

Введение в аудит

Чтобы контролировать процессы, проводить аудит операционной системы и расследовать инциденты в ОС Linux, используют утилиту **audit**.

Для установки user-space сервиса воспользуемся командой:

```
sudo apt install auditd
```

При работе с аудитом у нас есть несколько основных компонентов, с которыми мы будем взаимодействовать:

- `/etc/audit/auditd.conf` — файл конфигурации демона, настраивает то, *как* будет происходить логирование;
- `/etc/audit/audit.rules` — файл конфигурации аудита, настраивает то, *что* будет логироваться;
- `/var/log/audit/audit.log` — файл логов, куда собирается вся информация.

При установке демона `auditd`, он автоматически запускается, однако его всегда можно запустить/перезапустить/остановить командой:

```
sudo systemctl start/restart/stop auditd
```

```
(user@kali)-[/]  
└─$ systemctl status auditd  
● auditd.service - Security Auditing Service  
   Loaded: loaded (/usr/lib/systemd/system/auditd.service; disabled; preset: disabled)  
   Active: active (running) since Sat 2024-02-10 19:50:45 MSK; 1min 37s ago  
     Docs: man:auditd(8)  
           https://github.com/linux-audit/audit-documentation  
   Process: 12299 ExecStart=/sbin/auditd (code=exited, status=0/SUCCESS)  
   Process: 12305 ExecStartPost=/sbin/augenrules --load (code=exited, status=0/SUCCESS)  
   Main PID: 12301 (auditd)  
    Tasks: 2 (limit: 8084)  
   Memory: 668.0K (peak: 2.3M)  
      CPU: 62ms  
   CGroup: /system.slice/auditd.service  
           └─12301 /sbin/auditd  
  
фев 10 19:50:45 kali augenrules[12318]: enabled 1  
фев 10 19:50:45 kali augenrules[12318]: failure 1  
фев 10 19:50:45 kali augenrules[12318]: pid 12301  
фев 10 19:50:45 kali augenrules[12318]: rate_limit 0  
фев 10 19:50:45 kali augenrules[12318]: backlog_limit 8192  
фев 10 19:50:45 kali augenrules[12318]: lost 0  
фев 10 19:50:45 kali augenrules[12318]: backlog 4  
фев 10 19:50:45 kali augenrules[12318]: backlog_wait_time 60000  
фев 10 19:50:45 kali augenrules[12318]: backlog_wait_time_actual 0  
фев 10 19:50:45 kali systemd[1]: Started auditd.service - Security Auditing Service.  
lines 1-24...skipping...
```

Чтобы управлять аудитом, используют команду **auditctl**. Она и позволяет добавлять новые параметры и правила в `audit.rules`.

Откроем файл конфигурации аудита командой:

```
sudo nano /etc/audit/audit.rules
```

```
GNU nano 7.2 /etc/audit/audit.rules  
## This file is automatically generated from /etc/audit/rules.d  
-D  
-b 8192  
-f 1  
--backlog_wait_time 60000
```

Включаем аудит и сразу увеличиваем буфер логов до 500:

```
auditctl -e 1
```

```
auditctl -b 500
```

Поставим мониторинг на директорию /etc/passwd так, чтобы при любом изменении атрибутов, чтении, записи или исполнении файлов в этой директории, мы получали об этом информацию. Опцией -k мы задаем как бы лейбл для данного действия, чтобы потом в логах смогли быстро его найти:

```
auditctl -w /etc/passwd -p rwax -k act_passwd
```

```
(user@kali)-[/]
$ sudo auditctl -e 1
enabled 1
failure 1
pid 12301
rate_limit 0
backlog_limit 8192
lost 0
backlog 0
backlog_wait_time 60000
backlog_wait_time_actual 0

- w      Мониторить файл/директорию
- f      Действие на невозможность обработ
максимальная важность
- k      Фильтр ключевых слов

(user@kali)-[/]
$ sudo auditctl -b 500
enabled 1
failure 1
pid 12301
rate_limit 0
backlog_limit 500
lost 0
backlog 0
backlog_wait_time 60000
backlog_wait_time_actual 0

На примерах станет попроще, обещаем.
Например, включаем аудит и сразу увеличиваем бу
auditctl -e 1
auditctl -b 500

Начинаем расписывать правила:
auditctl -w /etc/passwd -p rwax -k act_passwd
Мониторинг на директорию /etc/passwd та
```

В качестве примера посмотрим содержимое файла командой:

```
cat /etc/passwd
```

```
(user@kali)-[/]
$ cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
```

Команда **ausearch** — один из способов быстрого просмотра логов. Вводим:

```
ausearch -k act_passwd
```

```
time->Sat Feb 10 20:04:53 2024
type=PROCTITLE msg=audit(1707584693.643:274): proctitle=7375646F0061757376561726368002D6B006163745F706173737764
type=PATH msg=audit(1707584693.643:274): item=0 name="/etc/passwd" inode=22806849 dev=08:02 mode=0100644 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1707584693.643:274): cwd="/"
type=SYSCALL msg=audit(1707584693.643:274): arch=c000003e syscall=257 success=yes exit=13 a0=ffffff9c a1=7fb283becf9 a2=80000 a3=0 items=1 ppid=4302 pid=13013 auid=1000 uid=1000 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=2 comm="sudo" exe="/usr/bin/sudo" subj=unconfined key="act_passwd"
```