

Bash Scripts

Brace expansion command to create the four subdirectories:

```
~$ mkdir -p backups/{freemem,diskuse,openlist,freedisk}
```

- Using brace expansion, create the following four directories:
~/backups/freemem
~/backups/diskuse
~/backups/openlist
~/backups/freedisk
~\$ mkdir -p backups/{freemem,diskuse,openlist,freedisk}

system.sh script edits:

```
#!/bin/bash
```

```
free -h > ~/backups/freemem/free_mem.txt  
du -h > ~/backups/diskuse/disk_usage.txt  
ls -l > ~/backups/openlist/open_list.txt  
df -h > ~/backups/freedisk/free_disk.txt
```

Command to make the system.sh script executable:

```
chmod u+x system.sh
```

Commands to test the script and confirm its execution:

```
sudo ./system.sh
```

(Received the error message that was mentioned in the assignment to ignore.)

I tested the script by do the following:

```
cat backups/freemem/free_mem.txt  
cat backups/diskuse/disk_usage.txt  
cat backups/openlist/open_list.txt  
cat backups/freedisk/free_disk.txt
```

Manage Log File Sizes

- Run `sudo nano /etc/logrotate.conf` to edit the logrotate configuration file.
Configure a log rotation scheme that backs up authentication messages to the `/var/log/auth.log`.

Config file edits:

```
/var/log/auth.log {  
rotate 7  
weekly  
notifempty  
delaycompress  
missingok  
endscript  
}
```

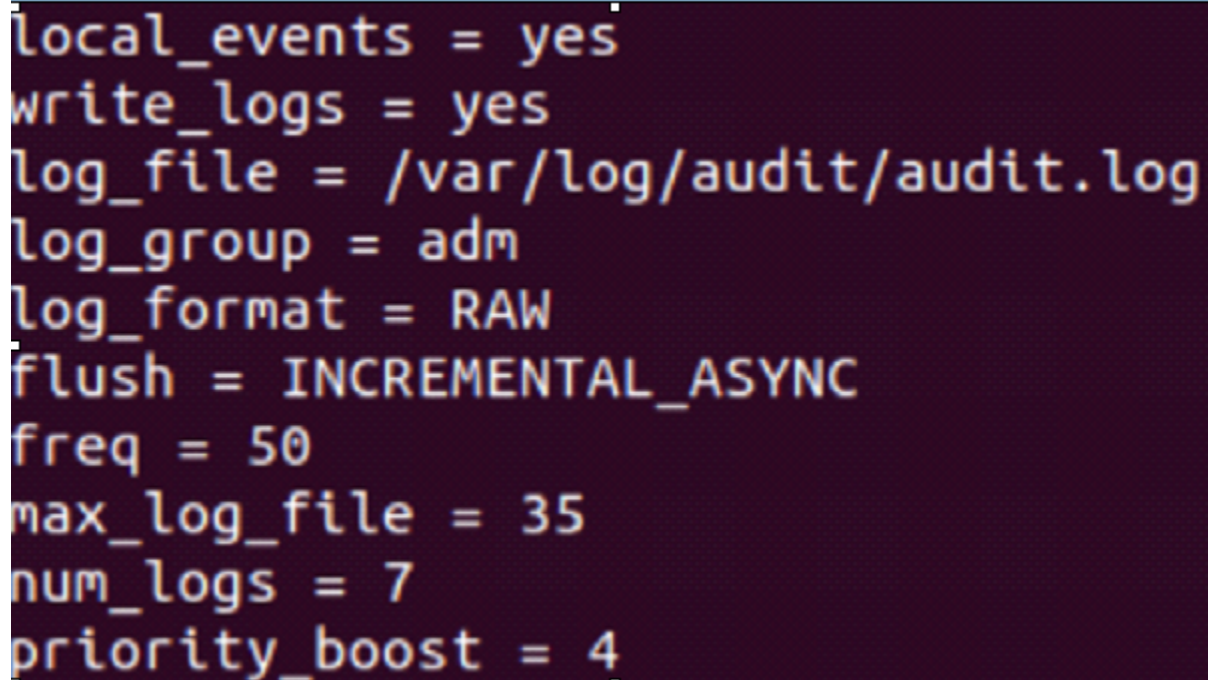
Check for Policy and File Violations

- Command to verify auditd is active: `systemctl`
- Command to set number of retained logs and maximum log file size:
- `sudo nano /etc/audit/auditd.conf`

Edits made to the configuration file

Max_log file = 35

Num_log = 7



```
local_events = yes  
write_logs = yes  
log_file = /var/log/audit/audit.log  
log_group = adm  
log_format = RAW  
flush = INCREMENTAL_ASYNC  
freq = 50  
max_log_file = 35  
num_logs = 7  
priority_boost = 4
```