



МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра Інформаційної Безпеки

Практикум з Основ технологій захисту інформації

Практичне завдання №1 “Механізми захисту ОС Linux”

Перевірів:

Виконав:

студент II курсу

групи ФБ-01

Сахній Н.Р.

Київ 2021

Практичне завдання №1 “Механізми захисту ОС Linux”.

- процедура реєстрації та властивості облікових записів
- навігація і пошук у файлової системі
- атрибути файлів
- керування доступом
- введення-виведення
- керування процесами
- контроль мережної активності

Використовуючі засоби Linux, знайти у системі відповіді на наступні питання. (Переважно, відповіддю буде результат деякої утиліти.) У звіті наведіть утиліти, що вивикористовували, та їх виведення (або фрагменти файлів налаштувань, де зберігається потрібна інформація). Для деяких завдань дано приклади команд.

*Завдання із зірочкою — не обов'язкові, але за них можуть нараховуватись додаткові бали.

Хід роботи:

1.1 Встановіть та запустіть VMWare.

1.2 Відкрийте віртуальну машину з встановленим Linux.

1.3 Вивчіть документацію і перевірте роботу наступних команд:

whoami, id,
pwd, cd, ls, find, grep, xargs, cut, awk chmod,
chown, chgrp, umask, lsattr, chattrln, touch,
mkdir, rmdir, rm
cat, cp, mv, wc, head, tail, sort, ps, top,
kill, renice, od, dd, ifconfig, traceroute,
netstat, fuser

Уважно вивчіть документацію по команді find.

2. Облікові записи та паролі

2.1 Аналіз підсистеми автентифікації

2.1.1 Які облікові записи користувачів є у вашій системі.

Щоб дізнатися які облікові записи користувачів є у вашій системі відкриємо файл /etc/passwd командою cat за допомогою термінала, увівши команду:

```
$ cat /etc/passwd
```

```
(nazar@snz24)-[~]  
$ 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  
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  
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin  
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin  
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin  
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin  
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin  
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin  
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
```

```
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:104:110:MySQL Server,,,:/nonexistent:/bin/false
tss:x:105:111:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:106:65534::/var/lib/strongswan:/usr/sbin/nologin
ntp:x:107:112::/nonexistent:/usr/sbin/nologin
messagebus:x:108:113::/nonexistent:/usr/sbin/nologin
redsocks:x:109:114::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:110:65534::/var/spool/rwho:/usr/sbin/nologin
iodine:x:111:65534::/run/iodine:/usr/sbin/nologin
miredo:x:112:65534::/var/run/miredo:/usr/sbin/nologin
_rpc:x:113:65534::/run/rpcbind:/usr/sbin/nologin
usbmux:x:114:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
tcpdump:x:115:120::/nonexistent:/usr/sbin/nologin
rtkit:x:116:121:RealtimeKit,,,:/proc:/usr/sbin/nologin
sshd:x:117:65534::/run/sshd:/usr/sbin/nologin
statd:x:118:65534::/var/lib/nfs:/usr/sbin/nologin
postgres:x:119:123:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
avahi:x:120:125:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
stunnel4:x:121:126::/var/run/stunnel4:/usr/sbin/nologin
Debian-snmp:x:122:127::/var/lib/snmp:/bin/false
ssllh:x:123:128::/nonexistent:/usr/sbin/nologin
nm-openvpn:x:124:129:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
nm-openconnect:x:125:130:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin
pulse:x:126:131:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
saned:x:127:134::/var/lib/saned:/usr/sbin/nologin
inetsim:x:128:136::/var/lib/inetsim:/usr/sbin/nologin
colord:x:129:137:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:130:138::/var/lib/geoclue:/usr/sbin/nologin
lightdm:x:131:139:Light Display Manager:/var/lib/lightdm:/bin/false
king-phisher:x:132:140::/var/lib/king-phisher:/usr/sbin/nologin
nazar:x:1000:1000:Nazar,,,:/home/nazar:/usr/bin/zsh
systemd-coredump:x:999:999:systemd Core Dumper::/usr/sbin/nologin
```

```
(nazar@snz24)-[~]
```

Один рядок відповідає опису одного облікового запису і складається з кількох полів, розділених двокрапкою. Де перше поле відповідає за назву користувача, наприклад, у рядок

nazar:x:1000:1000:Nazar,,,:/home/nazar:/usr/bin/zsh можна прочитати так:

- nazar - ім'я користувача для входу у систему;
- x - необов'язковий зашифрований пароль;
- 1000 - числовий ідентифікатор користувача (UID);
- 1000 - числовий ідентифікатор основної групи (GID);
- Nazar,,,- необов'язкове поле, яке використовується для вказівки додаткової інформації про користувача (наприклад, повне ім'я користувача);
- /home/nazar - домашній каталог користувача;
- /usr/bin/zsh - командний інтерпретатор користувача.

2.1.2 Які користувачі в поточний момент увійшли до системи ч-з процедуру login.

Команда `who` використовується для отримання списку користувачів, залогінених у системі

```
(nazar@snz24)-[~]
$ who
nazar    tty7          2021-11-06 13:34 (:0)

(nazar@snz24)-[~]
$
```

У виведенні знаходяться наступні стовпчики:

- nazar - ім'я користувача;
- tty - номер tty;

- 2021-11-06 13:34 - дата та час підключення;
- (:0) - адреса підключення.

2.1.3 Які з них увійшли локально, а які віддалено.

Користувач `nazar` увійшов локально, на що вказує значення адреси стовпчика `(:0)` саме так X-Windows представляє "X-дисплей", на якому знаходиться користувач

2.1.4 Які з облікових записів цих користувачів було створено після встановлення системи.



При встановленні системи `Linux` створюється обліковий запис **адміністратора**.

2.1.5 У які у групи входить поточний користувач.

Якщо необхідно отримати імена груп поточного користувача, то використовується опція:

```
$ id -Gn
```

```
(nazar@snz24)-[~]
$ id -Gn
nazar cdrom floppy sudo audio dip video plugdev netdev bluetooth scanner kaboxer
```

2.1.6 Які користувачі входять до кожної з груп (виведіть список груп та відповідних користувачів).

Щоб переглянути які користувачі входять до кожної з груп відкриємо файл `/etc/group` командою `cat` через термінал, ввівши команду:

```
$ cat /etc/group
```

```
(nazar@snz24)-[~]
$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:nazar
floppy:x:25:nazar
tape:x:26:
sudo:x:27:nazar
audio:x:29:pulse,nazar
dip:x:30:nazar
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
```

```
utmp:x:43:
video:x:44:nazar
sasl:x:45:
plugdev:x:46:nazar
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
systemd-timesync:x:101:
systemd-journal:x:102:
systemd-network:x:103:
systemd-resolve:x:104:
input:x:105:
kvm:x:106:
render:x:107:
crontab:x:108:
netdev:x:109:nazar
mysql:x:110:
tss:x:111:
ntp:x:112:
messagebus:x:113:
redsocks:x:114:
kismet:x:115:
mlocate:x:116:
ssh:x:117:
bluetooth:x:118:nazar
ssl-cert:x:119:postgres
tcpdump:x:120:
rtkit:x:121:
kali-trusted:x:122:
postgres:x:123:
i2c:x:124:
avahi:x:125:
stunnel4:x:126:
Debian-snmpp:x:127:
sshd:x:128:
nm-openvpn:x:129:
nm-openconnect:x:130:
pulse:x:131:
pulse-access:x:132:
scanner:x:133:saned,nazar
saned:x:134:
smbshare:x:135:
inetsim:x:136:
colord:x:137:
geoclue:x:138:
lightdm:x:139:
kpadmins:x:140:
nazar:x:1000:
kaboxer:x:141:nazar,root
systemd-coredump:x:999:
```

```
(nazar@snz24)-[~]
$
```

Наприклад, рядок `kaboxer:x:141:nazar, root` можна прочитати так:

- `kaboxer` - назва групи;
- `x` - необов'язковий зашифрований пароль;
- `141` - числовий ідентифікатор групи (GID);
- `nazar, root` - список користувачів, які знаходяться у групі.

2.1.10 Виведіть геші паролів, які є в системі.

(В протоколі роботи замаскуйте значення геш-функцій (замініть на інші символи).

Щоб переглянути геші паролів потрібно у терміналі за допомогою команди `cat` вміст файлу `/etc/shadow`, потрібно записати наступне:

```
$ sudo cat /etc/shadow
```

```
(nazar@snz24)-[~]  
$ sudo cat /etc/shadow  
[sudo] пароль до nazar:  
root:!:18937:0:99999:7:::  
daemon:!:18937:0:99999:7:::  
bin:!:18937:0:99999:7:::  
sys:!:18937:0:99999:7:::  
sync:!:18937:0:99999:7:::  
games:!:18937:0:99999:7:::  
man:!:18937:0:99999:7:::  
lp:!:18937:0:99999:7:::  
mail:!:18937:0:99999:7:::  
news:!:18937:0:99999:7:::  
uucp:!:18937:0:99999:7:::  
proxy:!:18937:0:99999:7:::  
www-data:!:18937:0:99999:7:::  
backup:!:18937:0:99999:7:::  
list:!:18937:0:99999:7:::  
irc:!:18937:0:99999:7:::  
gnats:!:18937:0:99999:7:::  
nobody:!:18937:0:99999:7:::  
_apt:!:18937:0:99999:7:::  
systemd-timesync:!:18937:0:99999:7:::  
systemd-network:!:18937:0:99999:7:::  
systemd-resolve:!:18937:0:99999:7:::  
mysql:!:18937:0:99999:7:::  
tss:!:18937:0:99999:7:::  
strongswan:!:18937:0:99999:7:::  
ntp:!:18937:0:99999:7:::  
messagebus:!:18937:0:99999:7:::  
redsocks:!:18937:0:99999:7:::  
rwhod:!:18937:0:99999:7:::  
iodine:!:18937:0:99999:7:::  
miredo:!:18937:0:99999:7:::  
_rpc:!:18937:0:99999:7:::  
usbmux:!:18937:0:99999:7:::  
tcpdump:!:18937:0:99999:7:::  
rtkit:!:18937:0:99999:7:::  
sshd:!:18937:0:99999:7:::  
statd:!:18937:0:99999:7:::  
postgres:!:18937:0:99999:7:::  
avahi:!:18937:0:99999:7:::  
stunnel4:!:18937:0:99999:7:::  
Debian-snmpp:!:18937:0:99999:7:::  
sslh:!:18937:0:99999:7:::  
nm-openvpn:!:18937:0:99999:7:::  
nm-openconnect:!:18937:0:99999:7:::  
pulse:!:18937:0:99999:7:::  
saned:!:18937:0:99999:7:::  
inetsim:!:18937:0:99999:7:::  
colord:!:18937:0:99999:7:::  
geoclue:!:18937:0:99999:7:::  
lightdm:!:18937:0:99999:7:::  
king-phisher:!:18937:0:99999:7:::
```

```
nazar:$6$zHvrJMa5Y690smbQ$z5zdL...:18937:0:99999:7:::
```



```
systemd-coredump:!*:18937:~::~:
```

```
(nazar@snz24)-[~]  
$
```

Наприклад, рядок `rwild:!:18937:0:99999:7:::` можна прочитати так:

- `rwild` - Ім'я користувача;
- `!` - Зашифрований пароль, Якщо поле пароля містить зірочку (*) або знак оклику (!), користувач не зможе увійти в систему з використанням аутентифікації за паролем. ;
- `18937` - Остання зміна пароля;
- `0` - Мінімальний вік пароля;
- `99999` - Максимальний вік пароля;
- `7` - Період попередження;
- `()` - Період бездіяльності
- `()` - Термін придатності
- `()` - Невикористаний

2.1.11 Яка геш-функція використовується для збереження паролів.

`6` - **SHA-512 із 86 символами**

`$Xwg3PsUW$` - Сіль та роздільники. Сіль - це маленький рядок символів для змішування функції хешування. Її мета - ускладнення виконання конкретних атак, заснованих на добірї пароля з його хешу. Ця сіль складається із символів `az`, `AZ`, `0-9`, `/` та `.`

Довгий рядок символів - хешований пароль

Довгий рядок та його довжина залежать від використаного методу хешування. З `$6` або `SHA-512`, вона буде з 86 символів.

2.1.12 Перевірте складність деякого паролю за допомогою *JohnTheRipper*.

Встановіть пакет з програмою: `#sudo apt-get install john`

Приклад:

```
#unshadow /etc/passwd /etc/shadow >shadowlist
```

```
#john --wordlist=/usr/share/john/password.lst --rules shadowlist
```

```
#john --show shadowlist
```

Процес пошуку може тривати необмежено довго. У будь-який час його можливо зупинити `Ctrl+C`. Щоб впевнитись, що пошук працює,

-Встановіть деякому користувачеві простий пароль та додайте його в файл словника *password.lst*.

```
(nazar@snz24)-[~]  
$ sudo useradd -p JFEMTh6W7MSys -s /bin/bash new_user
```

-Далі введемо команди із прикладу для перевірки заданого паролю на складність

```
(nazar@snz24)-[~]  
$ sudo unshadow /etc/passwd /etc/shadow > shadowlist  
  
(nazar@snz24)-[~]  
$ sudo john --wordlist=/usr/share/john/password.lst --format=descrypt shadowlist  
Using default input encoding: UTF-8  
Loaded 1 password hash (descrypt, traditional crypt(3) [DES 256/256 AVX2])  
No password hashes left to crack (see FAQ)
```

-У результаті пароль розшифровано, його значення були '12345'

```
(nazar@snz24)-[~]
$ sudo john --show shadowlist
new_user:12345:1001:1001::/home/new_user:/bin/bash

1 password hash cracked, 1 left

(nazar@snz24)-[~]
$
```

2.1.13 З'ясуйте, яка в системі встановлена політика паролів та вимоги до складності паролів. Дізнаємося яка в системі встановлена політика паролів та вимоги до складності паролів у файлі:

```
$ cat /etc/pam.d/common-password
```

```
(nazar@snz24)-[~]
$ cat /etc/pam.d/common-password
#
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords. The default is pam_unix.
#
# Explanation of pam_unix options:
#
# The "sha512" option enables salted SHA512 passwords. Without this option,
# the default is Unix crypt. Prior releases used the option "md5".
#
# The "obscure" option replaces the old 'OBSCURE_CHECKS_ENAB' option in
# login.defs.
#
# See the pam_unix manpage for other options.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.
#
# here are the per-package modules (the "Primary" block)
password [success=1 default=ignore] pam_unix.so obscure sha512
# here's the fallback if no module succeeds
password requisite 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
password required pam_permit.so
# and here are more per-package modules (the "Additional" block)
password optional pam_gnome_keyring.so
# end of pam-auth-update config

(nazar@snz24)-[~]
$
```

2.2 Створення, видалення, зміна облікових записів.

Вивчіть роботу наступних утиліт: useradd, groupadd, passwd, userdel.

