Цель работы

Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux

Задание

Выполнить все пункты работы, занося ответы на поставленные вопросы и замечания в отчёт.

Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создайте учётную запись пользователя guest
2. Задайте пароль для пользователя guest
3. Войдите в систему от имени пользователя guest.
4. Определите директорию, в которой вы находитесь, командой pwd. Сравните её с приглашением командной строки. Определите, является ли она вашей домашней директорией? Если нет, зайдите в домашнюю директорию. - Командная строка пишет, что я в "~" - домашнем каталоге. Нахожусь в домашней директории пользователя guest, в данный момент работаю под ней, значит да
5. Уточните имя вашего пользователя командой whoami.
6. Уточните имя вашего пользователя, его группу, а также группы, куда входит пользователь, командой id. Выведенные значения uid, gid и др. запомните. Сравните вывод id с выводом команды groups. - groups выводит название группы в которой находится пользователь, а id выводит значения в виде цифр и скобках букв, к которым принадлежит пользователь
7. Сравните полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки. - При создании пользователя без дополнительных флагов, ему присваивается uid, gid, groups с его именем
8. Просмотрите файл /etc/passwd
   Найдите в нём свою учётную запись. Определите uid пользователя.
   Определите gid пользователя. Сравните найденные значения с полученными в предыдущих пунктах. - 1001 и 1001 точно такие же как при выводе id
9. Определите существующие в системе директории
   Удалось ли вам получить список поддиректорий директории /home? Ка-
   кие права установлены на директориях? - Да, rwx - все права для владельца директорией и никаких для группы, в которой состоит владелец, и гостей
10. Проверьте, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home
    Удалось ли вам увидеть расширенные атрибуты директории?
    Удалось ли вам увидеть расширенные атрибуты директорий других пользователей? - Для guest домашнего каталога да, для другого нет, доступ запрещен
11. Создайте в домашней директории поддиректорию dir1
    Определите командами ls -l и lsattr, какие права доступа и расши-
    ренные атрибуты были выставлены на директорию dir1. - Все права для владельца, права исполнения для группы и чтение, исполнение для всех. Расширенных атрибутов на папке нет

12. Снимите с директории dir1 все атрибуты и проверьте с её помощью правильность выполнения команды ls -l
13. Попытайтесь создать в директории dir1 файл file1 командой
    echo "test" > /home/guest/dir1/file1
    Объясните, почему вы получили отказ в выполнении операции по созданию файла? Оцените, как сообщение об ошибке отразилось на создании файла? Проверьте действительно ли файл file1 не находится внутри директории dir1. - После предыдущего пункта все возможные права были отключены, в итоге работать с каталогом нельзя, нет доступа. Файл не создался, вернем права и проверим, файла нет.

```
[iayukhnin@localhost ~]$ sudo useradd guest
Creating mailbox file: File exists
[iayukhnin@localhost ~]$ sudo passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[iayukhnin@localhost ~]$ su - guest
Password:
[guest@localhost ~]$ pwd
/home/guest
[guest@localhost ~]$ whoami
guest
[guest@localhost ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@localhost ~]$ groups
guest
[guest@localhost ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:998:996:User for polkitd:/:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
sssd:x:997:993:User for sssd:/:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
pipewire:x:996:992:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
libstoragemgmt:x:995:991:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin
geoclue:x:994:989:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:993:988:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:992:987:User for cockpit-ws instances:/nonexisting:/sbin/nologin
setroubleshoot:x:991:986:SELinux troubleshoot server:/var/lib/setroubleshoot:/sbin/nologin
flatpak:x:990:985:User for flatpak system helper:/:/sbin/nologin
colord:x:989:984:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:988:983:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
systemd-oom:x:981:981:systemd Userspace OOM Killer:/:/usr/sbin/nologin
pesign:x:980:980:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
gnome-initial-setup:x:979:979::/run/gnome-initial-setup/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:978:978::/var/lib/chrony:/sbin/nologin
dnsmasq:x:977:977:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
iayukhnin:x:1000:1000:Yukhnin Ilia:/home/iayukhnin:/bin/bash
vboxadd:x:976:1::/var/run/vboxadd:/bin/false
guest:x:1001:1001::/home/guest:/bin/bash
[guest@localhost ~]$ ls -l /home/
total 4
drwx------.  4 guest     guest      112 Sep 10 16:01 guest
drwx------. 14 iayukhnin iayukhnin 4096 Sep 10 15:37 iayukhnin
[guest@localhost ~]$ lsattr /home/
lsattr: Permission denied While reading flags on /home/iayukhnin
---------------------- /home/guest
[guest@localhost ~]$ mkdir dir1
[guest@localhost ~]$ rm 1 dir
rm: cannot remove '1': Is a directory
rm: cannot remove 'dir': Is a directory
[guest@localhost ~]$ rm -R 1 dir
[guest@localhost ~]$ lsattr
---------------------- ./dir1
[guest@localhost ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 10 16:02 dir1
[guest@localhost ~]$ chmod 000 dir1/
[guest@localhost ~]$ ls -l
total 0
d---------. 2 guest guest 6 Sep 10 16:02 dir1
[guest@localhost ~]$ echo "test" > /home/guest/dir1/file1
-bash: /home/guest/dir1/file1: Permission denied
[guest@localhost ~]$ ls -l /home/guest/dir1/
ls: cannot open directory '/home/guest/dir1/': Permission denied
[guest@localhost ~]$ chmod 777 dir1/
[guest@localhost ~]$ ls -l /home/guest/dir1/
```

```
total 0
```

