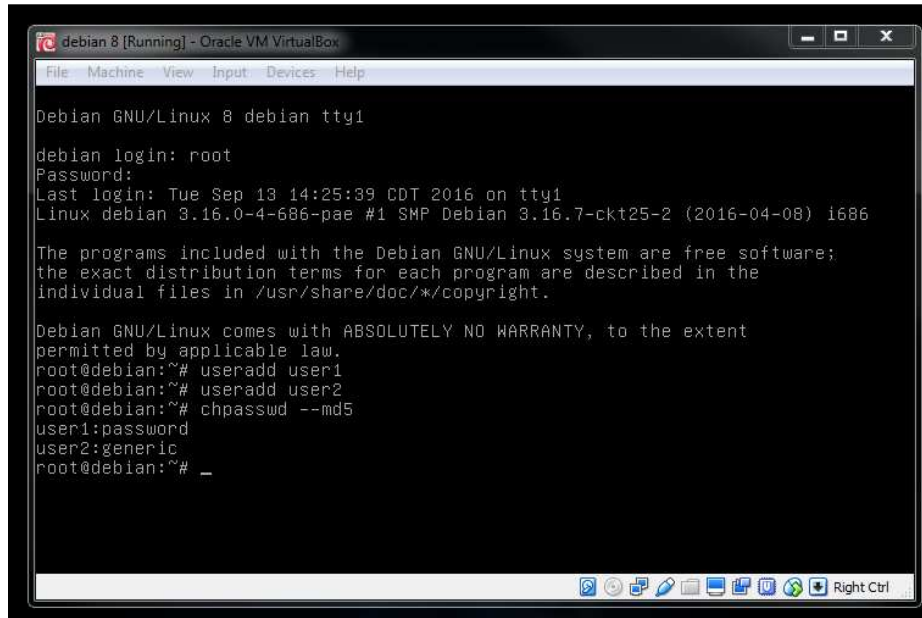


## Process for cracking passwords in Linux (Debian)

First off, we will want to have more easily cracked passwords. To do this, we **can** save our passwords in a less secure encryption standard. By default, Debian stores the passwords in SHA 512 encryption, but we can use the `chpasswd` command to force MD5 encryption. Consider the following:



```
debian 8 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Debian GNU/Linux 8 debian tty1
debian login: root
Password:
Last login: Tue Sep 13 14:25:39 CDT 2016 on tty1
Linux debian 3.16.0-4-686-pae #1 SMP Debian 3.16.7-ckt25-2 (2016-04-08) i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@debian:~# useradd user1
root@debian:~# useradd user2
root@debian:~# chpasswd --md5
user1:password
user2:generic
root@debian:~# _
```

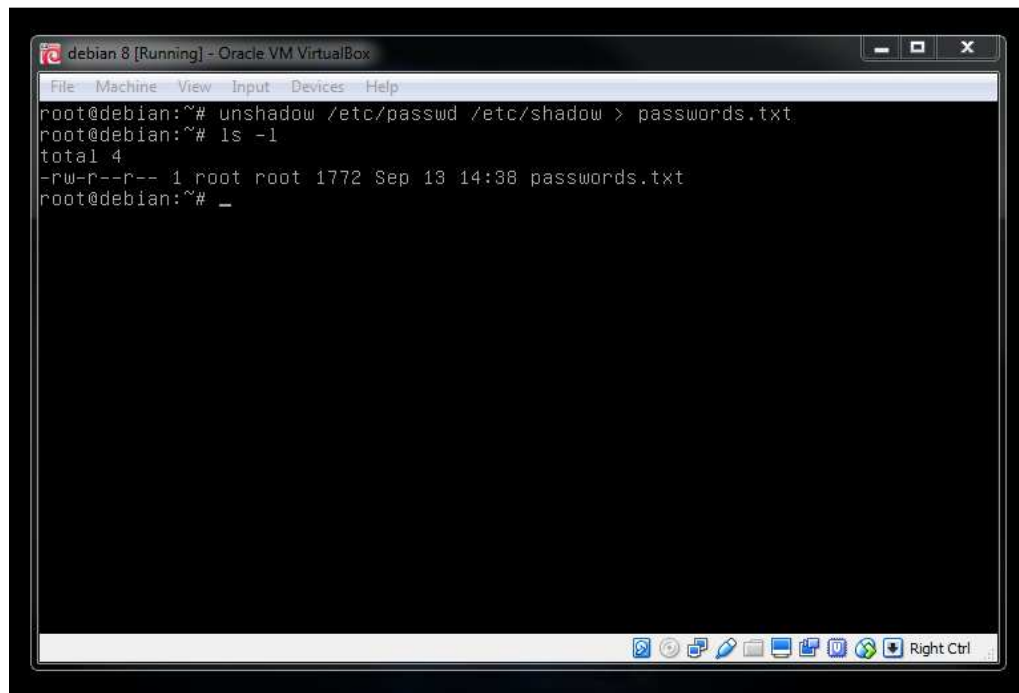
We enter the username password pair separated by a full colon on each line, and commit the changes with a Ctrl + D. Given we are using VirtualBox in this example, you must use the left Ctrl (control key) on your keyboard, as the right Ctrl key is mapped to VirtualBox management.