Створіть дві групи і два користувача. Додайте першого користувача в одну з цих груп, а другого - в обидві. Подивіться, що змінилося в файлах /etc/passwd, /etc/shadow і /etc/group.

```
(nazar@snz24)-[~]
$ sudo groupadd -g 1100 test1
[sudo] пароль до nazar:

(nazar@snz24)-[~]
$ sudo groupadd -g 1200 test2
```

Створимо дві групи

```
(nazar@snz24)-[~]
$ sudo useradd -G test1,test2 somebody

(nazar@snz24)-[~]
$ sudo useradd -G test2 somebody_else

(nazar@snz24)-[~]
$ cat /etc/group
test1:x:1100:somebody
test2:x:1200:somebody,somebody_else

(nazar@snz24)-[~]
$ cat /etc/passwd
somebody:x:1002:1002::/home/somebody:/bin/sh
somebody_else:x:1003:1003::/home/somebody_else:/bin/sh

(nazar@snz24)-[~]
$ sudo cat /etc/shadow
somebody:!:18945:0:99999:7:::
somebody_else:!:18945:0:99999:7:::
```

Добавимо користувачів
так як сказано в завданні

Продемонструємо нові рядки, які
добавились у файли /etc/group,
/etc/passwd і /etc/shadow

*

1 x

3. Файлова система

3.1 Знайдіть файли за деяким шаблоном:

3.1.1 файли, для яких не встановлено власника або групу власника;

```
#find / -nouser | xargs ls -ldb {} \;
```

```
#find / -nogroup | xargs ls -ldb {} \;
```

```
(nazar@snz24)-[~]
$ sudo find / -nouser | xargs ls -ldb {} \
pipe>
find: '/proc/12469/task/12469/fd/5': Немає такого файла або каталогу
find: '/proc/12469/task/12469/fdinfo/5': Немає такого файла або каталогу
find: '/proc/12469/fd/6': Немає такого файла або каталогу
find: '/proc/12469/fdinfo/6': Немає такого файла або каталогу
find: '/run/user/1000/gvfs': Відмовлено у доступі
ls: не вдалося отримати доступ до '{}': Немає такого файла або каталогу

(nazar@snz24)-[~]
$ sudo find / -nogroup | xargs ls -ldb {} \
pipe>
find: '/proc/12476/task/12476/fd/5': Немає такого файла або каталогу
find: '/proc/12476/task/12476/fdinfo/5': Немає такого файла або каталогу
find: '/proc/12476/fd/6': Немає такого файла або каталогу
find: '/proc/12476/fdinfo/6': Немає такого файла або каталогу
find: '/run/user/1000/gvfs': Відмовлено у доступі
ls: не вдалося отримати доступ до '{}': Немає такого файла або каталогу

(nazar@snz24)-[~]
$
```

3.1.2 файли, що доступні на запис для всіх користувачів (world-writable);

```
#find / -perm -002 | xargs ls -ldb {} \;
```

```
(nazar@snz24)-[~]
$ sudo find / -perm -002 | xargs ls -ldb {} \
pipe>
lrwxrwxrwx 1 root root 49 тра 1 2018 /var/lib/ghostscript/CMap/UniKS-UTF8-V → /usr/share/poppler/cMap/Adobe-Ko
ea1/UniKS-UTF8-V
lrwxrwxrwx 1 root root 38 тра 1 2018 /var/lib/ghostscript/CMap/V → /usr/share/poppler/cMap/Adobe-Japan1/V
lrwxrwxrwx 1 root root 46 тра 1 2018 /var/lib/ghostscript/CMap/WP-Symbol → /usr/share/poppler/cMap/Adobe-Japan
/WP-Symbol
lrwxrwxrwx 1 root root 28 сер 5 2018 /var/lib/ieee-data/iab.csv → /usr/share/ieee-data/iab.csv
lrwxrwxrwx 1 root root 28 сер 5 2018 /var/lib/ieee-data/iab.txt → /usr/share/ieee-data/iab.txt
lrwxrwxrwx 1 root root 32 сер 5 2018 /var/lib/ieee-data/.lastupdate → /usr/share/ieee-data/.lastupdate
lrwxrwxrwx 1 root root 28 сер 5 2018 /var/lib/ieee-data/mam.csv → /usr/share/ieee-data/mam.csv
lrwxrwxrwx 1 root root 28 сер 5 2018 /var/lib/ieee-data/mam.txt → /usr/share/ieee-data/mam.txt
lrwxrwxrwx 1 root root 30 сер 5 2018 /var/lib/ieee-data/oui36.csv → /usr/share/ieee-data/oui36.csv
lrwxrwxrwx 1 root root 30 сер 5 2018 /var/lib/ieee-data/oui36.txt → /usr/share/ieee-data/oui36.txt
lrwxrwxrwx 1 root root 28 сер 5 2018 /var/lib/ieee-data/oui.csv → /usr/share/ieee-data/oui.csv
lrwxrwxrwx 1 root root 28 сер 5 2018 /var/lib/ieee-data/oui.txt → /usr/share/ieee-data/oui.txt
drwx-wx-wt 2 root root 4096 тра 11 2020 /var/lib/php/sessions
lrwxrwxrwx 1 root root 9 лис 6 10:31 /var/lock → /run/lock
lrwxrwxrwx 1 root root 4 лис 6 10:31 /var/run → /run
lrwxrwxrwx 1 root root 7 лис 6 10:31 /var/spool/mail → ../mail
drwxrwxrwt 2 root root 4096 лип 5 2020 /var/spool/samba
drwxrwxrwt 7 root root 4096 лис 14 22:09 /var/tmp
```

... і так далі, адже їх багато

3.1.3 файли та каталоги зі встановленими атрибутами *SUID*, *SGID*, *Sticky bit*;

```
#find / -perm -4000 | xargs ls -l -ldb {} \;
```

```
(nazar@snz24)-[~]
$ sudo find / -perm -4000 | xargs ls -l -ldb {} \
find: '/proc/12810/task/12810/fd/5': Немає такого файла або каталогу
find: '/proc/12810/task/12810/fdinfo/5': Немає такого файла або каталогу
find: '/proc/12810/fd/6': Немає такого файла або каталогу
find: '/proc/12810/fdinfo/6': Немає такого файла або каталогу
find: '/run/user/1000/gvfs': Відмовлено у доступі
ls: не вдалося отримати доступ до '{}': Немає такого файла або каталогу
-rwsr-xr-x 1 root root 59680 бер 30 2020 /usr/bin/bwrap
-rwsr-xr-x 1 root root 58416 лют 7 2020 /usr/bin/chfn
-rwsr-xr-x 1 root root 52880 лют 7 2020 /usr/bin/chsh
-rwsr-xr-x 1 root root 34896 жов 12 2020 /usr/bin/fusermount3
-rwsr-xr-x 1 root root 88304 лют 7 2020 /usr/bin/gpasswd
-rwsr-xr-- 1 root kismet 125432 вер 25 2020 /usr/bin/kismet_cap_linux_bluetooth
-rwsr-xr-- 1 root kismet 186584 вер 25 2020 /usr/bin/kismet_cap_linux_wifi
-rwsr-xr-- 1 root kismet 113144 вер 25 2020 /usr/bin/kismet_cap_nrf_51822
-rwsr-xr-- 1 root kismet 117240 вер 25 2020 /usr/bin/kismet_cap_nrf_mousejack
```

```

-rwsr-xr-- 1 root kismet 117240 вер 25 2020 /usr/bin/kismet_cap_nxp_kw41z
-rwsr-xr-- 1 root kismet 117240 вер 25 2020 /usr/bin/kismet_cap_ti_cc_2531
-rwsr-xr-- 1 root kismet 117240 вер 25 2020 /usr/bin/kismet_cap_ti_cc_2540
-rwsr-xr-- 1 root kismet 117240 вер 25 2020 /usr/bin/kismet_cap_ubertooth_one
-rwsr-xr-x 1 root root 55528 лис 1 2020 /usr/bin/mount
-rwsr-xr-x 1 root root 44632 лют 7 2020 /usr/bin/newgrp
-rwsr-xr-x 1 root root 154352 бер 22 2019 /usr/bin/ntfs-3g
-rwsr-xr-x 1 root root 63960 лют 7 2020 /usr/bin/passwd
-rwsr-xr-x 1 root root 23440 сер 3 2020 /usr/bin/pkexec
-rwsr-xr-x 1 root root 71912 лис 1 2020 /usr/bin/su
-rwsr-xr-x 1 root root 178504 вер 24 2020 /usr/bin/sudo
-rwsr-xr-x 1 root root 35040 лис 1 2020 /usr/bin/umount
-rwsr-xr-x 1 root root 14832 жов 25 2020 /usr/bin/vmware-user-suid-wrapper
-rwsr-xr-- 1 root messagebus 51336 лип 2 2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 19040 сер 3 2020 /usr/libexec/polkit-agent-helper-1
-rwsr-xr-x 1 root root 473416 чер 7 2020 /usr/lib/openssh/ssh-keysign
-rwsr-sr-x 1 root root 14608 бер 31 2020 /usr/lib/xorg/Xorg.wrap
-rwsr-xr-x 1 root root 43952 сер 29 2019 /usr/sbin/mount.cifs
-rwsr-xr-x 1 root root 114784 лип 26 2020 /usr/sbin/mount.nfs
-rwsr-xr-- 1 root dip 386792 сер 23 2020 /usr/sbin/pppd

```

(nazar@snz24)-[~]

123 x

#find / -perm -2000 | xargs ls -l -ldb {} \;

```

(nazar@snz24)-[~]
$ sudo find / -perm -2000 | xargs ls -l -ldb {} \
pipe>
find: '/proc/12826/task/12826/fd/5': Немає такого файла або каталогу
find: '/proc/12826/task/12826/fdinfo/5': Немає такого файла або каталогу
find: '/proc/12826/fd/6': Немає такого файла або каталогу
find: '/proc/12826/fdinfo/6': Немає такого файла або каталогу
find: '/run/user/1000/gvfs': Відмовлено у доступі
ls: не вдалося отримати доступ до '{}': Немає такого файла або каталогу
drwxr-s--- 2 root dip 4096 лис 6 10:53 /etc/chatscripts
drwxr-s--- 2 root dip 4096 лис 6 10:53 /etc/ppp/peers
--wxr-S--t 1 nazar nazar 37 лис 9 14:01 /home/nazar/.local/share/Trash/files/lab5.11.txt
drwxr-sr-x+ 2 root systemd-journal 40 лис 6 11:04 /run/log/journal
drwxrwsr-x 2 postgres postgres 40 лис 6 11:04 /run/postgresql
-rwxr-sr-x 1 root shadow 80256 лют 7 2020 /usr/bin/chage
-rwxr-sr-x 1 root crontab 43568 лют 10 2020 /usr/bin/crontab
-rwxr-sr-x 1 root mail 23040 жов 11 2019 /usr/bin/dotlockfile
-rwxr-sr-x 1 root shadow 31160 лют 7 2020 /usr/bin/expiry
-rwxr-sr-x 1 root mlocate 39608 сер 6 2019 /usr/bin/mlocate
-rwxr-sr-x 1 root ssh 342152 чер 7 2020 /usr/bin/ssh-agent
-rwxr-sr-x 1 root tty 35048 лис 1 2020 /usr/bin/wall
-rwxr-sr-x 1 root tty 22760 лис 1 2020 /usr/bin/write.ul
-rwxr-sr-x 1 root utmp 14488 кві 16 2020 /usr/lib/x86_64-linux-gnu/utempter/utempter
-rwsr-sr-x 1 root root 14608 бер 31 2020 /usr/lib/xorg/Xorg.wrap
drwxrwsr-x 4 root staff 4096 лис 6 10:52 /usr/local/lib/python2.7
drwxrwsr-x 2 root staff 4096 лис 6 10:37 /usr/local/lib/python2.7/dist-packages
drwxrwsr-x 2 root staff 4096 лис 6 10:52 /usr/local/lib/python2.7/site-packages
drwxrwsr-x 3 root staff 4096 лис 6 10:32 /usr/local/lib/python3.8
drwxrwsr-x 2 root staff 4096 лис 6 10:32 /usr/local/lib/python3.8/dist-packages
drwxrwsr-x 3 root staff 4096 лис 6 10:51 /usr/local/lib/python3.9
drwxrwsr-x 2 root staff 4096 лис 6 10:51 /usr/local/lib/python3.9/dist-packages
drwxrwsr-x 2 root staff 4096 лис 6 10:52 /usr/local/share/fonts
-rwxr-sr-x 1 root shadow 39616 лют 14 2019 /usr/sbin/unix_chkpwd
drwxrwsr-x 2 root staff 4096 лис 4 2020 /var/local
drwxr-sr-x+ 3 root systemd-journal 4096 лис 6 11:04 /var/log/journal
drwxr-sr-x+ 2 root systemd-journal 4096 лис 6 13:34 /var/log/journal/cef969f013d42e6be11b8b7b31ed546
drwxr-s--- 2 mysql adm 4096 лис 14 15:02 /var/log/mysql
drwxrwsr-x 2 root mail 4096 лис 6 10:31 /var/mail

```

(nazar@snz24)-[~]

123 x

#find / -perm -1000 | xargs ls -ldb {} \;

```

(nazar@snz24)-[~]
$ sudo find / -perm -1000 | xargs ls -ldb {} \
find: '/proc/12842/task/12842/fd/5': Немає такого файла або каталогу
find: '/proc/12842/task/12842/fdinfo/5': Немає такого файла або каталогу
find: '/proc/12842/fd/6': Немає такого файла або каталогу
find: '/proc/12842/fdinfo/6': Немає такого файла або каталогу
find: '/run/user/1000/gvfs': Відмовлено у доступі
ls: не вдалося отримати доступ до '{}': Немає такого файла або каталогу
ls: не вдалося отримати доступ до '/tmp/systemd-private-b08f0b07651e4138b30633d3a4e60470-colord.service-CgQdrf/tmp': Відмовлено у доступі
ls: не вдалося отримати доступ до '/tmp/systemd-private-b08f0b07651e4138b30633d3a4e60470-upower.service-mLVQqf/tmp': Відмовлено у доступі
ls: не вдалося отримати доступ до '/tmp/systemd-private-b08f0b07651e4138b30633d3a4e60470-haveged.service-oVp0jh/tmp': Відмовлено у доступі
ls: не вдалося отримати доступ до '/tmp/systemd-private-b08f0b07651e4138b30633d3a4e60470-ModemManager.service-CAkhDf/tmp': Відмовлено у доступі
ls: не вдалося отримати доступ до '/tmp/systemd-private-b08f0b07651e4138b30633d3a4e60470-systemd-logind.service-r5WpEf/tmp': Відмовлено у доступі
ls: не вдалося отримати доступ до '/var/tmp/systemd-private-b08f0b07651e4138b30633d3a4e60470-systemd-logind.service-RLbmki/tmp': Відмовлено у доступі
ls: не вдалося отримати доступ до '/var/tmp/systemd-private-b08f0b07651e4138b30633d3a4e60470-colord.service-3RjMsg/tmp': Відмовлено у доступі
ls: не вдалося отримати доступ до '/var/tmp/systemd-private-b08f0b07651e4138b30633d3a4e60470-upower.service-FjgrCi/tmp': Відмовлено у доступі
ls: не вдалося отримати доступ до '/var/tmp/systemd-private-b08f0b07651e4138b30633d3a4e60470-haveged.service-x3iztg/tmp': Відмовлено у доступі
ls: не вдалося отримати доступ до '/var/tmp/systemd-private-b08f0b07651e4138b30633d3a4e60470-ModemManager.service-8vKhtj/tmp': Відмовлено у доступі

```



```

drwxrwxrwt 2 root root 40 лис 6 11:04 /dev/mqueue
drwxrwxrwt 2 root root 40 лис 6 11:04 /dev/shm
-rwxr-xr-t 1 nazar nazar 40 лис 13 12:33 /home/nazar/Документи/АКС/lab4.txt
-rwxr-xr-t 1 nazar nazar 40 лис 9 18:17 /home/nazar/.local/share/Trash/files/lab4.txt
-rwxr-xr-t 1 nazar nazar 14 лис 9 13:26 /home/nazar/.local/share/Trash/files/lab5.10.txt
-rwxr-xr-t 1 nazar nazar 37 лис 9 14:01 /home/nazar/.local/share/Trash/files/lab5.11.txt
-rwxr-xr-t 1 nazar nazar 14 лис 9 14:02 /home/nazar/.local/share/Trash/files/lab5.12.txt
-rwxr-xr-t 1 nazar nazar 16 лис 9 14:57 /home/nazar/.local/share/Trash/files/lab5.13.txt
-rwxr-xr-t 1 nazar nazar 16 лис 9 15:17 /home/nazar/.local/share/Trash/files/lab5.14.txt
-rwxr-xr-t 1 nazar nazar 16 лис 9 15:27 /home/nazar/.local/share/Trash/files/lab5.15.txt
-rwxr-xr-t 1 nazar nazar 16 лис 9 15:53 /home/nazar/.local/share/Trash/files/lab5.16.txt
-rwxr-xr-t 1 nazar nazar 16 лис 9 16:03 /home/nazar/.local/share/Trash/files/lab5.17.txt
-rwxr-xr-t 1 nazar nazar 16 лис 9 16:08 /home/nazar/.local/share/Trash/files/lab5.18.txt
-rwxr-xr-t 1 nazar nazar 16 лис 9 17:20 /home/nazar/.local/share/Trash/files/lab5.19.txt
-rwxr-xr-t 1 nazar nazar 16 лис 9 17:36 /home/nazar/.local/share/Trash/files/lab5.20.txt
-rwxr-xr-t 1 nazar nazar 16 лис 9 17:38 /home/nazar/.local/share/Trash/files/lab5.21.txt
-rwxr-xr-t 1 nazar nazar 39 лис 9 17:39 /home/nazar/.local/share/Trash/files/lab5.22.txt
-rwxr-xr-t 1 nazar nazar 16 лис 9 17:59 /home/nazar/.local/share/Trash/files/lab5.23.txt
-rwxr-xr-t 1 nazar nazar 16 лис 9 18:00 /home/nazar/.local/share/Trash/files/lab5.24.txt
-rwxr-xr-t 1 nazar nazar 16 лис 9 18:05 /home/nazar/.local/share/Trash/files/lab5.25.txt
-rwxr-xr-t 1 nazar nazar 40 лис 9 18:07 /home/nazar/.local/share/Trash/files/lab5.26.txt
-rwxr-xr-t 1 nazar nazar 40 лис 9 18:11 /home/nazar/.local/share/Trash/files/lab5.27.txt
-rwxr-xr-t 1 nazar nazar 40 лис 9 18:12 /home/nazar/.local/share/Trash/files/lab5.28.txt
-rwxr-xr-t 1 nazar nazar 40 лис 9 18:14 /home/nazar/.local/share/Trash/files/lab5.29.txt
-rwxr-xr-t 1 nazar nazar 13 лис 9 12:09 /home/nazar/.local/share/Trash/files/lab5.2.txt
-rwxr-xr-t 1 nazar nazar 13 лис 9 12:15 /home/nazar/.local/share/Trash/files/lab5.3.txt
-rwxr-xr-t 1 nazar nazar 14 лис 9 12:28 /home/nazar/.local/share/Trash/files/lab5.4.txt
-rwxr-xr-t 1 nazar nazar 14 лис 9 12:35 /home/nazar/.local/share/Trash/files/lab5.5.txt
-rwxr-xr-t 1 nazar nazar 14 лис 9 13:09 /home/nazar/.local/share/Trash/files/lab5.6.txt
-rwxr-xr-t 1 nazar nazar 14 лис 9 13:16 /home/nazar/.local/share/Trash/files/lab5.7.txt
-rwxr-xr-t 1 nazar nazar 14 лис 9 13:20 /home/nazar/.local/share/Trash/files/lab5.8.txt
-rwxr-xr-t 1 nazar nazar 14 лис 9 13:26 /home/nazar/.local/share/Trash/files/lab5.9.txt
-rwxr-xr-t 1 nazar nazar 13 лис 9 11:54 /home/nazar/.local/share/Trash/files/lab5.txt
drwxrwxrwt 3 root root 60 лис 6 11:04 /run/lock
drwxrwxrwt 2 root utmp 40 лис 6 11:04 /run/screen
drwx-----T 2 root root 0 лис 6 11:04 /sys/fs/bpf
drwxrwxrwt 15 root root 4096 лис 14 22:52 /tmp
drwxrwxrwt 2 root root 4096 лис 6 11:04 /tmp/.font-unix
drwxrwxrwt 2 root root 4096 лис 6 13:34 /tmp/.ICE-unix
drwxrwxrwt 2 root root 4096 лис 6 11:04 /tmp/.Test-unix
drwxrwxrwt 2 root root 4096 лис 9 11:46 /tmp/VMwareDnD
drwxrwxrwt 2 root root 4096 лис 14 22:52 /tmp/.X11-unix
drwxrwxrwt 2 root root 4096 лис 6 11:04 /tmp/.XIM-unix
drwx-wx-wt 2 root root 4096 тра 11 2020 /var/lib/php/sessions
drwxrwx--T 2 root sambashare 4096 лис 6 10:58 /var/lib/samba/usershares
drwxrwxr-t 2 root postgres 4096 лис 6 10:56 /var/log/postgresql
drwx-wx--T 2 root crontab 4096 лют 10 2020 /var/spool/cron/crontabs
drwxrwxrwt 2 root root 4096 лип 5 2020 /var/spool/samba
drwxrwxrwt 7 root root 4096 лис 14 22:39 /var/tmp

```

```

(nazar@snz24)-[~]
$

```

3.1.4 файли та каталоги з датою створення (оновлення) з майбутнього;

```
#find / -newer <file>
```

```

(nazar@snz24)-[~]
$ sudo find / -newer <file> {} \
>
zsh: Немає такого файла або каталогу: file

```

*3.1.5 Знайдіть у системі всі файли зі встановленими атрибутами *append* або *immutable*.

```
#lsattr -l -R /2>/dev/null | grep -E "(Append_Only | Immutable)"
```

3.2 Знайдіть, які файли на даний момент відкриті у системі та які програми їх

використовують.

Використаємо для перегляду перераховує інформацію про файли, відкриті процесами наступну команду:

```
$ sudo lsof
```

```

qterminal 6033 6035 QDBusConn nazar 13u CHR 136,0 0t0 3 /dev/pts/0
qterminal 6033 6035 QDBusConn nazar 14u CHR 226,128 0t0 179 /dev/dri/renderD128
qterminal 6033 6035 QDBusConn nazar 15w FIFO 0,12 0t0 86665 pipe
qterminal 6033 6035 QDBusConn nazar 16r REG 8,1 40624 1737159 /usr/share/icons/hicolor/icon-theme.cache
qterminal 6033 6035 QDBusConn nazar 17u CHR 226,128 0t0 179 /dev/dri/renderD128
qterminal 6033 6035 QDBusConn nazar 19u CHR 226,128 0t0 179 /dev/dri/renderD128
qterminal 6033 6035 QDBusConn nazar 20r a_inode 0,13 0 8962 inotify
qterminal 6033 6035 QDBusConn nazar 22r FIFO 0,12 0t0 86669 pipe
qterminal 6033 6035 QDBusConn nazar 23w FIFO 0,12 0t0 86669 pipe
zsh 6036 nazar cwd DIR 8,1 4096 1308504 /home/nazar/Документи/testlinks
zsh 6036 nazar rtd DIR 8,1 4096 2 /
zsh 6036 nazar txt REG 8,1 865848 1589473 /usr/bin/zsh
zsh 6036 nazar mem REG 8,1 199380 1575978 /usr/share/locale/uk/LC_MESSAGES/libc.mo
zsh 6036 nazar mem REG 8,1 14464 1589504 /usr/lib/x86_64-linux-gnu/zsh/5.8/zsh/regex.so
zsh 6036 nazar mem REG 8,1 202728 1840875 /usr/share/zsh/functions/Misc.zwc
zsh 6036 nazar mem REG 8,1 294424 1839982 /usr/share/zsh/functions/Completion/Base.zwc
zsh 6036 nazar mem REG 8,1 18752 1589507 /usr/lib/x86_64-linux-gnu/zsh/5.8/zsh/stat.so
zsh 6036 nazar mem REG 8,1 14600 1589513 /usr/lib/x86_64-linux-gnu/zsh/5.8/zsh/zleparameter.so
zsh 6036 nazar mem REG 8,1 189744 1840826 /usr/share/zsh/functions/Completion.zwc
zsh 6036 nazar mem REG 8,1 49104 1589502 /usr/lib/x86_64-linux-gnu/zsh/5.8/zsh/parameter.so
zsh 6036 nazar mem REG 8,1 39240 1589517 /usr/lib/x86_64-linux-gnu/zsh/5.8/zsh/zutil.so
zsh 6036 nazar mem REG 8,1 155552 1589482 /usr/lib/x86_64-linux-gnu/zsh/5.8/zsh/complete.so
zsh 6036 nazar mem REG 8,1 335648 1589512 /usr/lib/x86_64-linux-gnu/zsh/5.8/zsh/zle.so
zsh 6036 nazar mem REG 8,1 51696 1572263 /usr/lib/x86_64-linux-gnu/libnss_files-2.31.so
zsh 6036 nazar mem REG 8,1 2996560 1569862 /usr/lib/locale/locale-archive

```

Деякі з них

```

sudo 13616 root 0u CHR 136,0 0t0 3 /dev/pts/0
sudo 13616 root 1u CHR 136,0 0t0 3 /dev/pts/0
sudo 13616 root 2u CHR 136,0 0t0 3 /dev/pts/0
sudo 13616 root 3r FIFO 0,12 0t0 1513432 pipe
sudo 13616 root 4w FIFO 0,12 0t0 1513432 pipe
sudo 13616 root 5u netlink 0t0 1513441 AUDIT
sudo 13616 root 6u unix 0x00000000fe387b3a 0t0 1513454 type=DGRAM
lsof 13617 root cwd DIR 8,1 4096 1308504 /home/nazar/Документи/testlinks
lsof 13617 root rtd DIR 8,1 4096 2 /
lsof 13617 root txt REG 8,1 171488 1579772 /usr/bin/lsof
lsof 13617 root mem REG 8,1 2996560 1569862 /usr/lib/locale/locale-archive
lsof 13617 root mem REG 8,1 149608 1572268 /usr/lib/x86_64-linux-gnu/libpthread-2.31.so
lsof 13617 root mem REG 8,1 18688 1570289 /usr/lib/x86_64-linux-gnu/libdl-2.31.so
lsof 13617 root mem REG 8,1 584360 1571814 /usr/lib/x86_64-linux-gnu/libcpre2-8.so.0.9.0
lsof 13617 root mem REG 8,1 1839792 1570288 /usr/lib/x86_64-linux-gnu/libc-2.31.so
lsof 13617 root mem REG 8,1 167888 1571820 /usr/lib/x86_64-linux-gnu/libselinux.so.1
lsof 13617 root mem REG 8,1 27002 1572693 /usr/lib/x86_64-linux-gnu/gconv/gconv-modules.cache
lsof 13617 root mem REG 8,1 177928 1570283 /usr/lib/x86_64-linux-gnu/ld-2.31.so
lsof 13617 root 0u CHR 136,0 0t0 3 /dev/pts/0
lsof 13617 root 1u CHR 136,0 0t0 3 /dev/pts/0
lsof 13617 root 2u CHR 136,0 0t0 3 /dev/pts/0
lsof 13617 root 3r DIR 0,21 0 1 /proc
lsof 13617 root 4r DIR 0,21 0 1452929 /proc/13617/fd
lsof 13617 root 5w FIFO 0,12 0t0 1513460 pipe
lsof 13617 root 6r FIFO 0,12 0t0 1513461 pipe
lsof 13618 root cwd DIR 8,1 4096 1308504 /home/nazar/Документи/testlinks
lsof 13618 root rtd DIR 8,1 4096 2 /
lsof 13618 root txt REG 8,1 171488 1579772 /usr/bin/lsof
lsof 13618 root mem REG 8,1 2996560 1569862 /usr/lib/locale/locale-archive
lsof 13618 root mem REG 8,1 149608 1572268 /usr/lib/x86_64-linux-gnu/libpthread-2.31.so
lsof 13618 root mem REG 8,1 18688 1570289 /usr/lib/x86_64-linux-gnu/libdl-2.31.so
lsof 13618 root mem REG 8,1 584360 1571814 /usr/lib/x86_64-linux-gnu/libcpre2-8.so.0.9.0
lsof 13618 root mem REG 8,1 1839792 1570288 /usr/lib/x86_64-linux-gnu/libc-2.31.so
lsof 13618 root mem REG 8,1 167888 1571820 /usr/lib/x86_64-linux-gnu/libselinux.so.1
lsof 13618 root mem REG 8,1 177928 1570283 /usr/lib/x86_64-linux-gnu/ld-2.31.so
lsof 13618 root 4r FIFO 0,12 0t0 1513460 pipe
lsof 13618 root 7w FIFO 0,12 0t0 1513461 pipe

```

(nazar@snz24) - [~/Документи/testlinks]
\$

3.3 Знайдіть всі копії деякого файлу за жорстким посиланням. (якщо не знаєте таких файлів - створіть самостійно). Яке значення *inode* має цей файл?

```

(nazar@snz24) - [~]
$ cd /home/nazar/Документи/

(nazar@snz24) - [~/Документи]
$ mkdir testlinks 66 cd testlinks

(nazar@snz24) - [~/Документи/testlinks]
$ echo "symbolic links" > source

(nazar@snz24) - [~/Документи/testlinks]
$ cat source
symbolic links

(nazar@snz24) - [~/Документи/testlinks]
$ ln source hardlink

(nazar@snz24) - [~/Документи/testlinks]
$ cat hardlink
symbolic links

(nazar@snz24) - [~/Документи/testlinks]
$ ls -li
загалом 8
1308505 -rw----- 2 nazar nazar 15 лис 15 00:16 hardlink
1308505 -rw----- 2 nazar nazar 15 лис 15 00:16 source

```

Створимо жорстке посилання `hardlink` на файл `source`, викликавши утиліту `ln` без параметрів, і переглянемо вміст файлу-посилання `hardlink`

Значення *inode* цього файлу `1308505`
Тут число `2` вказує на кількість екземплярів початкового файлу

*Які файли у даній системі мають найбільше жорстких посилань?

