### Задание 20.2.2 (HW-03)

**Персонализация:** Михайлов Юрий Никитич (uramihajlov481@gmail.com)

**Лабораторная работа:** Задание**№**22.2.2 (HW-03)**:**

Общая информация:

* Период тестирования: 03.04.2024
* Задание: Логи

**Описание действий:  
  
1) Настройка конфигурации audit: -** Прежде всего, добавим в audit.rules правила для логирования изменений файлов в указанных директориях:  
  
**-w /etc -p wa**

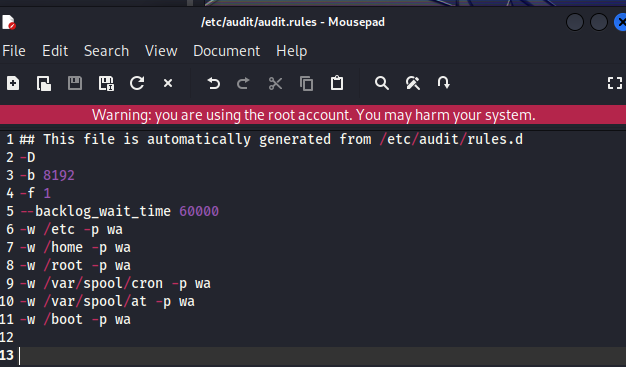
**-w /home -p wa**

**-w /root -p wa**

**-w /var/spool/cron -p wa**

**-w /var/spool/at -p wa**

**-w /boot -p wa**

****

**Эти строки означают следующее:**

* **-w** указывает на мониторинг файлов или директорий.
* **/путь/к/директории** указывает на директорию, изменения в которой мы хотим отслеживать.
* **-p wa** задает права доступа к файлам, которые мы хотим отслеживать: **w** для записи и **a** для атрибутов.

**2)**Теперь добавим правила для логирования syscall **execve** и **execveat**, исключив **/lib/systemd/systemd-logind**:

* **-a always,exit -F arch=b64 -S execve,execveat -F path!=/lib/systemd/systemd-logind**
* **-a always,exit -F arch=b32 -S execve,execveat -F path!=/lib/systemd/systemd-logind**

**Эти строки указывают следующее:**

* -a always,exit указывает на аудит каждого syscall, который завершается.
* -F arch=b64 и -F arch=b32 определяют архитектуру процессора (64 или 32 бита).
* -S execve,execveat указывает на аудит syscall'ов execve и execveat.
* -F path!=/lib/systemd/systemd-logind исключает указанный путь из аудита.

**3) Теперь чтоб после перезагрузки «sudo systemctl restart auditd» конфиг не вернулся в исходно состояние создадим файл «Сustom.rules» в /etc/audit/rules.d/**

**Внутрь команды:**

**-w /etc -p wa**

**-w /home -p wa**

**-w /root -p wa**

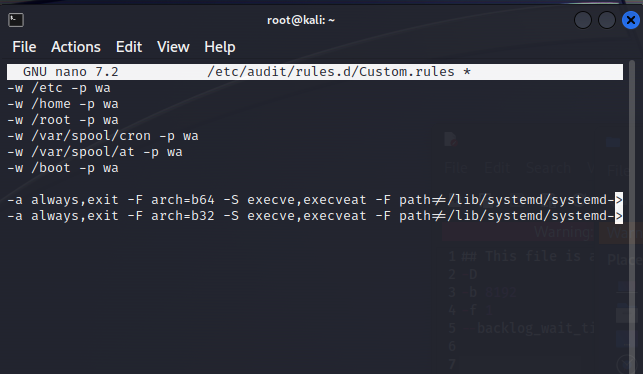
**-w /var/spool/cron -p wa**

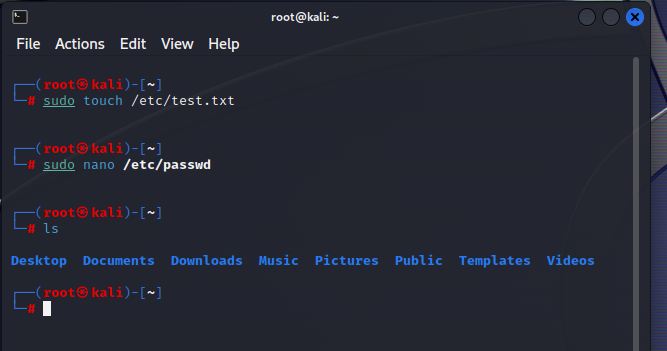
**-w /var/spool/at -p wa**

**-w /boot -p wa**

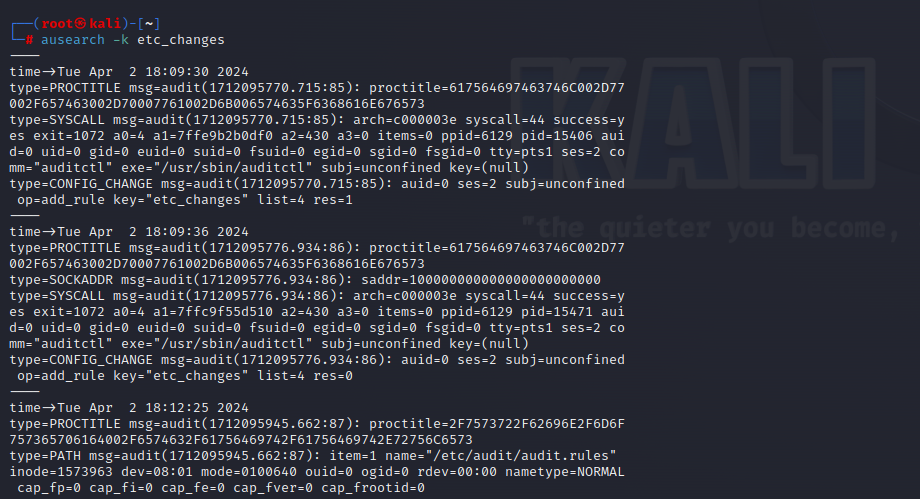
**-a always,exit -F arch=b64 -S execve,execveat -F path!=/lib/systemd/systemd-logind**

**-a always,exit -F arch=b32 -S execve,execveat -F path!=/lib/systemd/systemd-logind**



**4) Добавим изменений чтоб проверить работает ли  
  
**

**5) Видим что всё работает**

****