Also note, we are logged in as root in our example. This is necessary as we are adding users and we will need access to the `/etc/shadow` file, which has file permissions set to only allow root access (basically).

Next we need to install the password cracking utility John the Ripper. You should always do updates to Debian before you install new software, so execute the following commands:

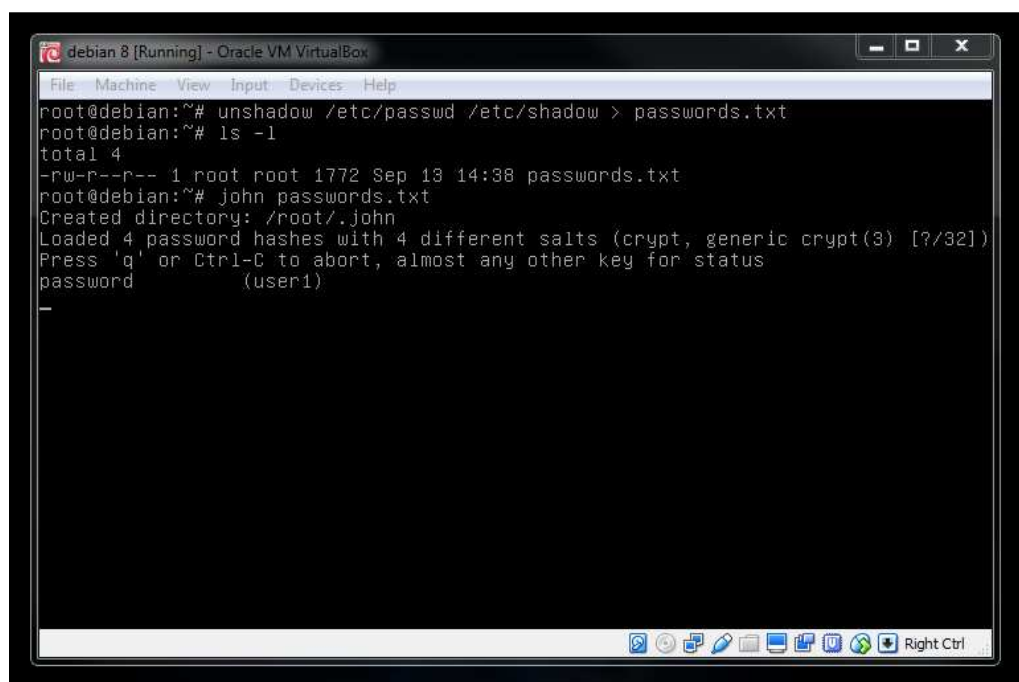
```
apt-get update
apt-get upgrade
apt-get install john
```

Once installed, we need to merge the `/etc/passwd` file (the file with the list of users) with the `/etc/shadow` file (the file that contains the encrypted passwords) into a text file that we can use with John the Ripper. Please note, we will use a utility called `unshadow` to merge these files, and it is installed as part of John the Ripper. Consider:



```
root@debian:~# unshadow /etc/passwd /etc/shadow > passwords.txt
root@debian:~# ls -l
total 4
-rw-r--r-- 1 root root 1772 Sep 13 14:38 passwords.txt
root@debian:~#
```

Now that we have a text file with the username and password pairs set, we need merely use it as an argument to the utility john. Consider:



```
root@debian:~# unshadow /etc/passwd /etc/shadow > passwords.txt
root@debian:~# ls -l
total 4
-rw-r--r-- 1 root root 1772 Sep 13 14:38 passwords.txt
root@debian:~# john passwords.txt
Created directory: /root/.john
Loaded 4 password hashes with 4 different salts (crypt, generic crypt(3) [?/32])
Press 'q' or Ctrl-C to abort, almost any other key for status
password (user1)
-
```

The utility will continue until it cracks all passwords it can, or until you hit Ctrl + C to stop the process. You can restart the process in the future by typing in the command “john passwords.txt” again, without quotes, of course.