14. Заполните таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет.
    Если операция разрешена, занесите в таблицу знак «+», если не разрешена, знак «-».

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименовывание файла	Смена атрибутов файла
d--------- (000)	0	-	-	-	-	-	-	-	-
d--x------ (100)	0	-	-	-	-	+	-	-	+
d-w------- (200)	0	-	-	-	-	-	-	-	-
d-wx------ (300)	0	+	+	-	-	+	-	+	+
dr-------- (400)	0	-	-	-	-	-	+	-	-
dr-x------ (500)	0	-	-	-	-	+	+	-	+
drw------- (600)	0	-	-	-	-	-	+	-	-
drwx------ (700)	0	+	+	-	-	+	+	+	+
d--------- (000)	--x------ (100)	-	-	-	-	-	-	-	-
d--x------ (100)	--x------ (100)	-	-	-	-	+	-	-	+
d-w------- (200)	--x------ (100)	-	-	-	-	-	-	-	-
d-wx------ (300)	--x------ (100)	+	+	-	-	+	-	+	+
dr-------- (400)	--x------ (100)	-	-	-	-	-	+	-	-
dr-x------ (500)	--x------ (100)	-	-	-	-	+	+	-	+
drw------- (600)	--x------ (100)	-	-	-	-	-	+	-	-
drwx------ (700)	--x------ (100)	+	+	-	-	+	+	+	+
d--------- (000)	-w------- (200)	-	-	-	-	-	-	-	-
d--x------ (100)	-w------- (200)	-	-	+	-	+	-	-	+
d-w------- (200)	-w------- (200)	-	-	-	-	-	-	-	-
d-wx------ (300)	-w------- (200)	+	+	+	-	+	-	+	+
dr-------- (400)	-w------- (200)	-	-	-	-	-	+	-	-
dr-x------ (500)	-w------- (200)	-	-	+	-	+	+	-	+
drw------- (600)	-w------- (200)	-	-	-	-	-	+	-	-
drwx------ (700)	-w------- (200)	+	+	+	-	+	+	+	+
d--------- (000)	-wx------ (300)	-	-	-	-	-	-	-	-
d--x------ (100)	-wx------ (300)	-	-	+	-	+	-	-	+
d-w------- (200)	-wx------ (300)	-	-	-	-	-	-	-	-
d-wx------ (300)	-wx------ (300)	+	+	+	-	+	-	+	+
dr-------- (400)	-wx------ (300)	-	-	-	-	-	+	-	-
dr-x------ (500)	-wx------ (300)	-	-	+	-	+	+	-	+
drw------- (600)	-wx------ (300)	-	-	-	-	-	+	-	-
drwx------ (700)	-wx------ (300)	+	+	+	-	+	+	+	+
d--------- (000)	r-------- (400)	-	-	-	-	-	-	-	-
d--x------ (100)	r-------- (400)	-	-	-	+	+	-	-	+
d-w------- (200)	r-------- (400)	-	-	-	-	-	-	-	-
d-wx------ (300)	r-------- (400)	+	+	-	+	+	-	+	+
dr-------- (400)	r-------- (400)	-	-	-	-	-	+	-	-
dr-x------ (500)	r-------- (400)	-	-	-	+	+	+	-	+
