Управление журналами событий в системе

Майоров Дмитрий Андреевич

Содержание i

1. Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе

2. Выполнение лабораторной работы

Открываем три терминала и в каждом получаем полномочия администратора

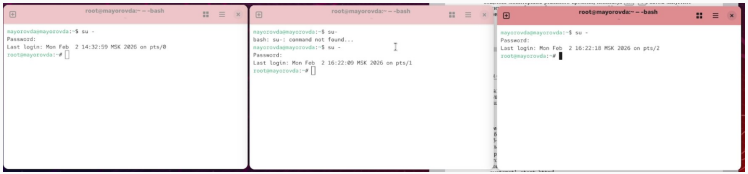

Рисунок 1

3. Выполнение лабораторной работы

На второй вкладке терминала запусткаем мониторинг системных событий в реальном времени

```
root@mayorovda:~# tail -f /var/log/messages
Feb  2 16:22:28 mayorovda kernel: traps: VBoxClient[11237] trap int3 ip:4
1dc5b sp:7feb26c35cd0 error:0 in VBoxClient[1dc5b,400000+bb000]
Feb  2 16:22:28 mayorovda systemd-coredump[11238]: Process 11234 (VBoxCli
ent) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Feb  2 16:22:28 mayorovda systemd[1]: Started systemd-coredump@645-11238-
0.service - Process Core Dump (PID 11238/UID 0).
Feb  2 16:22:29 mayorovda systemd-coredump[11239]: Process 11234 (VBoxCli
```

Рисунок 2

4. Выполнение лабораторной работы

В третьей вкладке терминала возвращаемся к учётной записи своего пользователя и пробуем получить полномочия администратора, но вводим неправильный пароль. Во второй вкладке терминала с мониторингом событий или ничего не отображается сообщение об ошибке

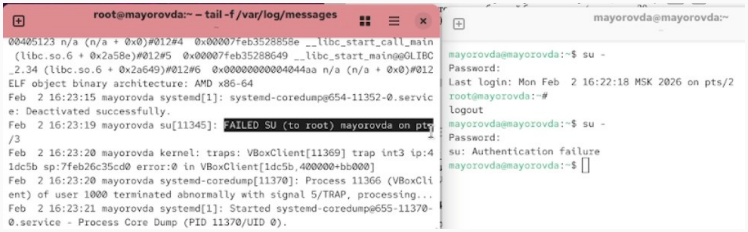

Рисунок 3

5. Выполнение лабораторной работы

В третьей вкладке терминала из оболочки пользователя вводим logger hello. Во второй вкладке терминала с мониторингом событий видим это же сообщение

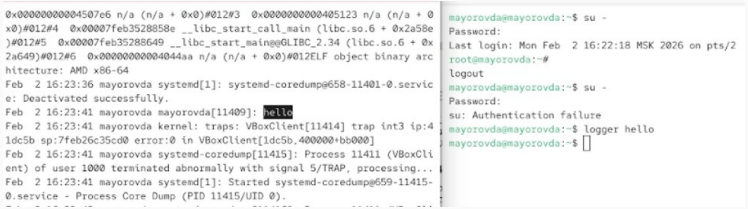

Рисунок 4

6. Выполнение лабораторной работы

Во второй вкладке терминала запускаем мониторинг сообщений безопасности

```
root@mayorovda:~# tail -n 20 /var/log/secure
Feb  2 14:32:21 mayorovda gdm-launch-environment][1418]: pam_unix(gdm
nch-environment:session): session closed for user gdm
```

Рисунок 5

7. Выполнение лабораторной работы

В первой вкладке терминала устанавливаем Apache

Рисунок 6

8. Выполнение лабораторной работы

Запускаем веб-службу

```
root@mayorovda:~# systemctl start httpd
root@mayorovda:~# systemctl enable httpd
Created symlink '/etc/systemd/system/multi-user.target.wants/httpd.servic
e' → '/usr/lib/systemd/system/httpd.service'.
```

Рисунок 7

9. Выполнение лабораторной работы

Во второй вкладке терминала смотрим журнал сообщений об ошибках веб-службы

Рисунок 8

10. Выполнение лабораторной работы

Открываем файл /etc/httpd/conf/httpd.conf для редактирования и вводим в конце следующую строку

Рисунок 9

11. Выполнение лабораторной работы

В каталоге /etc/rsyslog.d создаем файл мониторинга событий веб-службы

Рисунок 10

Открываем его для редактирования и прописываем там следующую строку

Рисунок 11

13. Выполнение лабораторной работы

В первой вкладке терминала перезагрузжаем конфигурацию rsyslogd и веб-службу

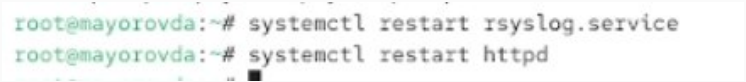

Рисунок 12

14. Выполнение лабораторной работы

В третьей вкладке терминала создаем отдельный файл конфигурации для мониторинга отладочной информации и вводим туда нужную команду

Рисунок 13

первой вкладке терминала снова перезапускаем rsyslogd

Рисунок 14

16. Выполнение лабораторной работы

Во второй вкладке терминала запускаем мониторинг отладочной информации, а в третьей вкладке терминала вводим следующую команду. В терминале с мониторингом смотрим сообщение отладки

```
root@mayorovda:~# tail -f /var/log/messages-debug
```

Рисунок 15

```
root@mayorovda:/etc/rsyslog.d# logger -p daemon.debug "Daemon Debug Messa
ge"
```

Рисунок 16

17. Выполнение лабораторной работы

Во второй вкладке терминала смотрим содержимое журнала с событиями с момента последнего запуска системы

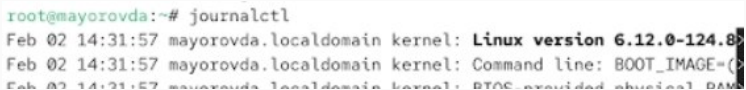

Рисунок 17

18. Выполнение лабораторной работы

Смотрим содержимое журнала без пейджера

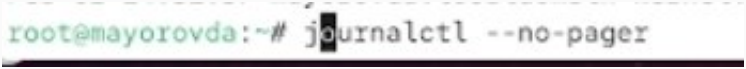

Рисунок 18

19. Выполнение лабораторной работы

Смотрим журнал в реальном времени

Рисунок 19

20. Выполнение лабораторной работы

Смотрим последние 20 строк журнала, сообщения об ошибках, все сообщения со вчерашнего дня, детальную информацию и доп. информацию о модуле sshd

Рисунок 20

Рисунок 21

21. Выполнение лабораторной работы

Создаем каталог для хранения записей журнала. Корректируем права доступа для каталога /var/log/journal, чтобы journald смог записывать в него информацию. Используем команду для принятия изменений. Смотрим сообщения журнала с момента перезагрузки

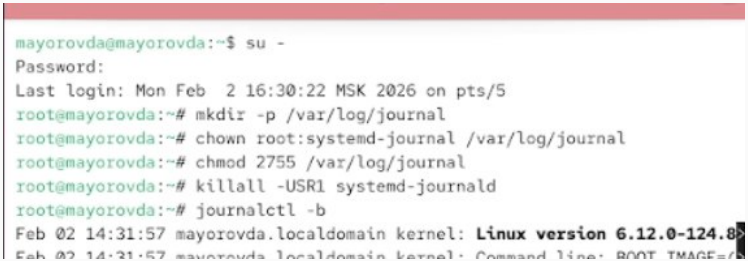

Рисунок 22

22. Выводы

Получены навыки работы с журналами мониторинга различных событий в системе