

Ch 6: Crack Linux passwords using John the Ripper

1. Start and login to your Kali Linux virtual machine as user **kali** with a password of **kali**.
2. Type **cd /usr/share/wordlists**, then **ls**. Notice the **rockyou.txt** file. On a fresh Kali Linux machine you might have to unzip the password file using a command such as **sudo gunzip rockyou.txt.gz**, but in the exercise we will use the supplied **rockyou.txt** file.
3. View the contents of the file by typing **cat rockyou.txt**. Press **CTRL+C** to stop the scrolling.
4. Change to your user home directory by typing **cd** and pressing ENTER.
5. Copy the contents of the Linux user account and password file to a single file using the **sudo unshadow /etc/passwd /etc/shadow > credfile.txt**
6. Enter **sudo john -wordlist=/usr/share/wordlists/rockyou.txt credfile.txt** to try to crack password hashes in the Linux **/etc/shadow** file.
7. Enter **sudo john --show credfile.txt**. Notice the passwords for the **kali** user and for account **uone** (created in an earlier exercise) are shown in plaintext.