3.4 Як порівняти два "майже однакових" файли: чи вони дійсно однакові, або мають незначні відмінності?

Файли можна порівняти "чи вони дійсно однакові" за допомогою команди:

```
$ diff -s source hardlink
```

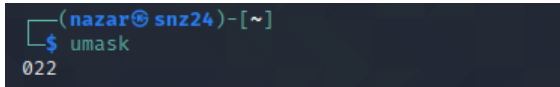
```

(nazar@snz24) - [~/Документи/testlinks]
$ diff -s source hardlink
Файли source та hardlink ідентичні

```

4. Права доступу

4.1 Яке значення *umask* діє у файловій системі зараз і де воно встановлюється.



```
(nazar@snz24) ~  
$ umask  
022
```

Утиліта *umask* - встановлює інверсню маску створюваних файлів 644

4.2 Створіть текстовий файл. Створіть жорстке і символічне посилання на даний файл.

Перемістіть ці посилання в інший каталог. Змініть права доступу на сам файл.

Перевірте, як змінилися права доступу на жорстке посилання. Видаліть файл, що ви створили і подивіться, як змінилося жорстке та символічне посилання.

4.3 Створіть такий виконуваний файл:

```
#!/bin/bash  
if [ -n "$1" ]  
then  
echo Script with parameter '$1' run  
else  
echo Script with no parameter run  
fi  
echo Effective user id:  
id
```

та продемонструйте на ньому дію атрибутів SUID та SGID.

4.4 Створіть ще одну копію цього скрипта та за допомогою *SUDO* дозволяйте деякому користувачеві запускати дану програму з правами root. Іншому користувачеві теж дозволяйте запускати дану програму з правами root (але тільки без аргументів).

*(В загальному випадку, за допомогою утиліти *sudo* надайте можливість деякому (НЕ root) користувачеві виконувати деяку програму (набір програм) з довільними (або тільки з певними) аргументами від імені іншого користувача (або суперкористувача).

4.5 Створіть "темний" каталог та перевірте його роботу.

***4.6 Нехай є дві групи користувачів (назвемо їх "редактори" та "читачі"), які колективно працюють над деяким набором документів у певній папці. Перша з цих груп повинна мати можливість створювати та редагувати документи, а друга - тільки читати той самий набір документів. Як здійснити це у Linux? Опишіть набір користувачів, директорій та налаштування прав доступу відповідно даного сценарію.

Чи можливо це реалізувати через стандартні права доступу Linux.

*4.7 В окремому каталозі налаштуйте даний сценарій роботи через списки контролю доступу Linux послуговуючись утилітами *setfacl* і *getfacl*.

5. Керування процесами та мережні сервіси

5.1 За допомогою команди *od (dd)* запустіть два нескінченних процеси. Через декілька секунд подивіться час виконання двох цих процесів і запам'ятайте відповідні PID.

Виберіть процес з більшим часом виконання і зменшіть його пріоритет. Через деякий час знову порівняйте час виконання цих двох процесів.

Тимчасово призупиніть молодший процес. Через кілька секунд продовжіть його виконання.

Видаліть старший процес і перевірте результат.

```
(nazar@snz24)-[~/Документи/testlinks]
$ od source
00000000 074563 061155 066157 061551 066040 067151 071553 000012
0000017
```

5.2 З'ясуйте, які в даній системі є відкриті мережні порти, які з них використовуються в даний момент. Яка програма використовує той чи інший мережний порт.

```
(nazar@snz24)-[~/Документи/testlinks]
$ netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 ::::ipv6-icmp           [::]:*                  7
Active UNIX domain sockets (only servers)
Proto RefCnt Flags               Type           State         I-Node  Path
unix  2      [ ACC ] STREAM           LISTENING      27785    @/tmp/.ICE-unix/1034
unix  2      [ ACC ] STREAM           LISTENING      22445    @/tmp/.X11-unix/X0
unix  2      [ ACC ] STREAM           LISTENING      26543    /run/user/1000/systemd/private
unix  2      [ ACC ] STREAM           LISTENING      26550    /run/user/1000/bus
unix  2      [ ACC ] STREAM           LISTENING      26551    /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ] STREAM           LISTENING      26552    /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ] STREAM           LISTENING      26553    /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ] STREAM           LISTENING      26554    /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ] STREAM           LISTENING      26555    /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ] STREAM           LISTENING      26556    /run/user/1000/pulse/native
unix  2      [ ACC ] STREAM           LISTENING      20154    /run/dbus/system_bus_socket
unix  2      [ ACC ] STREAM           LISTENING      27296    @/tmp/dbus-tV0uLwvx4e
unix  2      [ ACC ] STREAM           LISTENING      16192    /run/systemd/private
unix  2      [ ACC ] STREAM           LISTENING      16194    /run/systemd/userdb/io.systemd.DynamicUser
unix  2      [ ACC ] STREAM           LISTENING      16206    /run/systemd/fsck.progress
unix  2      [ ACC ] STREAM           LISTENING      16212    /run/systemd/journal/stdout
unix  2      [ ACC ] SEQPACKET        LISTENING      16216    /run/udev/control
unix  2      [ ACC ] STREAM           LISTENING      16423    /run/systemd/journal/io.systemd.journal
unix  2      [ ACC ] STREAM           LISTENING      22446    /tmp/.X11-unix/X0
unix  2      [ ACC ] STREAM           LISTENING      27718    /tmp/ssh-tibsXzL3cID2/agent.1034
unix  2      [ ACC ] STREAM           LISTENING      27786    /tmp/.ICE-unix/1034
```

5.3 Знайдіть, які мережні порти відкриті у системі та які програми використовують дані порти.

6. Результати роботи

6.1 Збережіть лістинг команд, що виконувались в роботі.

6.2 На основі аналізу отриманих результатів, зробіть висновок, де у вашій системі є вразливості (або їх ознаки).

Контрольні питання та завдання:

- Які підсистеми захисту повинні бути в операційній системі. У чому полягає їхня робота. У чому полягає їх налаштування в ОС Linux.

Сервіси і підсистеми захисту ОС:

- Ідентифікація та автентифікація
 - Керування доступом
 - Реєстрація, облік і аудит (+ захист і аналіз журналів реєстрації)
 - Захист оперативної пам'яті, знищення залишкових даних
 - Антивірусний захист
 - Управління політикою безпеки і параметрами захисту (інтерфейси управління)
 - Оповіщення, реагування і відновлення безпеки
 - Криптографічні функції (шифрування, цілісність, управління ключами)
 - Апаратні засоби
- Дізнайтеся ідентифікатори поточного користувача.

Команда `id` або ж `id -u`

```
(nazar@snz24)~$ id
uid=1000(nazar) gid=1000(nazar) grpid=1000(nazar),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),109(netdev),118(bluetooth),133(scanner),141(kaboxer)
```

- У яких файлах зібрано інформацію про всі облікові записи користувачів системи.

