Lab 4: Using John the Ripper to Crack Linux Passwords

Locating and Cracking Linux Passwords

1. To view the contents of the passwd file, type:

cat /etc/passwd

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

2. View the permissions on the /etc/passwd file by typing the following command:

ls -l /etc/passwd



3. To view the contents of the shadow file, type:

sudo cat /etc/shadow

Ảnh có chứa văn bản, ảnh chụp màn hình

Mô tả được tạo tự động

4. To create a new user named yoda, type the following command in the terminal:

sudo adduser yoda (then enter password green)

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

5. To create a new user named chewbacca, type the following command in the terminal:

sudo adduser chewbaca (then enter password green)

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

6. Now, view the changes made to the passwd file by typing the following:

tail /etc/passwd

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

9. Next, examine the alterations to the shadow file by typing the following:

sudo tail /etc/shadow

The “!” symbol represents that fact the password has not been set.

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

10. Examine the entries in the auth.log related to account changes by typing:

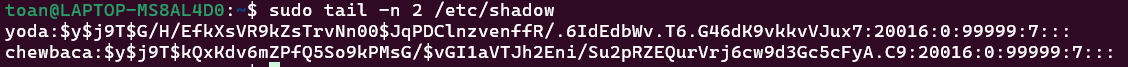
tail /var/log/auth.log

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

11. Next, examine the alterations to the shadow file by typing the following:

sudo tail -n 2 /etc/shadow



12. Examine the entries in the auth.log related to account changes by typing:

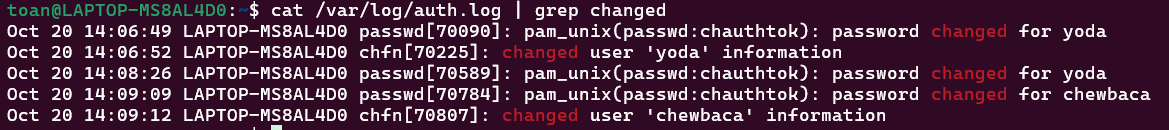
tail /var/log/auth.log

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

13. To look for specific information about password changes within auth.log, type:

cat /var/log/auth.log | grep changed



14. Install john by typing the following command:

sudo apt-get install john

Ảnh có chứa văn bản, ảnh chụp màn hình, thực đơn

Mô tả được tạo tự động

15. Type the following command to see available switches for the john command:

john

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

16. Type the following command to attempt to crack the passwords with john:

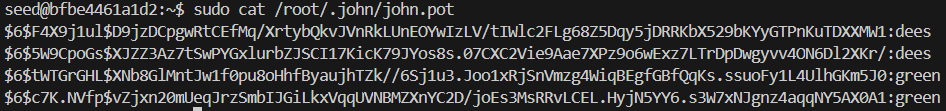
sudo john /etc/shadow

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

17. To view the password hashes and corresponding passwords, type the following:

sudo cat /root/.john/john.pot



18. Type the following command to attempt to crack the passwords with john

sudo john /etc/shadow

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, hàng

Mô tả được tạo tự động

19. Type the following command to remove the existing john.pot file:

sudo rm /root/.john/john.pot



20. Type the following command to re-crack the passwords with john

sudo john /etc/shadow

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

21. To view the first 20 lines of the file, type the following command in the terminal:

head -n 20 /usr/share/john/password.lst

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

22. Set chewbacca’s password to computer by typing computer twice after typing:

sudo passwd chewbaca

Ảnh có chứa văn bản, Phông chữ, ảnh chụp màn hình

Mô tả được tạo tự động

23. Type the following to run john again and the new password hash will be loaded.

sudo john /etc/shadow --wordlist=/usr/share/john/password.lst

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

24. To view the last 20 lines of the file, type the following command in the terminal:

tail /usr/share/john/password.lst

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, màn hình

Mô tả được tạo tự động

25. Set chewbaca’s password to **1q2w3e4r** by typing twice after typing:

sudo passwd chewbaca

Ảnh có chứa văn bản, Phông chữ, ảnh chụp màn hình

Mô tả được tạo tự động

26. Type the following to run john again and the new password hash will be loaded:

john /etc/shadow --wordlist=/usr/share/john/password.lst

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động