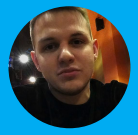
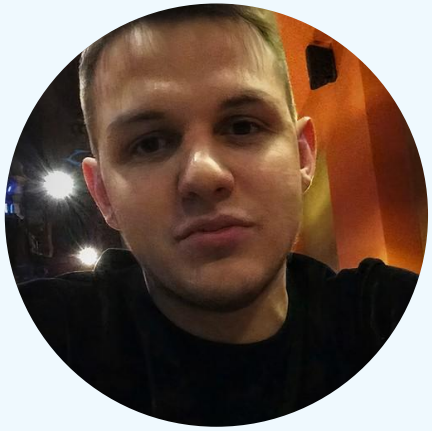
нетология

Linux Hardening



Антон
Лукашов



Антон Лукашов

Аналитик по информационной безопасности

в Совкомбанк

План занятия

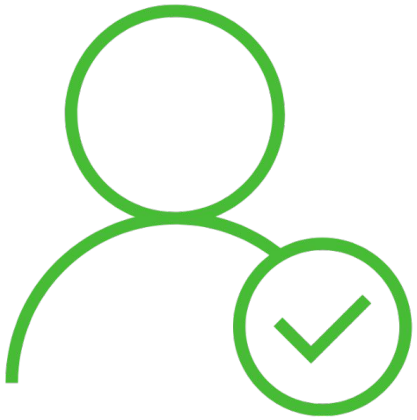
1. Пользователи и группы
2. Правы доступа
3. PAM
4. Шифрование
5. Система логирования
6. Итоги
7. Домашнее задание

Пользователи и группы

root

root (superuser, суперпользователь) – обязательный пользователь во всех Linux.

➡ Root может прочитать, удалить или изменить любой файл (следовательно и всё) в системе.



root

Для root:

- UID= 0;
- GUID= 0;
- домашний каталог = /root;

В некоторых дистрибутивах (Ubuntu) пользователю root запрещен вход в систему.

sudo

sudo – временное повышение прав текущего пользователя до root.

/etc/sudoers – список пользователей или групп, которым разрешено использовать sudo.

sudo

Для «безопасног о» ре дактирования нужно испо льзовать:

```
user@user:~$ sudo visudo
```

Если файл повре жден:

```
user@user:~$ pkexec nano /et c/sudoers
```

/etc/sudoers

Разделы #Host alias #User alias #Cmnd alias позволяют создать списки хостов, пользователей или команд, например:

Students_Alias STUD = student1, student2

Раздел команд:

- root ALL=(ALL:ALL)ALL – root может запускать любую команду в любой группе на любом хосте;
- %admin ALL=(ALL)ALL – аналогично для группы admin.

/etc/passwd

/etc/passwd – файл, содержащий список пользователей системы

```
user@user-VirtualBox:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
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
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
```

Пользователь : пароль : UID: GUID: полное_имя : каталог : оболочка

/etc/shadow

/etc/shadow – файл, содержащий список паролей пользователей.

```
user@user-VirtualBox:~$ sudo cat /etc/shadow
[sudo] password for user:
root:!:18365:0:99999:7:::
daemon:*:18295:0:99999:7:::
bin:*:18295:0:99999:7:::
sys:*:18295:0:99999:7:::
sync:*:18295:0:99999:7:::
games:*:18295:0:99999:7:::
man:*:18295:0:99999:7:::
lp:*:18295:0:99999:7:::
mail:*:18295:0:99999:7:::
news:*:18295:0:99999:7:::
uucp:*:18295:0:99999:7:::
proxy:*:18295:0:99999:7:::
www-data:*:18295:0:99999:7:::
backup:*:18295:0:99999:7:::
list:*:18295:0:99999:7:::
irc:*:18295:0:99999:7:::
gnats:*:18295:0:99999:7:::
```

Пользователь : пароль : дата : мин : макс ::::

/etc/group

/etc/group – файл, содержащий список групп пользователей.

```
user@user-VirtualBox:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,user
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
```

Группа : пароль : GID: список

login.defs

/etc/login.defs – файл, содер жащий параметры вх ода по умо лчанию.

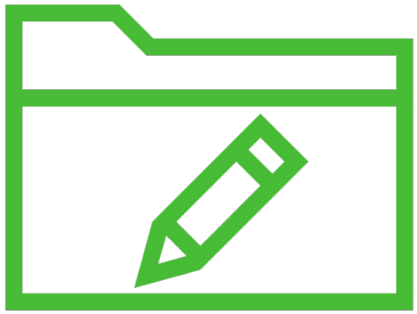
```
PASS_MIN_DAYS   0
PASS_WARN_AGE   7

#
# Min/max values for automatic uid selection in useradd
#
UID_MIN                  1000
UID_MAX                 60000
# System accounts
#SYS_UID_MIN              100
#SYS_UID_MAX              999

#
# Min/max values for automatic gid selection in groupadd
#
GID_MIN                  1000
GID_MAX                 60000
# System accounts
#SYS_GID_MIN              100
#SYS_GID_MAX              999

#
# Max number of login retries if password is bad. This will most likely be
--More--
```

Пользователи: редактирование

```
user@user:~$ usermod --lock xakep
user@user:~$ usermod -p passw ord xakep
user@user:~$ sudo passwd xak ep
user@user:~$ sudo userdel xak ep
```

Группы: редактирование

```
user@user:~$ groupadd ctf
user@user:~$ groupmod -n ctf f tc
user@user:~$ sudo groupdel f tc
```



Ограничение ресурсов

/etc/security/limits.conf – файл, содер жащий ограничения ре сурсов.

```
#         - maxsyslogins - max number of logins on the system
#         - priority - the priority to run user process with
#         - locks - max number of file locks the user can hold
#         - sigpending - max number of pending signals
#         - msgqueue - max memory used by POSIX message queues (bytes)
#         - nice - max nice priority allowed to raise to values: [-20, 19]
#         - rtprio - max realtime priority
#         - chroot - change root to directory (Debian-specific)
#
#<domain>      <type>  <item>         <value>
#

#*               soft    core            0
#root            hard    core            100000
#*               hard    rss             10000
#@student        hard    nproc           20
#@faculty        soft    nproc           20
#@faculty        hard    nproc           50
#ftp             hard    nproc           0
#ftp             -       chroot          /ftp
#@student        -       maxlogins       4

# End of file
```

Права доступа

Атрибуты файла

1. Права пользователя (r, w, x, -).
2. Права группы.
3. Права «всех других».

r w x r w - r - x

4 2 1 4 2 0 4 0 1

7 6 5

```
user@user-VirtualBox:~$ ls -l
total 2196
-r-------- 1 root root 1052672 авг  7 14:43 back
drwxr-xr-x 2 1210 root    4096 окт 23 18:54 community-rules
drwxr-xr-x 2 user user    4096 окт 24 22:42 Desktop
drwxr-xr-x 7 user user    4096 окт 24 22:44 dockpot
drwxr-xr-x 2 user user    4096 июл 27 17:18 Documents
drwxr-xr-x 3 user user    4096 ноя  9 07:46 Downloads
drwxr-xr-x 6 user user    4096 окт 25 21:15 dtk-dist
-rw-rw-r-- 1 user user  993280 окт 25 21:13 dtk.tar
drwxrwxr-x 5 user user    4096 апр 16  2020 go
drwxr-xr-x 6 root root    4096 окт 24 22:59 mhn
drwxr-xr-x 2 user user    4096 апр 13  2020 Music
drwxr-xr-x 2 user user    4096 окт 30 17:17 Pictures
drwxr-xr-x 5 user user    4096 апр 20  2020 projects
drwxr-xr-x 2 user user    4096 апр 13  2020 Public
drwxr-xr-x 7 user user    4096 окт 24 23:31 servletpot
drwxr-xr-x 2 user user    4096 апр 13  2020 Templates
-rw-r--r-- 1 user user  138994 ноя  6 08:00 test.svg
drwxr-xr-x 2 user user    4096 апр 13  2020 Videos
```

Атрибуты каталога

Биты доступа:

- **r** – чтение с одер жимого каталога;
- **w** – право с оздания / изменения / у даления файлов каталога;
- **x** – позво ляет де лать текущий каталог рабочим (pwd).

Специальные биты

Setuid (suid) – позволяет пользователю выполнять программу с правами владельца (s в атрибутах файла).

```
user@Asus:~$ ls -l /bin/sudo
-rwsr-xr-x 1 root root 166056 янв 19 17:21 /bin/sudo
```

Setgid (sgid) – работает аналогично setuid, но для группы.

Sticky – в таком каталоге пользователь может удалять только свои файлы (t в атрибутах файла).

```
user@Asus:~$ ls -ld /tmp/
drwxrwxrwt 23 root root 4096 янв 28 07:10 /tmp/
```

➡ Для большей безопасности при монтировании ФС можно указать параметр nosuid для отключения флагов suid и setgid.

chmod

chmod (change mode) – утилита для изменения прав доступа

- chmod +x <file> chmod -x <file>
- chmod g+r <file> chmod g-r <file>
- chmod o+w <file> chmod o-w <file>
- chmod 660 <file>
- chmod u+s <file> – установка SUID
- chmod g+s <file> – установка SGID
- chmod +t <file> – установка Sticky

chown, chgrp

chown (change owner) – утилита для изменения владельца файла.

```
user@user:~$ chown student file1
```

chgrp (change group) – утилита для изменения группы.

```
user@user:~$ chgrp student file1
```

umask

umask (user mask) – задает биты доступа, устанавливаемые по умолчанию для всех новых файлов.

Заметим, что бит X никогда не устанавливается для созданных файлов.

Umask обладает «инверсной» логикой, т.е. единицы в маске задают нули в правах доступа.

Поэтому, для обычного пользователя:

umask=0002 или -rw-rw-r--

По аналогии:

umask=0000 или -rw-rw-rw-

PAM

PAM

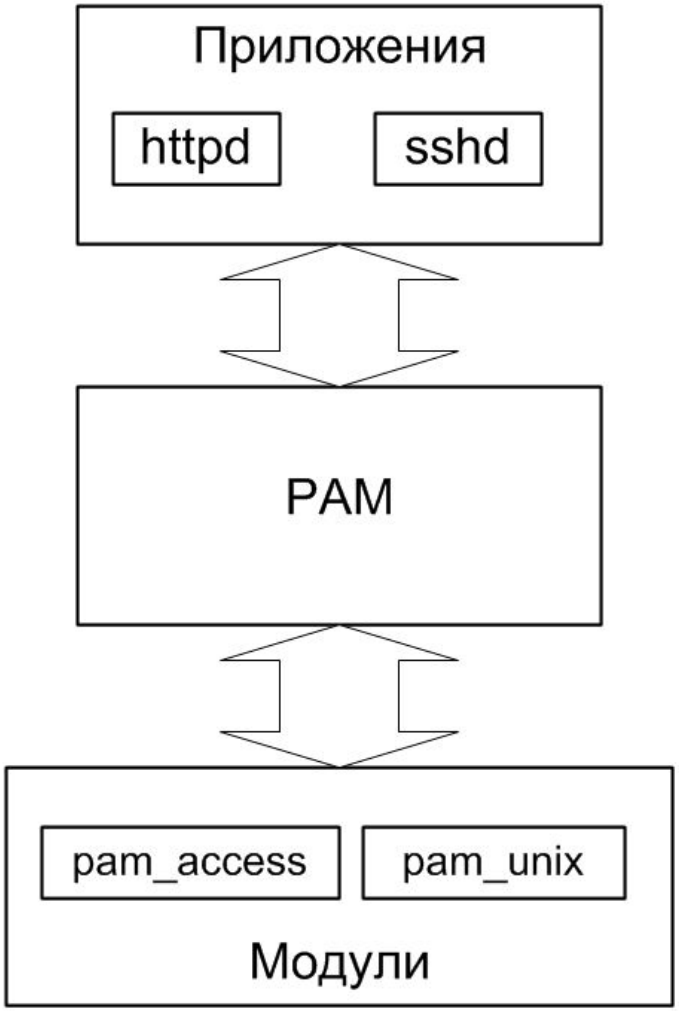
PAM (Pluggable Authentication Modules) – подключаемые модули аутентификации.

PAM – набор библиотек, с помощью которых можно настроить методы аутентификации пользователей.

Типы модулей PAM:

- модули учетных записей;
- модули аутентификации;
- модули паролей;
- модули сессий.

PAM



Ограничение попыток входа

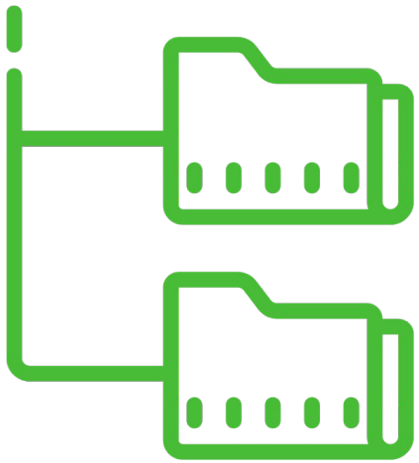
Структура каталогов PAM:

/etc/pam.d/ – файлы конфигураций приложений;

/lib/security/ – модули PAM;

/etc/security/ – файлы конфигураций для PAM-окружений;

/usr/share/doc/pam-*/ – документация.



Ограничение попыток входа

user@user:~$ sudo nano /et c/pam.d/c ommon-auth

```
  GNU nano 4.8                    /etc/pam.d/common-auth

# here are the per-package modules (the "Primary" block)
auth    [success=1 default=ignore]      pam_unix.so nullok_secure
# here's the fallback if no module succeeds

#auth   requisite                       pam_deny.so
auth   required                        pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around

auth    required    pam_tally2.so    onerr=fail deny=3 unlock_time=1500

auth    required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
auth    optional                        pam_cap.so
# end of pam-auth-update config
```

Шифрование

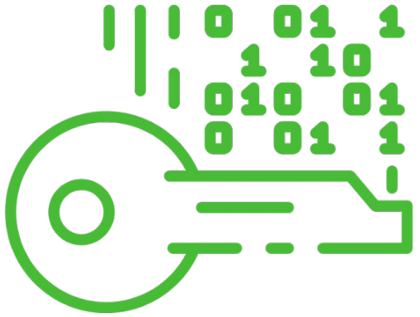
eCryptfs

eCryptfs – это POSIX-совместимая файловая система вложенного (stacked) шифрования.

eCryptfs защищает файлы для любой файловой системы, раздела и т.д.

Установка:

```
user@user:~$ sudo apt install ecryptfs-utils
```



Шифрование домашнего каталога

Создание новог о пользователя:

```
user@user:~$   sudo adduser  --encrypt-home user2
```

Проверка шифрования:

```
user@user:~$   su - user2
user2@user:~$   touch 123,  456
user2@user:~$   exit
user@user:~$   sudo ls /home/user2/
Access- Your-Private-Data.deskt op  README.txt
```

Шифрование каталогов

Миграция домашнего каталога по льзователя:

```
user@user:~$  sudo e cryptfs-migrat e-home  -u user1
```

Шифрование разде ла swap:

```
user@user:~$  sudo e cryptfs-setup-swap
```

Информация для восстановления:

```
user@user:~$  e cryptfs-unwrap-passphrase
```

LUKS

LUKS (Linux Unified Key Setup) – спецификация формата шифрования дисков, используемая в ОС Linux.

При помощи LUKS могут быть зашифрованы диски, работающие в ОС Linux как в настольных компьютерах, так и в разнообразных устройствах, например , сетевых накопителях.

Установка LUKS

Подготовка диска:

user@user:~$ sudo apt install gpar ted

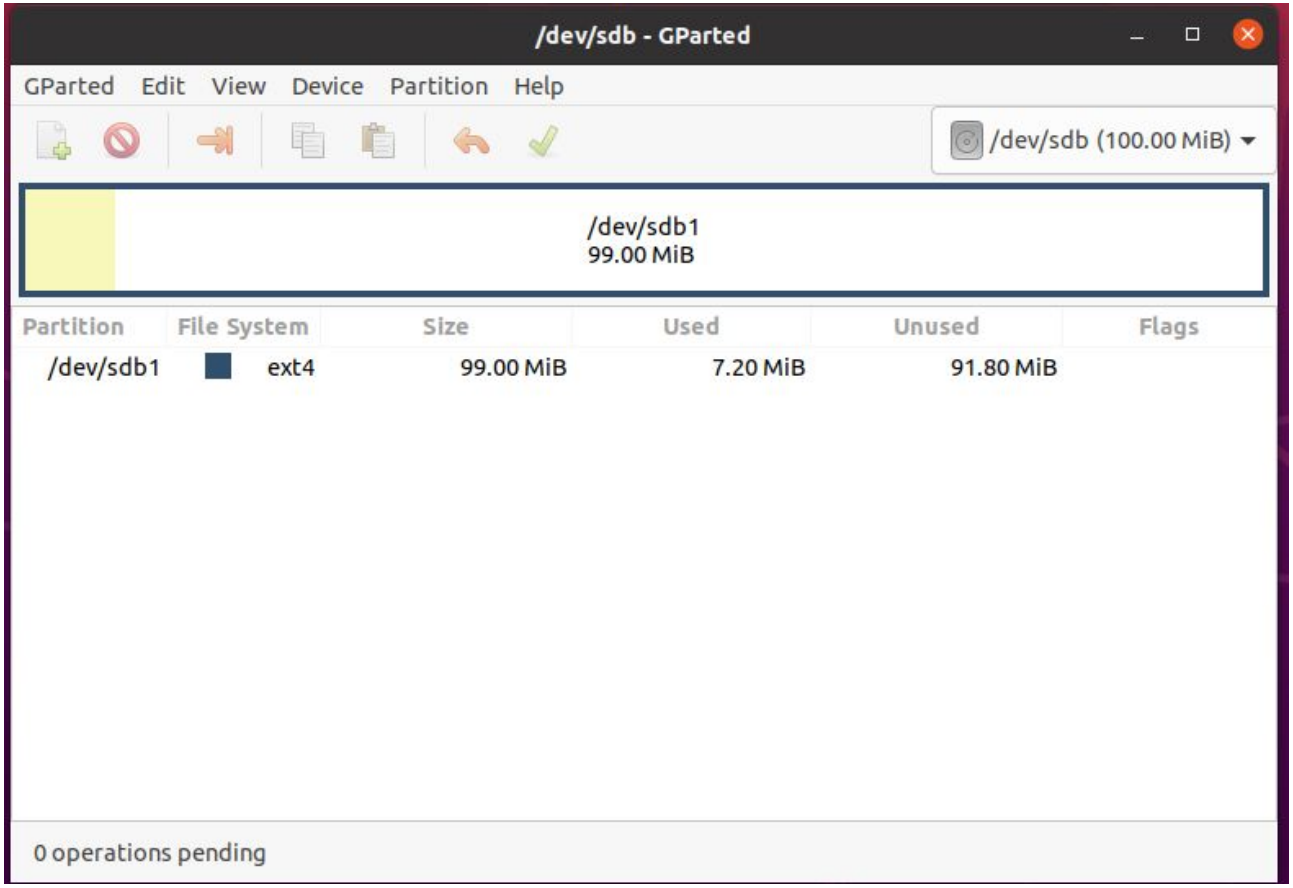
Установка LUKS (должна быть установлено по умо лчанию):

