

Лабораторная работа №2

Информационная безопасность

Леонтьева К. А., НПМбд-01-19

15 сентября 2022

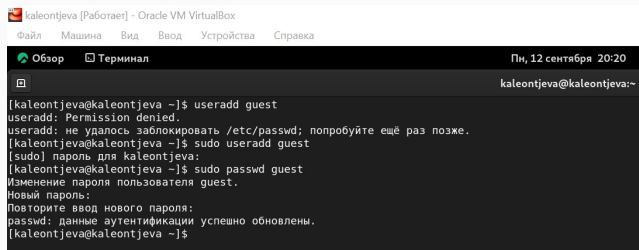
Российский университет дружбы народов

Москва, Россия

- 1) Получение практических навыков работы в консоли с атрибутами файлов
- 2) Закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux

- 1) Создать новую учётную запись
- 2) Проанализировать права доступа и расширенные атрибуты для директорий и файлов

- Создаем нового пользователя guest



```
kaleontjeva [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Обзор  Терминал  Пн, 12 сентября 20:20
kaleontjeva@kaleontjeva:~

[kaleontjeva@kaleontjeva ~]$ useradd guest
useradd: Permission denied.
useradd: не удалось заблокировать /etc/passwd; попробуйте ещё раз позже.
[kaleontjeva@kaleontjeva ~]$ sudo useradd guest
[sudo] пароль для kaleontjeva:
[kaleontjeva@kaleontjeva ~]$ sudo passwd guest
Изменение пароля пользователя guest.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[kaleontjeva@kaleontjeva ~]$
```

Figure 1: Рис.1: Создание пользователя

- Входим в систему от имени пользователя guest

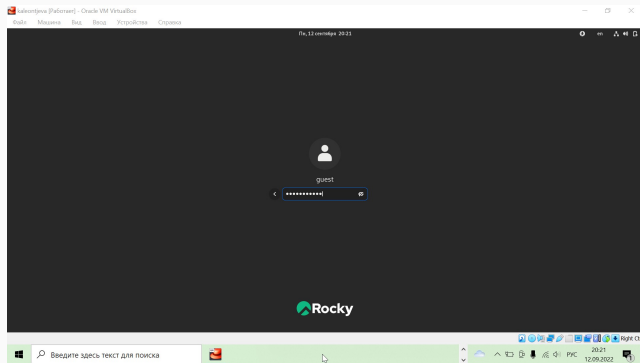
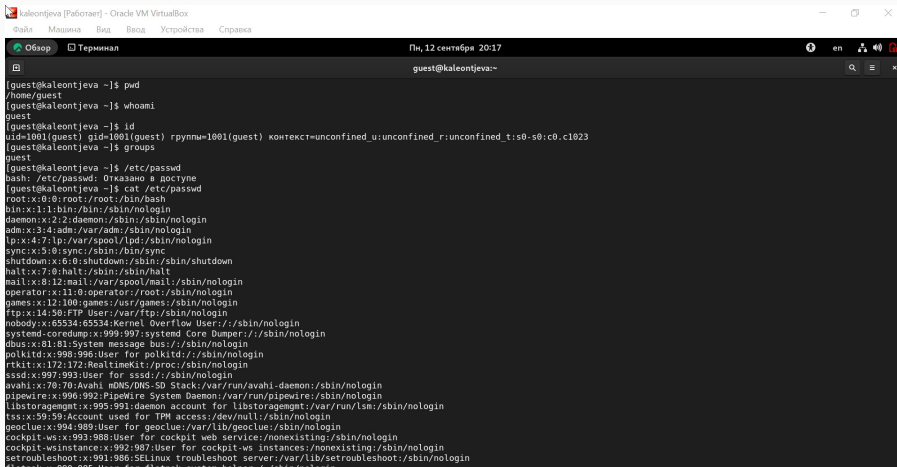


Figure 2: Рис.2: Вход в систему

Ход выполнения лабораторной работы

- Изучение команд `pwd`, `whoami`, `id`, `groups`, `cat`, сравнение полученных данных

