### **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: **ls -l shadow**
   * Command to set permissions (if needed): **sudo chmod 600 shadow**
2. Permissions on /etc/gshadow should allow only root read and write access.  
   * Command to inspect permissions: **ls -l gshadow**
   * Command to set permissions (if needed): **sudo chmod 600 gshadow**
3. Permissions on /etc/group should allow root read and write access, and allow everyone else read access only.  
   * Command to inspect permissions: **ls -l group**
   * Command to set permissions (if needed): **sudo chmod 644 group**
4. Permissions on /etc/passwd should allow root read and write access, and allow everyone else read access only.  
   * Command to inspect permissions: **ls -l passwd**
   * Command to set permissions (if needed): **sudo chmod 644 passwd**

### **Step 2: Create User Accounts**

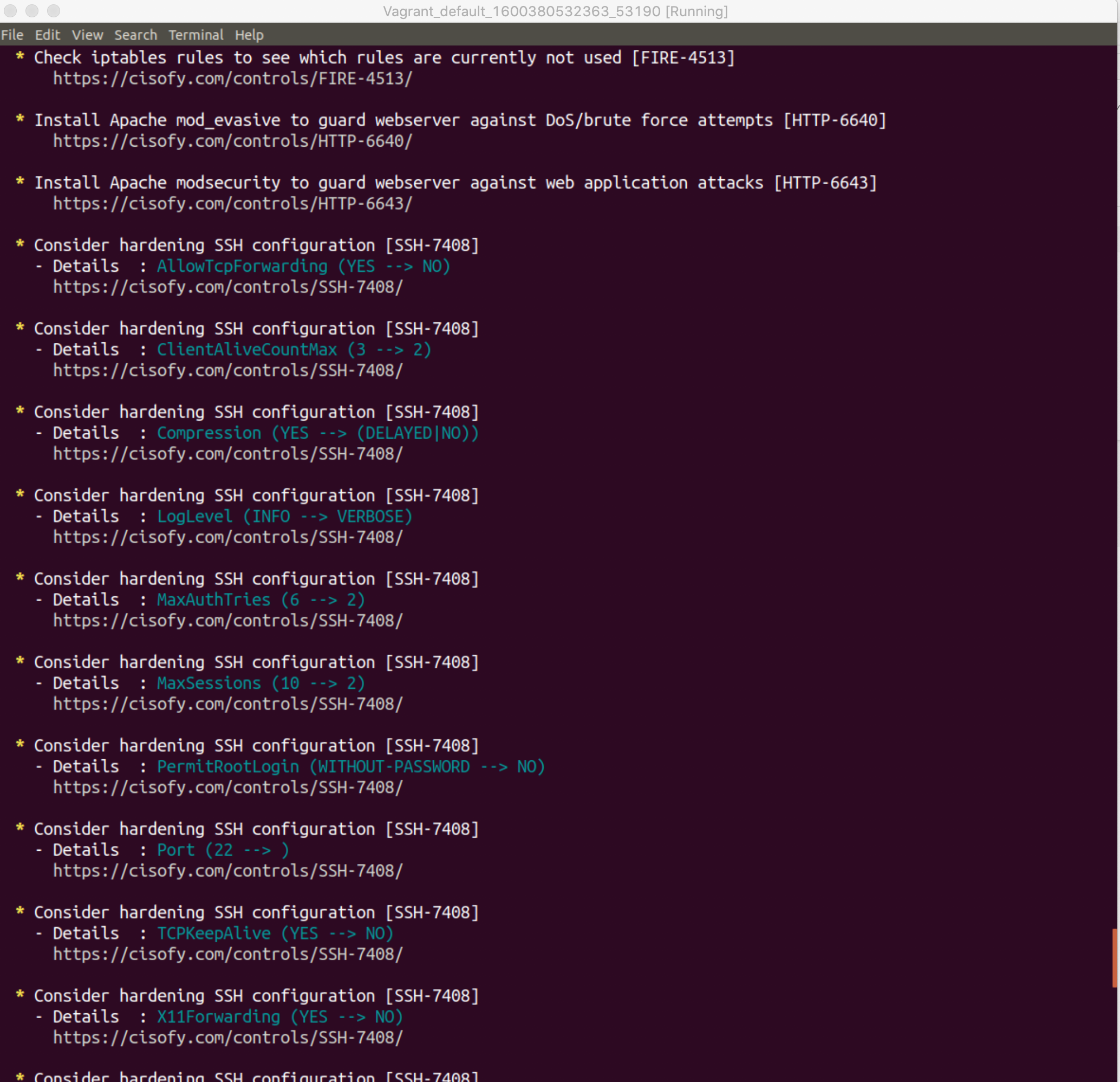
1. Add user accounts for sam, joe, amy, sara, and admin.  
   * Command to add each user account (include all five users):
     1. **Sudo adduser sam --system**
     2. **Sudo adduser joe --system**
     3. **Sudo adduser amy --system**
     4. **Sudo adduser sara --system**
     5. **Sudo adduser admin --system**
2. Force users to create 16-character passwords incorporating numbers and symbols.  
   * Command to edit pwquality.conf file: **sudo nano /etc/security/pwquality.conf**
   * Updates to configuration file:
     1. **Minlen = 16**
     2. **Dcredit = 16**
     3. **Ocredit = 16**
3. Force passwords to expire every 90 days.  
   * Command to to set each new user's password to expire in 90 days (include all five users):
     1. **sudo chage -M 90 sam**
     2. **sudo chage -M 90 joe**
     3. **sudo chage -M 90 amy**
     4. **sudo chage -M 90 sara**
     5. **sudo chage -M 90 admin**
4. Ensure that only the admin has general sudo access.  
   * Command to add admin to the sudo group: **sudo usermod -G sudo admin**

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

1. Add an engineers group to the system.  
   * Command to add group: **sudo addgroup engineers**
2. Add users sam, joe, amy, and sara to the managed group.  
   * Command to add users to engineers group (include all four users):
     1. **Sudo usermod -G engineers sam**
     2. **Sudo usermod -G engineers joe**
     3. **Sudo usermod -G engineers amy**
     4. **Sudo usermod -G engineers sara**
3. Create a shared folder for this group at /home/engineers.  
   * Command to create the shared folder: **mkdir /home/engineers**
4. Change ownership of the new engineers' shared folder to the engineers group.  
   * Command to change ownership of engineer's shared folder to engineer group:
     1. **Sudo chgrp engineers /home/engineers**

### **Step 4: Lynis Auditing**

1. Command to install Lynis: **sudo apt install Lynis**
2. Command to see documentation and instructions: **man Lynis**

1. Command to run an audit: **sudo lynis audit system**
2. 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: **sudo apt install chkrootkit**
2. Command to see documentation and instructions: **man chkrootkit**
3. Command to run expert mode: **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: