Lab 3: Using John the Ripper to Crack Linux Passwords

Introduction

In this lab, students will become familiar with the location where Linux passwords are stored and learn about tools and techniques for breaking Linux passwords.

Passwords help to secure systems running Linux and UNIX operating systems. If an attacker is able to get the root password on a Linux or UNIX system, they will be able to take complete control of that device. The protection of the root password is critical.

passwd file – User accounts on a Linux system are listed in the passwd file which is stored in the /etc directory. The passwd file has less restrictive permissions than the shadow file because it does not store the encrypted password hashes. On most Linux systems, any account has the ability to read the contents of the passwd file.

shadow file – The shadow file also stores information about user accounts on a Linux system. The shadow file also stores the encrypted password hashes, and has more restrictive permissions than the passwd file. On most Linux systems, only the root account has the ability to read the contents of the shadow file.

auth.log – This log file tracks SSH, or Secure Shell, connections. It provides information such as IP addresses, and date and time stamps. It also tracks other events related to security, such as the creation of new user's accounts and new group accounts.

John the Ripper – John the Ripper is an extremely fast password cracker that can crack passwords through a dictionary attack or through the use of brute force.

Cracking Linux Passwords with John the Ripper

Passwords help to secure systems running the Linux operating system. If an attacker is able to get the root password on a Linux system, they will be able to take complete control of that device. The password hashes on a Linux system reside in the shadow file. John the Ripper is an extremely powerful password cracker. It comes loaded by default on all versions of BackTrack, but can be downloaded at www.openwall.com/john/.

Keep in mind that Linux commands are case sensitive. The commands below must be entered exactly as shown.

Locating and Cracking Linux Passwords

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

   seed@ubuntu:~$ cat /etc/passwd

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

   seed@ubuntu:~$ ls -l /etc/passwd

Notice that all users have at least read permissions. Only root has write permissions. At one time, the password was stored in the passwd file. However, due to the fact the passwd file does not have very restrictive permissions, the password is no longer stored there. Instead, there is an X present, which designates that it is stored in the shadow file.

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

seed@ubuntu:~$ sudo cat /etc/shadow

If we create some additional accounts, we can see how the passwd and shadow files are altered. We can also view the information about account changes within the secure log.

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

   seed@ubuntu:~$ sudo adduser yoda (then enter password green)

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

   seed@ubuntu:~$ sudo adduser chewbaca (then enter password green)

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

   seed@ubuntu:~$ tail /etc/passwd

The tail command will display the last 10 lines of the file by default. When users are added to a Linux/UNIX system, the entries are added to the bottom of the file. On a typical Linux system, the first new user is given a User ID, or UID of 1001. Yoda and Chewbacca were given the next available user IDs. The root account has a UID of zero. If another account were able to obtain an UID of 0, the account would also have root permissions.

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

   seed@ubuntu:~$ tail /etc/shadow

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

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

    seed@ubuntu:~$ tail /var/log/auth.log

Next, we will give each user a password. We will use simple passwords for the exercise, but that should never be done on a production system. Avoid dictionary words because attackers can use programs like John the Ripper to crack short passwords or passwords that are found in a dictionary. Stick to passwords with a minimum of eight characters, uppercase and lowercase letters, and special characters. Retype the password and it will be accepted.
For security reasons, the password will not be displayed.

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

    seed@ubuntu:~$ tail –n 2 /etc/shadow

The password hashes are salted, which means if you give two users the same exact password, a different hash will be displayed. When salting is done, you will be unable to perform a rainbow table attack. Instead, you will need to perform a dictionary or brute force attack. You cannot use a rainbow table attack against a hash that has been salted.
Both user's passwords were set to "green" but are different because they were salted. Changes to accounts, such as setting a password, will be logged in the auth.log.

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

    seed@ubuntu:~$ tail /var/log/auth.log

Results will vary, but in some cases, only one or none of the password changes will show up in the log. They are in the log, but tail only provides the last ten entries of the file. Specific information within a file can be extracted by using the grep (global regular expression print) command. The grep command is native to most Linux distributions.

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

    seed@ubuntu:~$ cat /var/log/auth.log | grep changed

14. Install john by typing the following command:

    seed@ubuntu:~$ sudo apt-get install john

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

    seed@ubuntu:~$:john

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

    seed@ubuntu:~$:sudo john /etc/shadow

Notice that even though there were only 3 different passwords in the list, the messages from john indicated that it loaded 4 password hashes with 4 different salts. If you need to view the password hashes and the corresponding revealed passwords at future time, you can always retrieve them from the john.pot file where they are stored.

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

    seed@ubuntu:~$ sudo cat /root/.john/john.pot

Unfortunately, if you attempt to crack the password again, you will not have success.

18. Type the following command to attempt to crack the passwords with john
    seed@ubuntu:~$ sudo john /etc/shadow

This is because hashes and their corresponding passwords are stored within the john.pot file; john will not crack the password hash again. If you want the passwords to be cracked again, you will need to remove the information stored in the john.pot file.

19. Type the following command to remove the existing john.pot file:
    seed@ubuntu:~$ sudo rm /root/.john/john.pot
20. Type the following command to re-crack the passwords with john
    seed@ubuntu:~$sudo john /etc/shadow

The first four passwords cracked were done via brute force. A brute force attack on a password hash usually takes the longest. If a password has a large number of characters and is very complex, the brute force attack can take a very long time. John also gives the user the ability to utilize a password file. It comes with a password file called password.lst, located in the /usr/share/john directory, with 3546 words in its list.

21. To view the first 20 lines of the file, type the following command in the terminal:
    seed@ubuntu:~$ head -n 20 /usr/share/john/password.lst

If any account's passwords are changed, john will go through the cracking process again. We will set chewbaca's password to a word contained within the password.lst file.

22. Set chewbacca's password to **computer** by typing computer twice after typing:
    seed@ubuntu:~$ passwd chewbaca
23. Type the following to run john again and the new password hash will be loaded.
    seed@ubuntu:~$ john /etc/shadow --wordlist=/usr/share/john/password.lst

Since that word was one of the first few in the dictionary, john was able to crack the password in less than one second. Now we will try one of the last passwords in the list.

24. To view the last 20 lines of the file, type the following command in the terminal:
    seed@ubuntu:~$ tail password.lst
25. Set chewbaca's password to **1q2w3e4r** by typing twice after typing:

seed@ubuntu:~$ passwd chewbaca

26. Type the following to run john again and the new password hash will be loaded:
    seed@ubuntu:~$ john /etc/shadow --wordlist=/usr/share/john/password.lst

You can hit Enter during the cracking process to see which word is being tested.

1.2 Conclusion

In Linux, the names of the user accounts are listed in the /etc/passwd file. The hashes for the user's passwords are stored in the shadow file. The password hashes are salted, which means if you give two users the same exact password, a different hash will be displayed for each. When salting is done, you will be unable to perform a rainbow table attack. Instead, you will need to perform a dictionary or brute force attack. John the Ripper is a password cracker that allows an attacker to use brute force or a dictionary file to try to find the password for the hash. All cracked passwords and their corresponding hashes will be stored in the john.pot file. Any account changes are recorded in the auth.log file.