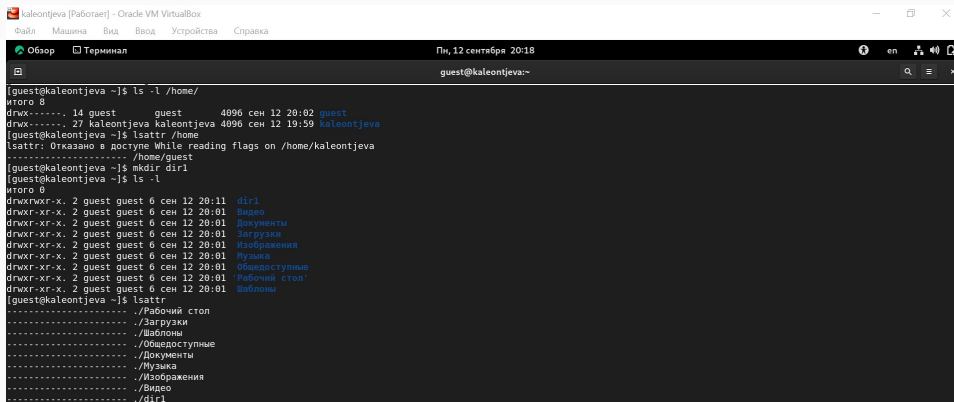


```
kaleontjeva [Работа] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Обзор  Терминал  Пн, 12 сентября 20:17
guest@kaleontjeva:~$ pwd
/home/guest
guest@kaleontjeva:~$ whoami
quest
guest@kaleontjeva:~$ id
uid=1001(guest) gid=1001(guest) rpyнны=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
guest@kaleontjeva:~$ groups
quest
guest@kaleontjeva:~$ /etc/passwd
bash: /etc/passwd: Отказано в доступе
guest@kaleontjeva:~$ 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:990:996: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:992:907:User for cockpit-ws instances:/nonexisting:/sbin/nologin
setroubleshoot:x:991:986:SELinux troubleshoot server:/var/lib/setroubleshoot:/sbin/nologin
d1-troubleshoot:x:990:985:User for d1-troubleshoot:/sbin/nologin
```

Figure 3: Рис.3: Команды `pwd`, `whoami`, `id`, `groups`, `cat`

- Просмотр прав доступа и расширенных атрибутов для директорий в системе



```
kaleontjeva [Работаer] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Обзор  Терминал  Пн, 12 сентября 20:18
guest@kaleontjeva:~

[guest@kaleontjeva ~]$ ls -l /home/
итого 8
drwx----- 14 guest      guest      4096 сен 12 20:02 guest
drwx----- 27 kaleontjeva kaleontjeva 4096 сен 12 19:59 kaleontjeva
[guest@kaleontjeva ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/kaleontjeva
----- /home/guest
[guest@kaleontjeva ~]$ mkdir dir1
[guest@kaleontjeva ~]$ ls -l
итого 0
drwxrwxr-x. 2 guest guest 6 сен 12 20:11 dir1
drwxr-xr-x. 2 guest guest 6 сен 12 20:01 Видео
drwxr-xr-x. 2 guest guest 6 сен 12 20:01 Документы
drwxr-xr-x. 2 guest guest 6 сен 12 20:01 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 12 20:01 Изображения
drwxr-xr-x. 2 guest guest 6 сен 12 20:01 Музыка
drwxr-xr-x. 2 guest guest 6 сен 12 20:01 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 12 20:01 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 сен 12 20:01 Шаблоны
[guest@kaleontjeva ~]$ lsattr
----- ./Рабочий стол
----- ./Загрузки
----- ./Шаблоны
----- ./Общедоступные
----- ./Документы
----- ./Музыка
----- ./Изображения
----- ./Видео
----- ./dir1
```

Figure 4: Рис.4: Права доступа и расширенные атрибуты

- Заполнение таблицы “Установленные права и разрешённые действия”

Права	Соз-	Уда-	Сме-	на	Сме-	на	Просмотр	Пере-	Смена
ди-	Пра-	да-	ле-	За-	Чте-	ди-	Просмотр	Пере-	Смена
рек-	ва	ние	ние	пись	ние	рек-	файлов в	имено-	атрибу-
то-	фай-	фай-	фай-	в	фай-	то-	директо-	вание	тов
рии	ла	ла	ла	файл	ла	рии	рии	файла	файла
d -w-	(400)	-	-	-	-	-	-	-	-
(200)									
d -wx	(400)	+	+	-	+	+	-	+	+
(300)									
d r-	(400)	-	-	-	-	-	+	-	-
(400)									
d r-x	(400)	-	-	-	+	+	+	-	+
(500)									
d rw-	(400)	-	-	-	-	-	+	-	-
(600)									

Figure 5: Рис.5: Установленные права и разрешённые действия

Ход выполнения лабораторной работы

- Заполнение таблицы «Минимально необходимые права для выполнения операций внутри директории»

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d -wx (300)	(000)
Удаление файла	d -wx (300)	(000)
Чтение файла	d -x (100)	(400)
Запись в файл	d -x (100)	(200)
Переименование файла	d -wx (300)	(000)
Создание поддиректории	d -wx (300)	(000)
Удаление поддиректории	d -wx (300)	(000)

Figure 6: Рис.6: Минимально необходимые права для выполнения операций внутри директории

- В ходе выполнения данной лабораторной работы я приобрела практические навыки работы в консоли с атрибутами файлов, закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux