

Презентация по второй лабораторной. Предмет - Информационная безопасность.

Попов Олег Павлович¹

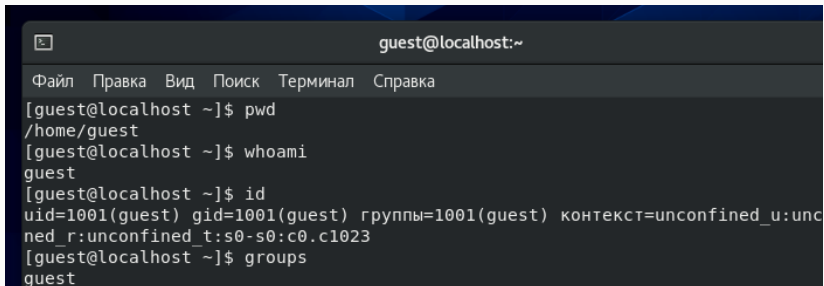
2021, 18 Сентября – 18 Сентября

¹RUDN University, Moscow, Russian Federation

Выполнение лабораторной

Выполнение команд

После создания пользователя guest начинаем выполнять лабораторную:



```
guest@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@localhost ~]$ pwd  
/home/guest  
[guest@localhost ~]$ whoami  
guest  
[guest@localhost ~]$ id  
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unc  
ned_r:unconfined_t:s0-s0:c0.c1023  
[guest@localhost ~]$ groups  
guest
```

Выполнение лабораторной

```
[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
dbus:x:81:81:System message bus:/:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
systemd-resolve:x:193:193:systemd Resolver:/:/sbin/nologin
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin
polkitd:x:998:996:User for polkitd:/:/sbin/nologin
geoclue:x:997:995:User for geoclue:/var/lib/geoclue:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
```

Выполнение лабораторной

```
pipewire:x:996:992:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
libstoragemgmt:x:995:989:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
qemu:x:107:107:qemu user:/:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
unbound:x:994:988:Unbound DNS resolver:/etc/unbound:/sbin/nologin
gluster:x:993:987:GlusterFS daemons:/run/gluster:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
saslauth:x:992:76:Saslauthd user:/run/saslauthd:/sbin/nologin
dnsmasq:x:985:985:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
radvd:x:75:75:radvd user:/:/sbin/nologin
sssd:x:984:984:User for sssd:/:/sbin/nologin
cockpit-ws:x:983:982:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:982:981:User for cockpit-ws instances:/nonexisting:/sbin/nologin
chrony:x:981:980::/var/lib/chrony:/sbin/nologin
colord:x:980:979:User for colord:/var/lib/colord:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
setroubleshoot:x:979:978::/var/lib/setroubleshoot:/sbin/nologin
flatpak:x:978:977:User for flatpak system helper:/:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
clevis:x:977:976:Clevis Decryption Framework unprivileged user:/var/cache/clevis
```

Выполнение лабораторной

```
clevis:x:977:976:Clevis Decryption Framework unprivileged user:/var/cache/clevis  
:/sbin/nologin  
gnome-initial-setup:x:976:975:./run/gnome-initial-setup:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin  
tcpdump:x:72:72:./:/sbin/nologin  
popovoleg:x:1000:1000:popovoleg:/home/popovoleg:/bin/bash  
guest:x:1001:1001:./home/guest:/bin/bash  
[guest@localhost ~]$ cat /etc/passwd | grep guest  
guest:x:1001:1001:./home/guest:/bin/bash
```