Щоб дізнатися які облікові записи користувачів є у вашій системі відкриємо файл `/etc/passwd` командою `cat` за допомогою терміналу, увівши команду:

```
$ cat /etc/passwd
```

- Який користувач в ОС Unix є суперкористувачем. Чи може довільний обліковий запис надавати повноваження суперкористувача. Які «особливі» повноваження має обліковий запис суперкористувача. `root`

5.1.1. Суперкористувач

У всіх системах на базі Linux завжди є один обліковий запис, який називається `root` або **суперкористувач**.



Суперкористувач має право на виконання будь-яких дій і зміни будь-яких параметрів. Більшість системних процесів працюють від імені `root`.



`sudo` - це назва програми, що надає **привілеї** `root` для виконання адміністративних дій.

`sudo` дозволяє легко контролювати доступ до важливих застосунків у системі. За замовчуванням, при

- Перевірте за допомогою утиліти JohnTheRipper стійкість пароля користувача root.

↑↑↑ 2.1.12 ↑↑↑

- Нехай відомий геш пароля, а також відома структура пароля. За допомогою утиліти JohnTheRipper відновіть пароль. Скільки потрібно для цього ітерацій?

???

- Знайдіть облікові записи, для яких не встановлено пароль.

Щоб переглянути геші паролів потрібно у терміналі за допомогою команди `cat` вміст файлу `/etc/shadow`, потрібно записати наступне:

```
$ sudo cat /etc/shadow
```

- Виведіть права доступу для деякого файлу.

```
ls -l
```

```
(nazar@snz24)~$ ls -l shadowlist
-rw-r--r-- 1 nazar nazar 3210 лис 14 19:54 shadowlist
```

- Скільки категорій користувачів можуть мати різні набори прав доступу на деякий файл або каталог.

Ці типи прав доступу можуть бути надані трьом категоріям користувачів: власникові файла, групі користувачів або всім іншим користувачам.

- Як змінити права доступу «за замовчуванням» для новостворюваних файлів.

```
umask
```

- Встановіть права доступу «за замовчуванням», щоб новостворювані файли отримували права доступу `rw- r-- r--` (`gwx r-x r--` або `gwxgw- rw-` тощо).

```
umask 644 ( umask 754 або umask 766)
```

- Що означає право доступу "x" для файлів.

Значення прав доступу у файлів і каталогів [\[ред. | ред. код \]](#)

Дозволи для файлів і каталогів мають деякі відмінності, які відображає наступна таблиця:

	Файл	Каталог
Read	читання з файлу	читання з каталогу (випис вмісту)
Write	запис до файлу	запис до каталогу (створення, видалення, перейменування файлів та підкаталогів)
eXecute	виконання (програма, скрипт)	відкриття каталогу

- Що означають права доступу "r" та "x" для каталогів.

Каталог
читання з каталогу (випис вмісту)
запис до каталогу (створення, видалення, перейменування файлів та підкаталогів)
відкриття каталогу

- Які права необхідно надати користувачеві, щоб він зміг видалити деякий каталог (або файл).

write для корінного каталогу

- Продемонструйте дію бітів SUID, SGID і StickyBit для каталогів та файлів.

Спеціальні права доступу [ред. | ред. код]

Також існують спеціальні біти, такі як **SUID**, **SGID** і **Sticky**-біт. Спеціальні права змінюють стандартну поведінку системи, що зручно в деяких спеціальних випадках.

- **SUID**-біт

програма працює з правами власника виконуваного файлу

- **SGID** біт

програма виконується з правами групи, що володіє файлом

- **sticky** біт

дозволяє видаляти і редагувати лише власні файли (для каталогу /tmp, тому що всі в ньому мають право запису)

- Які існують атрибути файлів та каталогів. Продемонструйте дію атрибутів immutable і append для каталогів і файлів.

Аатрибути файлів:

- i (immutable) - блокування змін
- a (append) - тільки додавання
- c (compress) - автономне стиснення / декомпресія
- s (shred) - гарантоване затирання секторів

- У чому полягають права «власника» файлу.

-
- Як змінити власника/групу власника деякого файлу.

chown [Опції] користувач [: Група] файл...

- Чи можна зробити інформацію файлу недоступною для суперкористувача.

Не можна

- Чим жорстке посилання відрізняється від символічного.

Основні властивості **символьних** посилань:

- можуть посилатися на файли і каталоги;
- після видалення, переміщення або перейменування файлу стають недійсними;
- права доступу і номер inode відрізняються від початкового файлу;
- права доступу для символічних посилань значення не мають (права доступу завжди `gwxrwxgwx`);
- при зміні прав доступу для початкового файлу, права на посилання залишаються незмінними;
- можна посилатися на інші розділи диска;
- містять тільки ім'я файлу, а не його вміст.

Розглянемо деякі властивості **жорстких** посилань:

- працюють тільки в межах однієї файлової системи (причина проста: лічильник посилання зберігається у самому [inode](#), а останній не може спільно використовуватися у різних файлових системах);
 - не можна посилатися на каталоги, лише на файли;
 - мають ту ж інформацію [inode](#) і набір дозволів, що і у початкового файла;
 - дозволи на посилання змінюються при зміні дозволів файла;
 - можна переміщувати та перейменовувати і, навіть, видаляти файл без шкоди посиланням.
-
- Чи можна створити жорстке посилання, що вказує на інше жорстке посилання (жорстке посилання, що вказує на символічне посилання; символічне посилання, що вказує на символічне посилання тощо...).

Так можна, перевіряв

- Скільки може існувати жорстких або символічних посилань на каталог або файл.

Довільна кількість

- Знайдіть в файловій системі всі файли (каталоги) за наступними умовами:
 - що належать певному користувачеві або групі;
 - не мають власника/групи (власник/група видалені);
 - з певними правами доступу (наприклад, 644, * 4 *, 6 ** і т.д.);
 - доступні для запису всім користувачам;
 - з встановленими бітами SUID / SGID / Sticky Bit;
 - з встановленими атрибутами Immutable або Append;
 - з часом оновлення файла до/після деякого часу (наприклад, до 10:00 am 1.04.2017 :)
 - по деякому шаблону імені;
 - містять деякий шаблон тексту;

* Використовуючи PAM - модулі:

- Встановити обмеження на складність пароля користувача (мінімальна кількість символів в паролі, мінімальна кількість змінених символів при зміні пароля; мінімальна кількість цифр, малих і великих літер та інших символів в паролі);
- Змінити алгоритм гешування паролів, що використовується в системі;
- Налаштуйте блокування облікового запису після певної кількості невірно введених паролів;
- Встановіть обмеження доступу деякого користувача за часом доби або днів тижня;
- Обмежте ресурси, що будуть доступні окремому користувачеві (кількість одночасних сеансів одного користувача; максимальна кількість запущених процесів; максимальна кількість пам'яті, доступна одному процесу; максимальна кількість дискового простору або файлів, які може створити користувач; максимальний розмір одного файлу; максимальна кількість одночасно відкритих файлів);
- Надайте можливість стати суперкористувачем тільки користувачам, які входять в деяку групу; дозвольте користувачам даної групи ставати суперкористувачем без введення пароля;
- Встановіть змінні оточення;

* Було запущено деяку програму. Як визначити, який з, можливо, кількох однойменних примірників в файловій системі дійсно був запущений. Як вплинути на вибір файлу, що запускається. Яке відношення це має до безпеки ОС.

* За допомогою chroot запустіть деяку програму (наприклад, ls, ifconfig, passwd ...) в замкнутому просторі;

* Які опції монтування файлової системи впливають на безпеку;

* Вивчіть документацію по Linux ACL і продемонструйте його використання;

* Як через механізм Linux ACL впровадити деякий сценарій нормативного керування доступом.