user@user:~$ sudo apt -get install cryptsetup

Проверка у становки:

user@user:~$ cryptsetup --version

LUKS: подготовка раздела



Шифрование раздела LUKS

Подготовка разде ла (luksFormat):

```
user@user:~$ sudo cryptsetup -y -v --type luks2 luksFormat /de v/sdb1
```

Монтирование разде ла:

```
user@user:~$ sudo cryptsetup luksOpen /de v/sdb1 disk
user@user:~$ ls /de v/mapper/disk
```

Форматирование разде ла:

```
user@user:~$ sudo dd if=/de v/zero o f=/dev/mapper/disk
user@user:~$ sudo mkfs.e xt4 /de v/mapper/disk
```

Шифрование раздела LUKS

Монтирование «открытого» раздела:

```
user@user:~$ mkdir .secret
user@user:~$ sudo mount /dev/mapper/disk .secret/
```

Завершение работы:

```
user@user:~$ sudo umount .secret
user@user:~$ sudo cryptsetup luksClose disk
```

Система логирования

Основные лог-файлы

Debian:

```
user@user:~$  sudo cat /var/log/auth.log
user@user:~$  sudo cat /var/log/syslog
```

Red Hat:

```
user@user:~$  sudo cat /var/log/messages
user@user:~$  sudo cat /var/log/se  cure
```

Основные лог-файлы

/var/log/k ern.log – события ядра (debian);

/var/log/wtmp /var/run/utmp – список зах одов по льзоват елей (binary!);

/var/log/btmp – список не удачных вх одов по льзоват елей (binary!);

/var/log/fail2ban – лог fail2ban;

/var/log/suricata/suricata.log (fast .log) – лог suricata;

journalctl – журнал syst emd.

Просмотр лог-файлов

Просмотр длинных текстов:

user@user:~$ sudo less /var/log/syslog

Просмотр последних строк:

user@user:~$ sudo tail /var/log/syslog

Отслеживание появления новых строк:

user@user:~$ sudo tail -f /var/log/syslog

Поиск подстроки в текстовом файле:

user@user:~$ sudo grep 'fail' syslog

user@user:~$ sudo grep -i 'fail' syslog (нечувствительный к регистру)

Просмотр лог-файлов

Заход пользователей и загрузка:

user@user:~$ last (/var/log/wtmp)

Неудачные попытки входа:

user@user:~$ sudo last -f /var/log/btmp

Список пользователей и дата последнего входа:

user@user:~$ lastlog

Итоги

Итоги

Сегодня мы рас смотрели настройки для безопасной рабо ты в Linux:

- права дос тупа;
- PAM;
- шифрование;
- логирование.

Домашнее задание

Домашнее задание

Давайте посмотрим ваше домашнее задание.

- Вопросы по домашней работе задавайте **в чате** мессенджера.
- Задачи можно сдавать **по частям**.
- Зачёт по домашней работе проставляется после того, как **приняты все задачи**.

нетология

Задавайте вопросы и пишите отзыв о лекции!

Антон Лукашов