



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«МИРЭА–Российский технологический университет»

РТУ МИРЭА

Колледж программирования и кибербезопасности

Отчет о выполнении практического задания
по дисциплине «МДК.01.04 Эксплуатация автоматизированных
(информационных) систем в защищенном исполнении»
на тему «Настройка системы для задач аудита»

Практическое задание № 14

Специальность – 10.05.02 Информационная безопасность
автоматизированных систем

Выполнил студент:

_____ Маркаров М.О.

Группа: ИБ-32

Руководитель:

_____ Герасин В.Ю.

Работа защищена с оценкой _____

Дата защиты _____

Москва

2025

Практическая работа № 14

Тема: Настройка системы для задач аудита

Цель: Научиться настраивать и проводить аудит безопасности на операционных системах Windows и Linux, а также ознакомить студентов с базовыми инструментами и методами аудита.

Ход работы:

```
(root@kali)-[~/home/kali]
└─# sudo apt install auditd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libssl-dev libtirpc-dev
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  cryptsetup cryptsetup-bin cryptsetup-initramfs cryptsetup-nuke-password libaudit-common libaudit1 libaparse0t64 libc-bin libc-dev-bin lib
  libc-l10n libc6 libc6-dev libc6-i386 libcryptsetup12 libnss-systemd libpam-systemd libssl3t64 libsystemd libsystemd0 libudev1 lib
  linux-sysctl-defaults locales openssl openssl-provider-legacy systemd systemd-cryptsetup systemd-dev systemd-sysv udev
Suggested packages:
  audispd-plugins glibc-doc libnss-nis libnss-nisplus libtss2-rc0t64 libarchive13t64 libbdw1t64 libelf1t64 systemd-container systemd-homed
  systemd-boot systemd-resolved systemd-repart
The following packages will be REMOVED:
  libssl3
The following NEW packages will be installed:
  auditd libaparse0t64 libssl3t64 linux-sysctl-defaults openssl-provider-legacy systemd-cryptsetup
The following packages will be upgraded:
  cryptsetup cryptsetup-bin cryptsetup-initramfs cryptsetup-nuke-password libaudit-common libaudit1 libc-bin libc-dev-bin libc-devtools lib
  libc6-dev libc6-i386 libcryptsetup12 libnss-systemd libpam-systemd libsystemd libsystemd0 libudev1 linux-base locales openssl syst
  systemd-dev systemd-sysv udev
26 upgraded, 6 newly installed, 1 to remove and 2063 not upgraded.
Need to get 12.4 MB/26.1 MB of archives.
After this operation, 4,876 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 openssl amd64 3.4.1-1 [1,427 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 openssl-provider-legacy amd64 3.4.1-1 [302 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 libssl3t64 amd64 3.4.1-1 [2,304 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 libsystemd0 amd64 257.2-3 [450 kB]
Get:7 http://kali.download/kali kali-rolling/main amd64 libnss-systemd amd64 257.2-3 [215 kB]
Get:8 http://kali.download/kali kali-rolling/main amd64 systemd-dev all 257.2-3 [70.9 kB]
Get:9 http://kali.download/kali kali-rolling/main amd64 libpam-systemd amd64 257.2-3 [293 kB]
Get:11 http://kali.download/kali kali-rolling/main amd64 systemd-sysv amd64 257.2-3 [61.1 kB]
Get:13 http://http.kali.org/kali kali-rolling/main amd64 auditd amd64 1:4.0.2-2+b2 [217 kB]
Get:15 http://kali.download/kali kali-rolling/main amd64 libudev1 amd64 257.2-3 [149 kB]
Get:16 http://kali.download/kali kali-rolling/main amd64 linux-sysctl-defaults all 4.11 [5,244 B]
Get:17 http://kali.download/kali kali-rolling/main amd64 linux-base all 4.11 [31.2 kB]
Get:18 http://kali.download/kali kali-rolling/main amd64 systemd-cryptsetup amd64 257.2-3 [169 kB]
Get:4 http://mirror.amuksa.com/kali kali-rolling/main amd64 libsystemd-shared amd64 257.2-3 [2,139 kB]
Get:5 http://mirror.amuksa.com/kali kali-rolling/main amd64 systemd amd64 257.2-3 [3,094 kB]
Get:10 http://http.kali.org/kali kali-rolling/main amd64 libaudit1 amd64 1:4.0.2-2+b2 [55.1 kB]
Get:12 http://http.kali.org/kali kali-rolling/main amd64 libaparse0t64 amd64 1:4.0.2-2+b2 [68.6 kB]
Get:14 http://mirror.amuksa.com/kali kali-rolling/main amd64 udev amd64 257.2-3 [1,360 kB]
Fetched 12.4 MB in 19s (639 kB/s)
Extracting templates from packages: 100%
Preconfiguring packages ...
(Reading database ... 399423 files and directories currently installed.)
Preparing to unpack .../libc-l10n_2.40-3_all.deb ...
Unpacking libc-l10n (2.40-3) over (2.37-12) ...
Preparing to unpack .../openssl_3.4.1-1_amd64.deb ...
Unpacking openssl (3.4.1-1) over (3.0.11-1) ...
Preparing to unpack .../libcryptsetup12_2%3a2.7.5-1_amd64.deb ...
Unpacking libcryptsetup12:amd64 (2:2.7.5-1) over (2:2.6.1-5) ...
dpkg: libssl3:amd64: dependency problems, but removing anyway as you requested:
  wpasupplicant depends on libssl3 (>= 3.0.0).
  vboot-utils depends on libssl3 (>= 3.0.0).
```

