Une image contenant cadenas, verrouiller

Le contenu généré par l’IA peut être incorrect.

|  |
| --- |
| TryHackMe  Capture the Flag  Room : BillingV2 (easy) |
| TryHackMe | Cyber Security TrainingUne image contenant oiseau, Graphique, conception  Description générée automatiquement |
| Réalisé par : CHARPEIL Romain |

## Scanning

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

### Enumération

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

Le contenu généré par l’IA peut être incorrect.

### Exploitation

Depuis l’interface, j’ai essayé SQli, XSSi, dirsearch, changer les cookies, mais aucun n’a été concluant

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

Le contenu généré par l’IA peut être incorrect.

C’est un software date de 2007, des vulnérabiltés doivent être possible.

Directement depuis exploit db, je n’en ai pas trouvé, mais sur internet quand on tape ‘mbilling exploit ‘ :

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

Le contenu généré par l’IA peut être incorrect.

On s’aperçoit qu’il y a un exploit, depuis Metasploit qui met en place un shell sur le serveur cible :

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

Le contenu généré par l’IA peut être incorrect.

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

Le contenu généré par l’IA peut être incorrect.

On peut lire le user.txt dans /home/magnus

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

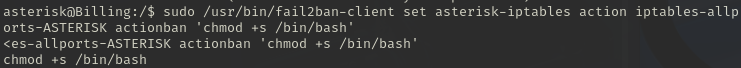
Le contenu généré par l’IA peut être incorrect.

### Elévation de privilèges

Directement je fais un sudo -l et je m’aperçois qu’on a les droits SUDO pour /usr/bin/fail2ban

*Fail2Ban est un outil de sécurité utilisé pour protéger les serveurs contre les attaques par force brute et autres tentatives malveillantes en bloquant temporairement les adresses IP suspectes. Il fonctionne en analysant les fichiers de logs des services (comme SSH, Apache, Nginx, etc.) et en appliquant des règles de bannissement via iptables, firewalld ou d'autres pare-feux.*

sudo /usr/bin/fail2ban-client set asterisk-iptables action iptables-allports-ASTERISK actionban 'chmod +s /bin/bash'



* Actionban : Action déclenchée lors du bannissement d'une IP (ex: bloquer via iptables).
* Ici, elle est détournée pour ajouter le **bit SUID** à /bin/bash, permettant son exécution avec les droits **root**.

*Le bit SUID (Set User ID) est une permission spéciale dans les systèmes Linux et Unix qui permet à un fichier exécutable d'être exécuté avec les privilèges du propriétaire du fichier, plutôt que ceux de l'utilisateur qui l'exécute*

sudo /usr/bin/fail2ban-client set asterisk-iptables banip 1.2.3.4



* Simule le bannissement d'une IP, exécutant ainsi chmod +s /bin/bash en tant que root

/bin/bash -p

* Lance un shell avec les privilèges conservés (SUID), donnant un accès root

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

Le contenu généré par l’IA peut être incorrect.