Выполнение лабораторной

```
[guest@localhost ~]$ ls -l /home/
итого 8
drwx-----. 15 guest      guest      4096 окт  2 15:11 guest
drwx-----. 15 popovoleg popovoleg 4096 окт  2 15:08 popovoleg
[guest@localhost ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/popovoleg
----- /home/guest
[guest@localhost ~]$ lsattr /home/
lsattr: Отказано в доступе While reading flags on /home/popovoleg
----- /home/guest
[guest@localhost ~]$ mkdir dir1
[guest@localhost ~]$ ls -l /home/
итого 8
drwx-----. 16 guest      guest      4096 окт  2 15:18 guest
drwx-----. 15 popovoleg popovoleg 4096 окт  2 15:08 popovoleg
[guest@localhost ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/popovoleg
----- /home/guest
[guest@localhost ~]$ chmod 000 dir1
[guest@localhost ~]$ ls -l /home/
итого 8
drwx-----. 16 guest      guest      4096 окт  2 15:18 guest
```

Выполнение лабораторной

```
[guest@localhost ~]$ ls -l /home/
итого 8
drwx-----. 16 guest      guest      4096 окт  2 15:18 guest
drwx-----. 15 popovoleg popovoleg 4096 окт  2 15:08 popovoleg
[guest@localhost ~]$ ls -l
итого 0
d------. 2 guest guest 6 окт  2 15:18  dir1
drwxr-xr-x. 2 guest guest 6 окт  2 15:11  Видео
drwxr-xr-x. 2 guest guest 6 окт  2 15:11  Документы
drwxr-xr-x. 2 guest guest 6 окт  2 15:11  Загрузки
drwxr-xr-x. 2 guest guest 6 окт  2 15:11  Изображения
drwxr-xr-x. 2 guest guest 6 окт  2 15:11  Музыка
drwxr-xr-x. 2 guest guest 6 окт  2 15:11  Общедоступные
drwxr-xr-x. 2 guest guest 6 окт  2 15:11  'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 окт  2 15:11  Шаблоны
[guest@localhost ~]$ chmod 777 dir1
[guest@localhost ~]$ ls -l
итого 0
drwxrwxrwx. 2 guest guest 6 окт  2 15:18  dir1
drwxr-xr-x. 2 guest guest 6 окт  2 15:11  Видео
drwxr-xr-x. 2 guest guest 6 окт  2 15:11  Документы
drwxr-xr-x. 2 guest guest 6 окт  2 15:11  Загрузки
drwxr-xr-x. 2 guest guest 6 окт  2 15:11  Изображения
drwxr-xr-x. 2 guest guest 6 окт  2 15:11  Музыка
```


Выполнение лабораторной

```
[guest@localhost ~]$ ls -l
итого 0
drwxrwxrwx. 2 guest guest 6 окт  2 15:18 dir1
drwxr-xr-x. 2 guest guest 6 окт  2 15:11 Видео
drwxr-xr-x. 2 guest guest 6 окт  2 15:11 Документы
drwxr-xr-x. 2 guest guest 6 окт  2 15:11 Загрузки
drwxr-xr-x. 2 guest guest 6 окт  2 15:11 Изображения
drwxr-xr-x. 2 guest guest 6 окт  2 15:11 Музыка
drwxr-xr-x. 2 guest guest 6 окт  2 15:11 Общедоступные
drwxr-xr-x. 2 guest guest 6 окт  2 15:11 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 окт  2 15:11 Шаблоны
[guest@localhost ~]$ lsattr
----- ./Рабочий стол
----- ./Загрузки
----- ./Шаблоны
----- ./Общедоступные
----- ./Документы
----- ./Музыка
----- ./Изображения
----- ./Видео
----- ./dir1
[guest@localhost ~]$ chmod 000 dir1
[guest@localhost ~]$ ls -l
```

Выполнение лабораторной

```
[guest@localhost ~]$ chmod 000 dir1
[guest@localhost ~]$ ls -l
итого 0
d----- . 2 guest guest 6 окт  2 15:18  dir1
drwxr-xr-x. 2 guest guest 6 окт  2 15:11  Видео
drwxr-xr-x. 2 guest guest 6 окт  2 15:11  Документы
drwxr-xr-x. 2 guest guest 6 окт  2 15:11  Загрузки
drwxr-xr-x. 2 guest guest 6 окт  2 15:11  Изображения
drwxr-xr-x. 2 guest guest 6 окт  2 15:11  Музыка
drwxr-xr-x. 2 guest guest 6 окт  2 15:11  Общедоступные
drwxr-xr-x. 2 guest guest 6 окт  2 15:11  'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 окт  2 15:11  Шаблоны
[guest@localhost ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@localhost ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе
[guest@localhost ~]$ +
```

Выполнение лабораторной

Права дир.	Права файла	Создание файла	Удаление файла	Чтение файла	Запись в файл	Переим. файла	Создание поддир.	Удаление поддир.
000	000	-	-	-	-	-	-	-
100	000	-	-	-	-	-	-	-
200	000	-	-	-	-	-	-	-
300	000	+	-	-	-	-	+	+
400	000	-	-	-	-	-	-	-
500	000	-	-	-	-	-	-	-
600	000	-	-	-	-	-	-	-
700	000	+	-	-	-	-	+	+
000	100	-	-	-	-	-	-	-
100	100	-	-	-	-	-	-	-
200	100	-	-	-	-	-	-	-
300	100	+	+	-	-	+	+	+
400	100	-	-	-	-	-	-	-
500	100	-	-	-	-	-	-	-
600	100	-	-	-	-	-	-	-
700	100	+	+	-	-	+	+	+
000	200	-	-	-	-	-	-	-
100	200	-	-	-	-	-	-	-
200	200	-	-	-	-	-	-	-
300	200	+	+	-	+	+	+	+
400	200	-	-	-	-	-	-	-
500	200	-	-	-	-	-	-	-
600	200	-	-	-	-	-	-	-
700	200	+	+	-	+	+	+	+

Выполнение лабораторной

000	300	-	-	-	-	-	-	-
100	300	-	-	-	-	-	-	-
200	300	-	-	-	-	-	-	-
300	300	+	+	-	+	+	+	+
400	300	-	-	-	-	-	-	-
500	300	-	-	-	-	-	-	-
600	300	-	-	-	-	-	-	-
700	300	+	+	-	+	+	+	+
000	400	-	-	-	-	-	-	-
100	400	-	-	-	-	-	-	-
200	400	-	-	-	-	-	-	-
300	400	+	+	+	-	+	+	+
400	400	-	-	-	-	-	-	-
500	400	-	-	-	-	-	-	-
600	400	-	-	-	-	-	-	-
700	400	+	+	+	-	+	+	+
000	500	-	-	-	-	-	-	-
100	500	-	-	-	-	-	-	-
200	500	-	-	-	-	-	-	-
300	500	+	+	+	-	+	+	+
400	500	-	-	-	-	-	-	-
500	500	-	-	-	-	-	-	-
600	500	-	-	-	-	-	-	-
700	500	+	+	+	-	+	+	+
000	600	-	-	-	-	-	-	-
100	600	-	-	-	-	-	-	-

Выполнение лабораторной

200	600	-	-	-	-	-	-	-
300	600	+	+	+	+	+	+	+
400	600	-	-	-	-	-	-	-
500	600	-	-	-	-	-	-	-
600	600	-	-	-	-	-	-	-
700	600	+	+	+	+	+	+	+
000	700	-	-	-	-	-	-	-
100	700	-	-	-	-	-	-	-
200	700	-	-	-	-	-	-	-
300	700	+	+	+	+	+	+	+
400	700	-	-	-	-	-	-	-
500	700	-	-	-	-	-	-	-
600	700	-	-	-	-	-	-	-
700	700	+	+	+	+	+	+	+

Выполнение лабораторной

	Минимальные права директории	Минимальные права файла
Создание файла	300	000
Удаление файла	300	100
Чтение файла	300	400
Запись файла	300	200
Переименование файла	300	100
Создание поддиректории	300	000
Удаление поддиректории	300	000