Рис. 1 Устанавливаем пакет apt install auditd

На (рис. 1) демонстрируется установка пакета auditd где наглядна показана команда и сам процесс установки.

```
in apt-key(8) for details.

└─[root@kali]─[/home/kali]
# sudo systemctl start auditd
└─[root@kali]─[/home/kali]
# sudo systemctl enable auditd

Synchronizing state of auditd.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable auditd
Created symlink '/etc/systemd/system/multi-user.target.wants/auditd.service' → '/usr/lib/systemd/system/auditd.service'.

└─[root@kali]─[/home/kali]
# sudo systemctl status auditd

● auditd.service - Security Audit Logging Service
    Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; preset: disabled)
    Active: active (running) since Tue 2025-03-04 10:58:59 EST; 1min 56s ago
      Invocation: 381d508f10d34825903f002c6a81ec5f
        Docs: man:auditd(8)
               https://github.com/linux-audit/audit-documentation
     Main PID: 54317 (auditd)
       Tasks: 2 (limit: 9429)
      Memory: 664K (peak: 1.6M)
        CPU: 13ms
       CGroup: /system.slice/auditd.service
                 └─54317 /usr/sbin/auditd

Mar 04 10:58:59 kali systemd[1]: Starting auditd.service - Security Audit Logging Service ...
Mar 04 10:58:59 kali auditd[54317]: No plugins found, not dispatching events
Mar 04 10:58:59 kali systemd[1]: Started auditd.service - Security Audit Logging Service.
Mar 04 10:58:59 kali auditd[54317]: Init complete, auditd 4.0.2 listening for events (startup state enable)
```

Рис. 2 Процесс включения запуска и включения пакета auditd

На (рис. 2) демонстрируется процесс включения через команду sudo systemctl start auditd и после этого включения пакета sudo systemctl enable auditd. После ввода команды необходимо было проверить на работоспособность пакета прописав команду sudo systemctl status auditd.

Вывод: в результате практической работы мы применяли ряд команд для того чтобы обновить дескриптор kali Linux для того чтобы подключиться к репозиторию который позволяет отслеживать изменения в файловой системе и действия пользователей.