.**Henry Bartechko: Week 4 Homework Submission File: Linux Systems Administration**

**Step 1: Ensure/Double Check Permissions on Sensitive Files**

1. Permissions on /etc/shadow should allow only root **read** and **write** access.
   * Command to inspect permissions:
   * **sysadmin@UbuntuDesktop:/etc$ sudo ls -l shadow**
   * **-rw-r----- 1 root shadow 2888 Dec 7 13:58 shadow**
   * Command to set permissions (if needed):
   * **sysadmin@UbuntuDesktop:/etc$ sudo chmod 600 shadow**
   * **-rw------- 1 root shadow 2888 Dec 7 13:58 shadow**
2. Permissions on /etc/gshadow should allow only root **read** and **write** access.
   * Command to inspect permissions:
   * **sysadmin@UbuntuDesktop:/etc$ sudo ls -l gshadow**
   * **-rw-r----- 1 root shadow 1076 Dec 7 13:58 gshadow**
   * Command to set permissions (if needed):
   * **sysadmin@UbuntuDesktop:/etc$ sudo chmod 600 gshadow**
   * **-rw------- 1 root shadow 1076 Dec 7 13:58 gshadow**
3. Permissions on /etc/group should allow root **read** and **write** access, and allow everyone else read access only.
   * Command to inspect permissions:
   * **sysadmin@UbuntuDesktop:/etc$ sudo ls -l group**
   * **-rw-r--r-- 1 root root 1303 Dec 7 13:58 group**
   * Command to set permissions (if needed):
   * **sysadmin@UbuntuDesktop:/etc$ sudo chmod 644 group**
   * **-rw-r--r-- 1 root root 1303 Dec 7 13:58 group**
4. Permissions on /etc/passwd should allow root read and write access, and allow everyone else read access only.
   * Command to inspect permissions:
   * **sysadmin@UbuntuDesktop:/etc$ sudo ls -l passwd**
   * **-rw-r--r-- 1 root root 3214 Dec 7 13:58 passwd**
   * Command to set permissions (if needed):
   * **sysadmin@UbuntuDesktop:/etc$ sudo chmod 644 passwd**
   * **-rw-r--r-- 1 root root 3214 Dec 7 13:58 passwd**

**Step 2: Create User Accounts**

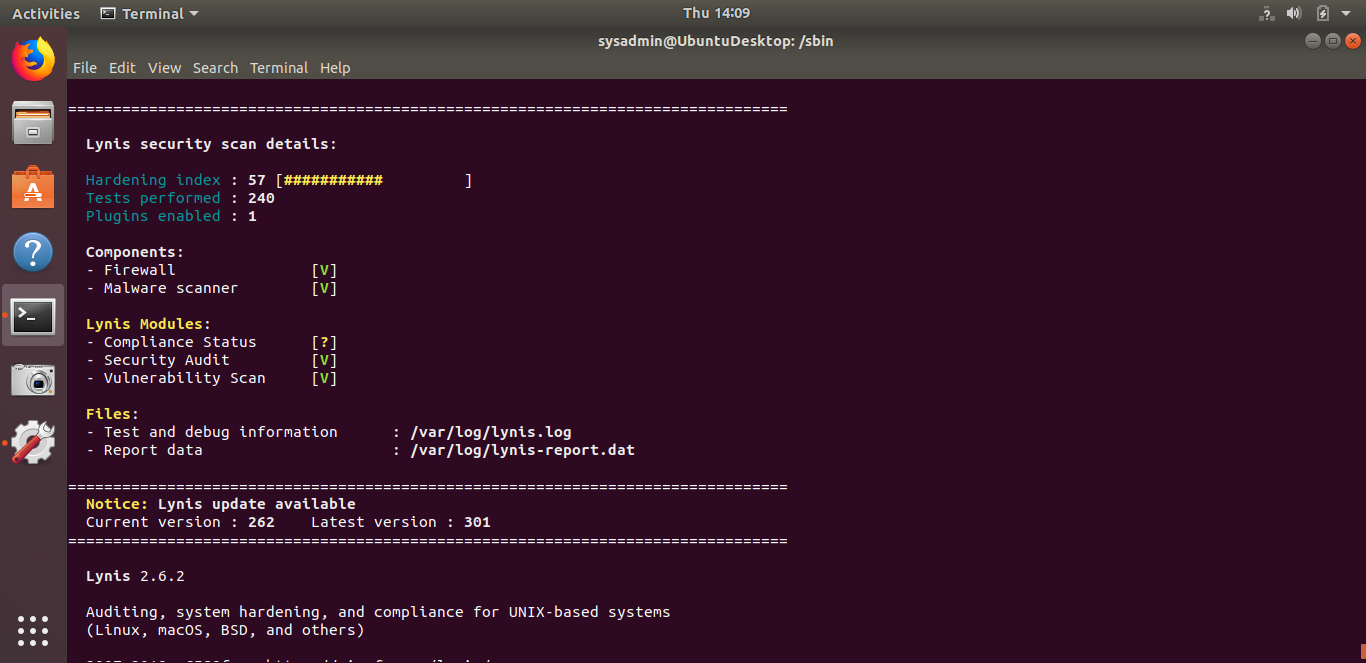
1. Add user accounts for sam, joe, amy, sara, and admin.
   * Command to add each user account (include all five users):
   * **sysadmin@UbuntuDesktop:/$ sudo adduser sam**
   * **sam:x:1012:1014:,,,:/home/sam:/bin/bash**
   * **sysadmin@UbuntuDesktop:/$ sudo adduser joe**
   * **joe:x:1013:1015:,,,:/home/joe:/bin/bash**
   * **sysadmin@UbuntuDesktop:/$ sudo adduser amy**
   * **amy:x:1014:1016:,,,:/home/amy:/bin/bash**
   * **sysadmin@UbuntuDesktop:/$ sudo adduser sara**
   * **sara:x:1015:1017:,,,:/home/sara:/bin/bash**
   * **sysadmin@UbuntuDesktop:/$ sudo adduser admin**
   * **admin:x:1016:1018:,,,:/home/admin:/bin/bash**
2. Ensure that only the admin has general **sudo** access.
   * Command to add admin to the sudo group:
   * **sysadmin@UbuntuDesktop:/$ sudo usermod -aG sudo admin**
   * **sysadmin@UbuntuDesktop:/etc$ sudo visudo**
   * **# Members of the admin group may gain root privileges**
   * **%admin ALL=(ALL) ALL**

