Architecture d'un Système d'Exploitation

Introduction à la sécurité informatique en environnement HPC

Travaux Pratiques

F. Combeau

7 et 21 novembre 2022

1. Le fichier d'importation de la machine virtuelle est le fichier :
   `CentOS7_2022.ova`

   sha256sum :
   `bd7e8b09fda589df4e477af34812bc0dd36e5bd6c2718279f271af1f59f3cf82 CentOS7_2022.ova`

2. Tout le TP se déroulera dans la machine virtuelle « CentOS7_2022 »

3. Importer la machine virtuelle « CentOS7_2022 » (**`CentOS7_2022.ova`**) dans Virtual Box en mode 64 bits et la démarrer

---

4. Se connecter en mode console sur la machine virtuelle « CentOS7_2022 » avec le compte root (password : ensiie_R00T!)

5. Quel type d'authentification avez-vous utilisé pour vous connecter ?

6. Où est stocké le mot de passe de root et sous quelle forme ? Pourquoi ?

7. Pouvez-vous déterminer le mot de passe de Bob ? Et celui d'Alice ?

8. Regardez la configuration PAM de login (/etc/pam.d/login). Que se passerait-il si la ligne pam_unix.so passait de « sufficient » à « required » **(ne pas faire cette modification)** pour le login de root en mode console ? Et pour Bob ?

9. Sous le compte root, connectez-vous en SSH sur la machine locale avec le compte de Bob (ssh bob@localhost). Est-ce possible ?

10. Regardez dans les logs pour voir si voyez une trace de votre connexion (/var/log/secure). A quoi ressemble cette trace ?

11. Regardez la configuration PAM de sshd (/etc/pam.d.sshd). Modifiez la ligne pam_succeed_if.so de « requisite » à « required », puis de « required » à « sufficient ». D'aprés vous, qu'est-ce que cela va changer ? Expliquez brièvement pourquoi.

12. Sous le compte root, connectez-vous en ssh sous le compte d'Alice. Est-ce que cela fonctionne ? Pourquoi ? A quoi correspond le mot de passe demandé ? Que voyez-vous dans

les logs pour cette connexion ? Est-ce que l'authentification a été réalisée par les PAM ? Quel type d'authentification a été utilisé ?

---

13. Sous le compte de Bob, créé un répertoire « test ». Quelles sont ses protections ? Pourquoi ?

14. Sous root, créez un fichier dans le répertoire « test » de Bob. Avez-vous le droit ? A qui appartient ce fichier et quelles sont ses protections ? Pourquoi ?

15. Sous Bob, avez-vous le droit d'effacer le fichier de root dans « test » ? Pourquoi ?

16. Rajouter le « sticky bit » au répertoire « test ». Comment faites-vous ?

17. Sous root, créez un autre fichier dans le répertoire « test » de Bob. Avez-vous toujours le droit ?

18. Sous Bob, avez-vous le droit d'effacer le fichier de root dans « test » ?

19. Sous root, changez le propriétaire du répertoire « test » de Bob pour root. Comment faites-vous ?

20. Sous root, créez un nouveau fichier dans le répertoire « test » de Bob. Est-ce que Bob peut l'effacer ? Pourquoi ?

---

21. Recherchez sur le système un exécutable avec le setuid bit positionné (la commande find avec les arguments -perm et -type est votre ami) ? Pouvez-vous expliquer pourquoi un des exécutables que vous avez trouvé a besoin de ce ce setuid bit ?

---

22. Bob a besoin de partager un fichier qu'il va périodiquement mettre à jour pour Alice et réciproquement. Sans modifier les protections des répertoires HOME d'Alice et Bob, comment pouvez-vous répondre à ce besoin ?

---

23. Regardez la configuration sshd (/etc/ssh/sshd_config) pour l'utilisateur sftp. Que remarquez-vous ? Essayez de vous connecter en ssh avec l'utilisateur sftp. Essayez de vous connecter en sftp avec l'utilisateur sftp (sftp sftp@localhost). Que remarquez-vous (vous pouvez vous connecter en sftp avec l'utilisateur Bob pour comparer) ?

---

24. Est-ce que root peut prendre l'identité de Bob et d'Alice avec la commande su ? Est-ce qu'une authentification a été demandée ? Pourquoi ? Quelle est la différence entre les commandes « su bob » et « su - bob » ?

25. Est-ce que Bob peut prendre l'identité de root avec la commande su ? Est-ce qu'une authentification a été demandée ?

26. Est-il possible d'interdire Bob de se servir de la commande su pour passer root, même s'il connaît le mot de passe de root ? Comment faire ?

27. Est-ce que Bob peut passer root en utilisant ssh (ssh root@localhost) ? Comment lui

interdire de passer root en utilisant ssh (configuration PAM ou sshd) ?

---

28. Est-ce que Bob est autorisé à utiliser la commande sudo ? Si non, que doit-on faire pour l'autoriser (il existe deux méthodes : une avec modification du fichier /etc/sudoers et une sans aucune modification à ce fichier) ? Doit-il connaître le mot de passe root pour utiliser sudo ?

29. Est-il possible d'autoriser Bob à utiliser uniquement certaines commandes en tant que root sans lui donner un accès interactif en tant que root (par exemple, cat /var/log/secure) ? Si oui, comment ?Et sans qu'il est à taper son mot de passe ?

---

30. Quel est le shell d'Alice ? Où est-il défini ?

31. Que se passe-t-il si on le change par /bin/false ? Et par /sbin/nologin ? Y-a-t-il une différence ?

32. Que se passe-t-il si on change le shell d'Alice par /bin/rbash ?

33. Comment est défini /bin/rbash (ls -l /bin/rbash) ?

---

34. Créez un système de fichiers chiffré dans un fichier local via un loop device (en root):
    - créez un fichier rempli de zéro de 10 Mo :
      dd if=/dev/zero of=cryptofs bs=1024 count=10240
    - créez un loop device (/dev/loop0) pointant vers le fichier local cryptofs :
      losetup /dev/loop0 ./cryptofs
    - chiffrez le loop device (/dev/loop0) via la commande cryptosetup :
      cryptsetup luksFormat /dev/loop0
    - ouvrez le device chiffré pour le mapper sur un device déchiffré :
      cryptsetup luksOpen /dev/loop0 dm-cryptofs
    - créez un système de fichiers dans le device déchiffré :
      mkfs.ext4 /dev/mapper/dm-cryptofs
    - montez le système de fichiers déchiffré dans un répertoire :
      mount /dev/mapper/dm-cryptofs /mnt
    - utilisez le point de montage comme n'importe lequel point de montage (créez des fichiers texte)

35. Créez un système de fichiers non chiffré dans un fichier local via un loop device (en root):
    - créez un fichier rempli de zéro de 10 Mo :
      dd if=/dev/zero of=nocryptofs bs=1024 count=10240
    - créez un loop device (/dev/loop0) pointant vers le fichier local cryptofs :
      losetup /dev/loop1 ./nocryptofs
    - créez un système de fichiers dans le device non chiffré :
      mkfs.ext4 /dev/loop1
    - montez le système de fichiers chiffré dans un répertoire :
      mount /dev/loop1 /mnt1
    - recopiez le contenu du point de montage chiffré (/mnt) vers le point de montage non chiffré (/mnt1)
      cp -R /mnt /mnt1

36. Lancez la commande strings sur le fichier local chiffré et sur le fichier local non chiffré. Que constatez-vous ?

---

37. Lancez la commande sestatus en tant que root ? Que renvoie cette commande ?

38. Lancez la commande ps axZ et regardez les contextes SELinux. Que constatez-vous pour les services et le service sshd ?

39. Lancez la commande ls -lZ /etc/ssh/. Que constatez-vous ?

40. Que se passerait-il si le service sshd était utilisé par un utilisateur malveillant pour passer root (id sous root donne le contexte SELinux de root) ?

---

41. Lancez la commande sous root iptables -L -v. Que fait cette commande ? Est-ce que notre système utilise un pare-feu local ? Y-a-t-il une règle qui interdit tout par défaut pour les flux entrants ? Est-ce les flux sortants sont filtrés ? Est-ce que les connexions entrantes vers le service sshd sont autorisées ? Est-ce que cette règle a été utilisée pour nos précédentes connexions ssh ?

---

42. Lancez la commande ssh -p 8000 localhost, sous Bob. Que fait cette commande ? Est-ce qu'elle fonctionne ? Pourquoi ?

43. Lancez la commande ssh -L8000:localhost:22 localhost, sous Bob. Que fait cette commande ? Est-ce qu'elle fonctionne ? Pourquoi ? Quelle application voyez-vous à une telle commande (option -L et option -R de ssh) ?

---

44. Quels sont les fichiers présents dans /var/log gérés par rsyslog (/etc/rsyslog.conf et /etc/rsyslog.d) ?

45. Envoyez un log de facility local3 et de priority info (commande logger) ? Dans quel fichier de logs, votre message apparaît-il ?

46. Modifiez la configuration de rsyslog pour que tous les message de facility local3 soient stockés dans le fichier /var/log/local3.

47. Est-ce que le système dispose d'une politique d'archivage des logs (logrotate) ? Si oui, quels sont les fichiers concernés par cette politique ? Que faudrait-il modifier dans le fichier de configuration de logrotate pour y ajouter /var/log/local3 ?