drw------- (600)	r-------- (400)	-	-	-	-	-	+	-	-
drwx------ (700)	r-------- (400)	+	+	-	+	+	+	+	+
d--------- (000)	r-x------ (500)	-	-	-	-	-	-	-	-
d--x------ (100)	r-x------ (500)	-	-	-	+	+	-	-	+
d-w------- (200)	r-x------ (500)	-	-	-	-	-	-	-	-
d-wx------ (300)	r-x------ (500)	+	+	-	+	+	-	+	+
dr-------- (400)	r-x------ (500)	-	-	-	-	-	+	-	-
dr-x------ (500)	r-x------ (500)	-	-	-	+	+	+	-	+
drw------- (600)	r-x------ (500)	-	-	-	-	-	+	-	-
drwx------ (700)	r-x------ (500)	+	+	-	+	+	+	+	+
d--------- (000)	rw------- (600)	-	-	-	-	-	-	-	-
d--x------ (100)	rw------- (600)	-	-	+	+	+	-	-	+
d-w------- (200)	rw------- (600)	-	-	-	-	-	-	-	-
d-wx------ (300)	rw------- (600)	+	+	+	+	+	-	+	+
dr-------- (400)	rw------- (600)	-	-	-	-	-	+	-	-
dr-x------ (500)	rw------- (600)	-	-	+	+	+	+	-	+
drw------- (600)	rw------- (600)	-	-	-	-	-	+	-	-
drwx------ (700)	rw------- (600)	+	+	+	+	+	+	+	+
d--------- (000)	rwx------ (700)	-	-	-	-	-	-	-	-
d--x------ (100)	rwx------ (700)	-	-	+	+	+	-	-	+
d-w------- (200)	rwx------ (700)	-	-	-	-	-	-	-	-
d-wx------ (300)	rwx------ (700)	+	+	+	+	+	-	+	+
dr-------- (400)	rwx------ (700)	-	-	-	-	-	+	-	-
dr-x------ (500)	rwx------ (700)	-	-	+	+	+	+	-	+
drw------- (600)	rwx------ (700)	-	-	-	-	-	+	-	-
drwx------ (700)	rwx------ (700)	+	+	+	+	+	+	+	+

15. На основании заполненной таблицы определите те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполните следующую таблицу

Операция	**Минимальные права на директорию**	**Минимальные права на файл при доступе в директорию (300) и (700)**
Создание файла	(300)	(000)
Удаление файла	(300)	(000)
Чтение файла	(100)	(400)
Запись в файл	(100)	(200)
Переименование файла	(300)	(000)

Операция	Минимальные права на директорию	Минимальные права на файл при доступе в директорию (300) и (700)
Создание поддиректории	(300)	(000)
Удаление поддиректории	(300)	(000)

Выводы

В ходе выполнения данной лабораторной работы я приобрел навыки дискреционного разграничения прав в Linux.

Список литературы

- Лабораторная работа №2