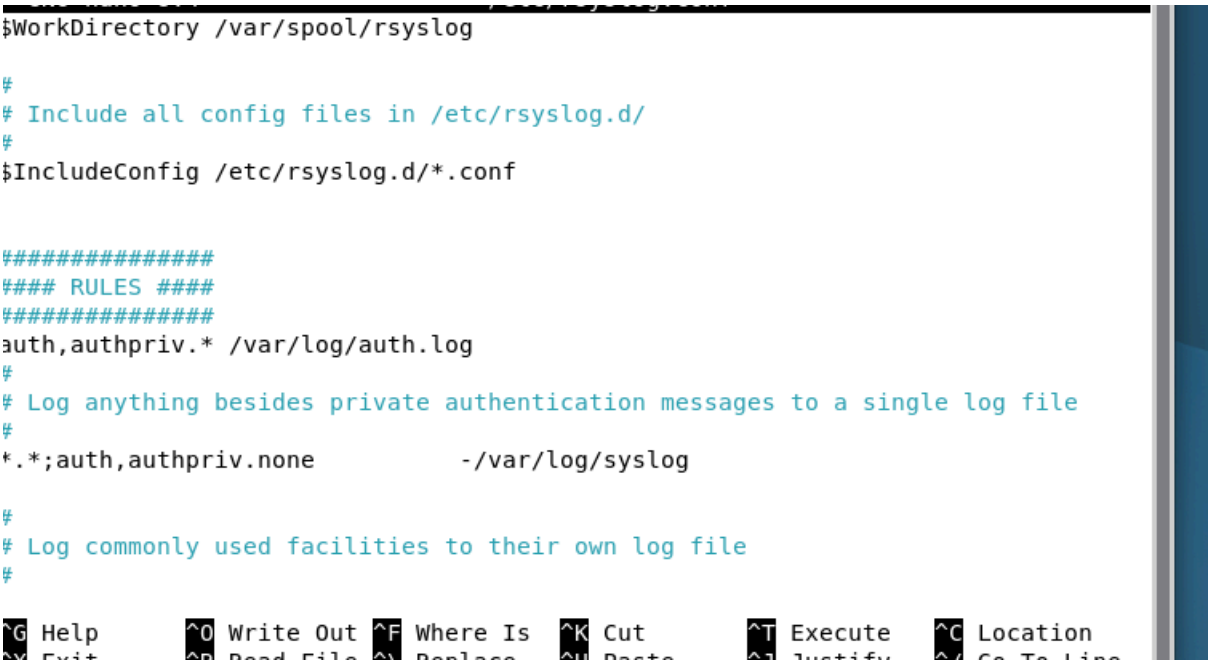
1. Налаштування syslog (rsyslog)

apt update && apt install rsyslog
nano /etc/rsyslog.conf

Рядок для додавання у файл:

auth,authpriv.* /var/log/auth.log



systemctl restart rsyslog

2. Налаштування ротації журналів (Logrotate)

nano /etc/logrotate.d/rsyslog

Блок конфігурації для вставки/редагування:

```
/var/log/auth.log {
    daily
    rotate 7
    missingok
    notifempty
    compress
```

```
    delaycompress
    postrotate
        /usr/lib/rsyslog/rsyslog-rotate
    endscript
}
```

Перевірка:

```
logrotate -d /etc/logrotate.d/rsyslog
```

3. Налаштування аудиту (Auditd)

```
apt install auditd
systemctl enable --now auditd
touch /root/secret_file
auditctl -w /root/secret_file -p rwxa -k secret_file_watch
```

4. Відслідковування системних викликів

```
id -u
auditctl -a always,exit -F arch=b64 -S all -F auid=1000 -k user_trace
auditctl -a always,exit -F arch=b64 -S rmdir -k rmdir_detect
auditctl -l
```

5. Відслідковування процесу MC

```
apt install mc strace
strace -o mc_log.txt -f mc
grep openat mc_log.txt | head -n 10
```

6. Перевірка rmdir та генерація звіту (aureport)

```
mkdir /tmp/test_dir
rmdir /tmp/test_dir
ausearch -k rmdir_detect --raw | aureport --syscall
aureport --syscall
```

Ось покроковий чеклист (список перевірки), щоб переконатися, що **все завдання виконано на 100% правильно**.

Виконуйте команди по черзі та порівнюйте свій результат з тим, що написано в "Очікуваний результат".

---

1. Перевірка Syslog (auth.log) та Logrotate

Команда:

Bash
grep "auth.*var/log/auth.log" /etc/rsyslog.conf && logrotate -d /etc/logrotate.d/rsyslog 2>&1 | grep -A 2 "/var/log/auth.log"

Очікуваний результат:

1. Має вивести рядок конфігурації (наприклад: `auth,authpriv.* /var/log/auth.log`).
2. Має вивести параметри ротації: `rotate 7` (або `7 rotations`) та `daily` (або `after 1 days`).
    - *Якщо ви це бачите — частина з логами зарахована.*

---

2. Перевірка правил аудиту (Auditd)

Команда:

Bash
auditctl -l

Очікуваний результат: Ви повинні побачити **три** правила (порядок може відрізнятися):

1. `-w /root/secret_file -p rwxa -k my_file_watch` (Стеження за файлом).
2. `-a always,exit ... -F auid=1000 ... -k user_trace` (Стеження за вашим користувачем, UID має бути 1000).
3. `-a always,exit ... -S rmdir ... -k rmdir_detect` (Стеження за командою rmdir).
    - *Якщо всі три є — частина з правилами зарахована.*

---

3. Перевірка "бойової" роботи аудиту (rmdir)

Ми зараз створимо і видалимо папку, а потім перевіримо, чи це записалося в звіт.

Команди (виконувати одну за одною):

Bash
mkdir /tmp/test_audit
rmdir /tmp/test_audit
ausearch -k rmdir_detect --raw | aureport --syscall --summary

Очікуваний результат: Вивід останньої команди має показати табличку, де буде згадано `rmdir`. Наприклад:

Plaintext
Syscall Summary Report
==========
Total Syscall
==========
1   rmdir

- *Якщо rmdir з'явився у звіті — система аудиту працює правильно.*

---

4. Перевірка трасування процесу mc

Вам потрібно переконатися, що файл логу створений і містить дані про системні виклики.

Команда:

Bash
head -n 5 mc_log.txt

(Якщо ви ще не робили цього кроку, виконайте: `strace -o mc_log.txt -f mc`, вийдіть з mc (F10), а потім перевірте).

Очікуваний результат: Ви побачите список системних викликів, наприклад:

Plaintext
execve("/usr/bin/mc", ["mc"], 0x7ffd...) = 0
brk(NULL)   = 0x55...
access("/etc/ld.so.preload", R_OK)   = -1 ENOENT

- *Якщо бачите подібний текст — трасування виконано успішно.*

Якщо всі 4 пункти дали очікуваний результат — вітаю, лабораторна робота виконана ідеально! Чи потрібна допомога з аналізом виводу `mc` (які файли він відкривав)?