ dans le variable Login, je devrais pouvoir Bypass l’authentification :

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Le contenu généré par l’IA peut être incorrect.

On a bien réussi à Bypass l’authentification

Une image contenant texte, capture d’écran, Police, logiciel

Le contenu généré par l’IA peut être incorrect.

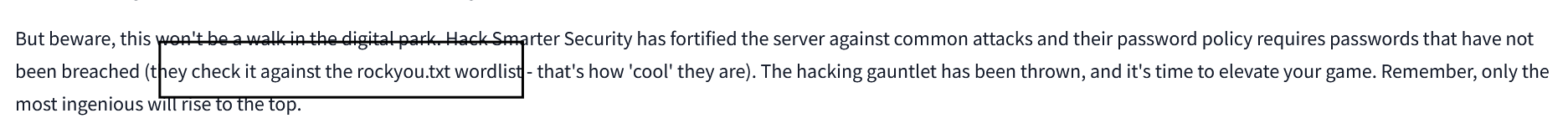
Ici, on a un nom, possiblement un utilisateur ‘tyler’

J’ai essayé de m’y connecter en ssh mais je n’ai pas le mot de passe :

Je vais essayer avec hydre de le brute force :

hydra -l <nom\_utilisateur> -P <fichier\_mots\_de\_passe> ssh://<adresse\_IP>

Ça n’a pas fonctionné car :



Ils ont mis en place une politique de mots de passe qui interdisent d’utiliser les mots de passe provenant de la wordlist rockyou.txt

Par contre j’ai vu ça :

Une image contenant texte, Police, capture d’écran

Le contenu généré par l’IA peut être incorrect.

Il y un autre utilisateur, qui est donc également impacté par la CVE, nous allons nous y connecter :

Une image contenant texte, capture d’écran, logiciel, Police

Le contenu généré par l’IA peut être incorrect. \*SilverAdmin

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Le contenu généré par l’IA peut être incorrect.

On est bien loggé en tant qu’administrateur :

Je n’ai rien de trouvé qui pourrait être un indice depuis l’administrateur, par contre un autre utilisateur est apparu :

Une image contenant texte, ligne, Police, capture d’écran

Le contenu généré par l’IA peut être incorrect.

‘Manager’

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Le contenu généré par l’IA peut être incorrect.

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Le contenu généré par l’IA peut être incorrect.

On a bien réussi à s’authentifier, on peut voir une notification non lue :

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

On a des identifiants de connexion SSH au serveur cible :

User : tim

Password : cm0nt!md0ntf0rg3tth!spa$$w0rdagainlol

Une image contenant texte, Police, capture d’écran

Le contenu généré par l’IA peut être incorrect.



## Elévation de Privilèges



Cela signifie que notre utilisateur Tim a accès aux logs,

Si on cat /var/log/auth.log.2 :

Une image contenant texte, capture d’écran, Police

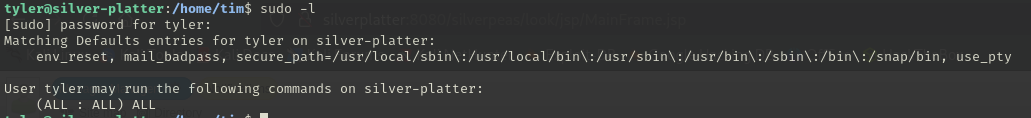
Le contenu généré par l’IA peut être incorrect.

Dec 13 15:45:57 silver-platter sudo: tyler : TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/docker run --name silverpeas -p 8080:8000 -d -e DB\_NAME=Silverpeas -e DB\_USER=silverpeas -e DB\_PASSWORD= \_Zd\_zx7N823/ -v silverpeas-log:/opt/silverpeas/log -v silverpeas-data:/opt/silvepeas/data --link postgresql:database silverpeas:6.3.1

Si on utilise ce mot de passe pour se connecter à Tyler :

Une image contenant texte, Police, capture d’écran, ligne

Le contenu généré par l’IA peut être incorrect.



Si je comprend bien, l’utilisateur a tout les droits, donc il peut lister le contenu dans root grâce à sudo :

