

Лабораторная работа №2

Основы информационной безопасности

Мишина А. А.

28 февраля 2024

- Мишина Анастасия Алексеевна
- НПИбд-02-22

Выполнение лабораторной 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.

Создание пользователя guest

```
[aamishina@aamishina ~]$ su -  
Password:  
[root@aamishina ~]# useradd guest  
[root@aamishina ~]# su guest  
[guest@aamishina root]$ su -  
Password:  
Last login: Wed Feb 28 00:33:57 MSK 2024 on pts/0  
[root@aamishina ~]# passwd guest  
Changing password for user guest.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@aamishina ~]# su guest  
[guest@aamishina root]$ pwd  
/root  
[guest@aamishina root]$ cd ~  
[guest@aamishina ~]$ pwd  
/home/guest  
[guest@aamishina ~]$ whoami  
guest  
[guest@aamishina ~]$ █
```

Рис. 1: Создание пользователя, определение домашнего каталога

```
[guest@aamishina ~]$ whoami
guest
[guest@aamishina ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unc
onfined_t:s0-s0:c0.c1023
[guest@aamishina ~]$ groups
guest
[guest@aamishina ~]$
```

Рис. 2: Команды id и groups

```
[guest@aamishina ~]$ 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 Users:/:/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
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
rtkit:x:112:112:RealtimeKit:/proc:/sbin/nologin
pipewire:x:907:903:Pipewire System Daemons:/var/run/pipewire:/sbin/nologin
sssd:x:996:992:User for sssd:/:/sbin/nologin
libstoragemgmt:x:998:990:daemon account for libstoragemgmt:/:usr/sbin/nologin
systemd-oom:x:989:989:systemd Userspace OOM Killer:/:usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/:usr/sbin/nologin
geoclue:x:988:987:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:987:986:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-ws-instance:x:986:985:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:985:984:User for flatpak system helper:/:/sbin/nologin
colord:x:984:983:User for colord:/var/lib/colord:/sbin/nologin
setroubleshoot:x:983:982:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
clevis:x:982:981:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
gdm:x:42:42:/:/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:981:980:/:run/gnome-initial-setup:/sbin/nologin
design:x:980:979:Group for the design signing daemon:/run/design:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:379:978:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:976:977:dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
aamishina:x:1000:1000:aamishina:/home/aamishina:/bin/bash
guest:x:1001:1001:/:home/guest:/bin/bash
[guest@aamishina ~]$
```

Рис. 3: Просмотр /etc/passwd

Директории и поддиректории

```
[guest@aamishina ~]$  
[guest@aamishina ~]$ ls -l /home/  
total 4  
drwx-----. 14 aamishina aamishina 4096 Feb 16 23:11 aamishina  
drwx-----.  4 guest      guest      92 Feb 28 00:34 guest  
[guest@aamishina ~]$  
[guest@aamishina ~]$  
[guest@aamishina ~]$  
[guest@aamishina ~]$ lsattr /home  
lsattr: Permission denied While reading flags on /home/aamishina  
----- /home/guest  
[guest@aamishina ~]$  
[guest@aamishina ~]$
```

Рис. 4: Просмотр существующих директорий, расширенных атрибутов поддиректорий

Создание директории dir1

```
[guest@aamishina ~]$ ls -l /home/guest/  
total 0  
drwxr-xr-x. 2 guest guest 6 Feb 28 00:42 dir1  
[guest@aamishina ~]$  
[guest@aamishina ~]$  
[guest@aamishina ~]$  
[guest@aamishina ~]$ lsattr /home/guest  
----- /home/guest/dir1
```

Рис. 5: Права доступа новой директории dir1

Изменение прав доступа dir1

```
[guest@aamishina ~]$  
[guest@aamishina ~]$ chmod 000 dir1  
[guest@aamishina ~]$ ls -l  
total 0  
d------. 2 guest guest 6 Feb 28 00:42 dir1  
[guest@aamishina ~]$  
[guest@aamishina ~]$  
[guest@aamishina ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Permission denied  
[guest@aamishina ~]$ ls -l /home/guest/dir1  
ls: cannot open directory '/home/guest/dir1': Permission denied  
[guest@aamishina ~]$
```

Рис. 6: Снятие прав доступа новой директории dir1

Операции для заполнения таблиц

```
[guest@aamishina ~]$ chmod 200 dir1
[guest@aamishina ~]$ ls -l
total 0
d-w-----. 2 guest guest 6 Feb 28 00:42 dir1
[guest@aamishina ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@aamishina ~]$ cd dir1
bash: cd: dir1: Permission denied
[guest@aamishina ~]$ touch /home/guest/dir1/file1.txt
touch: cannot touch '/home/guest/dir1/file1.txt': Permission denied
[guest@aamishina ~]$
[guest@aamishina ~]$
[guest@aamishina ~]$ chmod 300 dir1
[guest@aamishina ~]$ ls -l
total 0
d-wx-----. 2 guest guest 6 Feb 28 00:42 dir1
[guest@aamishina ~]$ touch /home/guest/dir1/file1.txt
[guest@aamishina ~]$ echo "test" > /home/guest/dir1/file1.txt
[guest@aamishina ~]$ cat /home/dir1/file1.txt
cat: /home/dir1/file1.txt: No such file or directory
[guest@aamishina ~]$ cd dir1
[guest@aamishina dir1]$
```

Рис. 7: Попытки выполнения операций при разных правах доступа

Операции для заполнения таблиц

```
[guest@aamishina ~]$ chmod 400 dir1
[guest@aamishina ~]$ touch /home/guest/dir1/file2.txt
touch: cannot touch '/home/guest/dir1/file2.txt': Permission denied
[guest@aamishina ~]$ echo "test" > /home/guest/dir1/file2.txt
bash: /home/guest/dir1/file2.txt: Permission denied
[guest@aamishina ~]$ cd dir1
bash: cd: dir1: Permission denied
[guest@aamishina ~]$ chmod 500
chmod: missing operand after '500'
Try 'chmod --help' for more information.
[guest@aamishina ~]$ chmod 500 dir1
[guest@aamishina ~]$ touch /home/guest/dir1/file2.txt
touch: cannot touch '/home/guest/dir1/file2.txt': Permission denied
[guest@aamishina ~]$ echo "test" > /home/guest/dir1/file2.txt
bash: /home/guest/dir1/file2.txt: Permission denied
[guest@aamishina ~]$ cd dir1
[guest@aamishina dir1]$ cd ~
[guest@aamishina ~]$ chmod 600
chmod: missing operand after '600'
Try 'chmod --help' for more information.
[guest@aamishina ~]$ chmod 600 dir1
[guest@aamishina ~]$ touch /home/guest/dir1/file2.txt
touch: cannot touch '/home/guest/dir1/file2.txt': Permission denied
[guest@aamishina ~]$ echo "test" > /home/guest/dir1/file2.txt
bash: /home/guest/dir1/file2.txt: Permission denied
[guest@aamishina ~]$ cd dir1
bash: cd: dir1: Permission denied
[guest@aamishina ~]$ chmod 700 dir1
[guest@aamishina ~]$ touch /home/guest/dir1/file2.txt
[guest@aamishina ~]$ echo "test" > /home/guest/dir1/file2.txt
[guest@aamishina ~]$ cd dir1
[guest@aamishina dir1]$
```

Рис. 8: Попытки выполнения операций при разных правах доступа

Установленные права и разрешенные действия

Таблица 1: Установленные права и разрешенные действия

Права						Смена			
ди- рек- то- рии	Права фай- ла	Создание фай- ла	Удаление фай- ла	Запись в файл	Чтение фай- ла	ди- рек- то- рии	Просмотр файлов и дирек- тории	Переименование файла	Смена атри- бутов файла
000	000	-	-	-	-	-	-	-	-
100	100	-	-	-	-	+	-	-	+
200	200	-	-	-	-	-	-	-	-
300	300	+	+	+	-	+	-	+	+

Установленные права и разрешенные действия

Таблица 2: Установленные права и разрешенные действия

Права ди- рек- то- рии	Права					Смена			
	Права фай- ла	Создание фай- ла	Удаление фай- ла	Запись в файл	Чтение фай- ла	ди- рек- то- рии	Просмотр файлов и дирек- тории	Переимено- вание файла	Смена атри- бутов файла
400	400	-	-	-	-	-	+	-	-
500	500	-	-	-	+	+	+	-	+
600	600	-	-	-	-	-	+	-	-
700	700	+	+	+	+	+	+	+	+

Таблица 3: Минимальные права для совершения операций

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	300	200
Удаление файла	300	200
Чтение файла	500	400
Запись в файл	300	200
Переименование файла	300	200
Создание поддиректории	300	300
Удаление поддиректории	300	300

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