**Step 3: Create User Group and Collaborative Folder**

1. Add an engineers group to the system.
   * Command to add group:
   * **sysadmin@UbuntuDesktop:/$ sudo addgroup engineers**
   * **Adding group `engineers' (GID 1019) ...**
   * **Done.**
2. Add users sam, joe, amy, and sara to the managed group.
   * Command to add users to engineers group (**include all four users**):
   * **sysadmin@UbuntuDesktop:/home/engineers$ sudo gpasswd -M sam,joe,amy,sara engineers**
   * **sysadmin@UbuntuDesktop:/etc$ less group**
   * **engineers:x:1019:sam,joe,amy,sara**
3. Create a shared folder for this group at /home/engineers.
   * Command to create the shared folder:
   * **sysadmin@UbuntuDesktop:/home/engineers$ sudo mkdir engineers\_shared\_folder**
   * **sysadmin@UbuntuDesktop:/home/engineers$ ls**
   * **engineers\_shared\_folder**
4. Change ownership on the new **engineers' shared folder** to the engineers group.
   * Command to change ownership of engineer's shared folder to engineer group:
   * **sysadmin@UbuntuDesktop:/home/engineers$ sudo chgrp -R engineers /home/engineers/engineers\_shared\_folder**
   * **sysadmin@UbuntuDesktop:/home/engineers$ ls -l**
   * **total 4**
   * **drwxr-xr-x 2 root engineers 4096 Jan 5 15:34 engineers\_shared\_folder**

**Step 4: Lynis Auditing**

1. Command to install **Lynis**:
   * **qsysadmin@UbuntuDesktop:/sbin$ sudo apt install lynis**
2. Command to see documentation and instructions:
   * **sysadmin@UbuntuDesktop:/sbin$ sudo lynis --help**
3. Command to run an audit:
   * **sysadmin@UbuntuDesktop:/sbin$ sudo lynis audit system**
4. Provide a report from the Lynis output on what can be done to harden the system.
   * Screenshot of report output:



**Bonus**

1. Command to install chkrootkit:
   * **sysadmin@UbuntuDesktop:/sbin$ sudo apt install chkrootkit**
2. Command to see documentation and instructions:
   * **sysadmin@UbuntuDesktop:/sbin$ sudo chkrootkit --help**
3. Command to run expert mode:
   * **sysadmin@UbuntuDesktop:/sbin$ sudo chkrootkit -x**
4. Provide a report from the chrootkit output on what can be done to harden the system.
   * Screenshot of end of sample output:

