OTUS
HomeWorks

Домашняя работа на тему:
«Обзор встроенных механизмов защиты в Linux»

Цель второй домашней работы – освоение практических примеров использования chroot, apparmor, pam.d, polkit.

Для реализации поставленной цели был взят ***Vagrantfile*** из материалов и развёрнута лабораторная среда, представленная набором из
2-х виртуальных машин: ***CentOS*** и ***Ubuntu***.

labuzhskiy@MINT-LIN-CIN-X64 ~/.vagrant.d/boxes/4lesson-dz $ vagrant ssh centos
Last login: Sun Sep 1 12:17:41 2019 from 10.0.2.2

Выполнение поставленных задач начал с изучение policykit-1:

polkit:

1. Знакомство с системой.
[vagrant@centos ~]$ ls -l /dev/disk
total 0
drwxr-xr-x. 2 root root 100 Sep 1 11:54 by-id
drwxr-xr-x. 2 root root 100 Sep 1 11:54 by-path
drwxr-xr-x. 2 root root 60 Sep 1 11:54 by-uuid
[vagrant@centos ~]$ ls -l /dev/disk/by-uuid
total 0
lrwxrwxrwx. 1 root root 10 Sep 1 11:54 8ac075e3-1124-4bb6-bef7-a6811bf8b870 -> ../../sda1
[vagrant@centos ~]$ ls -l /dev/
total 0
crw-------. 1 root root   10, 235 Sep 1 11:54 autofs
drwxr-xr-x. 2 root root   100 Sep 1 11:54 block
drwxr-xr-x. 2 root root   80 Sep 1 11:54 bsg
crw-------. 1 root root   10, 234 Sep 1 11:54 btrfs-control
drwxr-xr-x. 2 root root   2580 Sep 1 11:54 char
crw-------. 1 root root   5,   1 Sep 1 11:54 console
lrwxrwxrwx. 1 root root   11 Sep 1 11:54 core -> /proc/kcore
drwxr-xr-x. 3 root root   60 Sep 1 11:54 cpu
crw-------. 1 root root   10, 61 Sep 1 11:54 cpu_dma_latency
crw-------. 1 root root   10, 62 Sep 1 11:54 crash
drwxr-xr-x. 5 root root   100 Sep 1 11:54 disk
lrwxrwxrwx. 1 root root   13 Sep 1 11:54 fd -> /proc/self/fd
crw-rw-rw-. 1 root root   1,   7 Sep 1 11:54 full
crw-rw-rw-. 1 root root   10, 229 Sep 1 11:54 fuse
crw-------. 1 root root   10, 228 Sep 1 11:54 hpet
drwxr-xr-x. 2 root root   0 Sep 1 11:54 hugepages
crw-------. 1 root root   10, 183 Sep 1 11:54 hwrng
lrwxrwxrwx. 1 root root   25 Sep 1 11:54 initctl -> /run/systemd/initctl/fifo
drwxr-xr-x. 3 root root   220 Sep 1 11:54 input
crw-r--r--. 1 root root   1, 11 Sep 1 11:54 kmsg
srw-rw-rw-. 1 root root   0 Sep 1 11:54 log

```
crw-rw----. 1 root disk     10, 237 Sep  1 11:54 loop-control
drwxr-xr-x. 2 root root           60 Sep  1 11:54 mapper
crw-------. 1 root root     10, 227 Sep  1 11:54 mcelog
crw-r-----. 1 root kmem      1,   1 Sep  1 11:54 mem
drwxrwxrwt. 2 root root           40 Sep  1 11:54 mqueue
drwxr-xr-x. 2 root root           60 Sep  1 11:54 net
crw-------. 1 root root     10,  60 Sep  1 11:54 network_latency
crw-------. 1 root root     10,  59 Sep  1 11:54 network_throughput
crw-rw-rw-. 1 root root      1,   3 Sep  1 11:54 null
crw-------. 1 root root     10, 144 Sep  1 11:54 nvram
crw-------. 1 root root      1,  12 Sep  1 11:54 oldmem
crw-r-----. 1 root kmem      1,   4 Sep  1 11:54 port
crw-------. 1 root root    108,   0 Sep  1 11:54 ppp
crw-rw-rw-. 1 root tty       5,   2 Sep  1 13:00 ptmx
drwxr-xr-x. 2 root root           0 Sep  1 11:54 pts
crw-rw-rw-. 1 root root      1,   8 Sep  1 11:54 random
drwxr-xr-x. 2 root root           60 Sep  1 11:54 raw
lrwxrwxrwx. 1 root root           4 Sep  1 11:54 rtc -> rtc0
crw-------. 1 root root    252,   0 Sep  1 11:54 rtc0
brw-rw----. 1 root disk      8,   0 Sep  1 11:54 sda
brw-rw----. 1 root disk      8,   1 Sep  1 11:54 sda1
brw-rw----. 1 root disk      8,  16 Sep  1 11:54 sdb
crw-rw----. 1 root disk     21,   0 Sep  1 11:54 sg0
crw-rw----. 1 root disk     21,   1 Sep  1 11:54 sg1
drwxrwxrwt. 2 root root           40 Sep  1 11:54 shm
crw-------. 1 root root     10, 231 Sep  1 11:54 snapshot
drwxr-xr-x. 3 root root          180 Sep  1 11:54 snd
lrwxrwxrwx. 1 root root          15 Sep  1 11:54 stderr -> /proc/self/fd/2
lrwxrwxrwx. 1 root root          15 Sep  1 11:54 stdin -> /proc/self/fd/0
lrwxrwxrwx. 1 root root          15 Sep  1 11:54 stdout -> /proc/self/fd/1
crw-rw-rw-. 1 root tty       5,   0 Sep  1 11:54 tty
crw--w----. 1 root tty       4,   0 Sep  1 11:54 tty0
crw--w----. 1 root tty       4,   1 Sep  1 11:54 tty1
crw--w----. 1 root tty       4,  10 Sep  1 11:54 tty10
crw--w----. 1 root tty       4,  11 Sep  1 11:54 tty11
crw--w----. 1 root tty       4,  12 Sep  1 11:54 tty12
crw--w----. 1 root tty       4,  13 Sep  1 11:54 tty13
crw--w----. 1 root tty       4,  14 Sep  1 11:54 tty14
crw--w----. 1 root tty       4,  15 Sep  1 11:54 tty15
crw--w----. 1 root tty       4,  16 Sep  1 11:54 tty16
crw--w----. 1 root tty       4,  17 Sep  1 11:54 tty17
crw--w----. 1 root tty       4,  18 Sep  1 11:54 tty18
crw--w----. 1 root tty       4,  19 Sep  1 11:54 tty19
crw--w----. 1 root tty       4,   2 Sep  1 11:54 tty2
crw--w----. 1 root tty       4,  20 Sep  1 11:54 tty20
crw--w----. 1 root tty       4,  21 Sep  1 11:54 tty21
crw--w----. 1 root tty       4,  22 Sep  1 11:54 tty22
crw--w----. 1 root tty       4,  23 Sep  1 11:54 tty23
crw--w----. 1 root tty       4,  24 Sep  1 11:54 tty24
crw--w----. 1 root tty       4,  25 Sep  1 11:54 tty25
crw--w----. 1 root tty       4,  26 Sep  1 11:54 tty26
crw--w----. 1 root tty       4,  27 Sep  1 11:54 tty27
```

```
crw--w----. 1 root tty       4,  28 Sep  1 11:54 tty28
crw--w----. 1 root tty       4,  29 Sep  1 11:54 tty29
crw--w----. 1 root tty       4,   3 Sep  1 11:54 tty3
crw--w----. 1 root tty       4,  30 Sep  1 11:54 tty30
crw--w----. 1 root tty       4,  31 Sep  1 11:54 tty31
crw--w----. 1 root tty       4,  32 Sep  1 11:54 tty32
crw--w----. 1 root tty       4,  33 Sep  1 11:54 tty33
crw--w----. 1 root tty       4,  34 Sep  1 11:54 tty34
crw--w----. 1 root tty       4,  35 Sep  1 11:54 tty35
crw--w----. 1 root tty       4,  36 Sep  1 11:54 tty36
crw--w----. 1 root tty       4,  37 Sep  1 11:54 tty37
crw--w----. 1 root tty       4,  38 Sep  1 11:54 tty38
crw--w----. 1 root tty       4,  39 Sep  1 11:54 tty39
crw--w----. 1 root tty       4,   4 Sep  1 11:54 tty4
crw--w----. 1 root tty       4,  40 Sep  1 11:54 tty40
crw--w----. 1 root tty       4,  41 Sep  1 11:54 tty41
crw--w----. 1 root tty       4,  42 Sep  1 11:54 tty42
crw--w----. 1 root tty       4,  43 Sep  1 11:54 tty43
crw--w----. 1 root tty       4,  44 Sep  1 11:54 tty44
crw--w----. 1 root tty       4,  45 Sep  1 11:54 tty45
crw--w----. 1 root tty       4,  46 Sep  1 11:54 tty46
crw--w----. 1 root tty       4,  47 Sep  1 11:54 tty47
crw--w----. 1 root tty       4,  48 Sep  1 11:54 tty48
crw--w----. 1 root tty       4,  49 Sep  1 11:54 tty49
crw--w----. 1 root tty       4,   5 Sep  1 11:54 tty5
crw--w----. 1 root tty       4,  50 Sep  1 11:54 tty50
crw--w----. 1 root tty       4,  51 Sep  1 11:54 tty51
crw--w----. 1 root tty       4,  52 Sep  1 11:54 tty52
crw--w----. 1 root tty       4,  53 Sep  1 11:54 tty53
crw--w----. 1 root tty       4,  54 Sep  1 11:54 tty54
crw--w----. 1 root tty       4,  55 Sep  1 11:54 tty55
crw--w----. 1 root tty       4,  56 Sep  1 11:54 tty56
crw--w----. 1 root tty       4,  57 Sep  1 11:54 tty57
crw--w----. 1 root tty       4,  58 Sep  1 11:54 tty58
crw--w----. 1 root tty       4,  59 Sep  1 11:54 tty59
crw--w----. 1 root tty       4,   6 Sep  1 11:54 tty6
crw--w----. 1 root tty       4,  60 Sep  1 11:54 tty60
crw--w----. 1 root tty       4,  61 Sep  1 11:54 tty61
crw--w----. 1 root tty       4,  62 Sep  1 11:54 tty62
crw--w----. 1 root tty       4,  63 Sep  1 11:54 tty63
crw--w----. 1 root tty       4,   7 Sep  1 11:54 tty7
crw--w----. 1 root tty       4,   8 Sep  1 11:54 tty8
crw--w----. 1 root tty       4,   9 Sep  1 11:54 tty9
crw-rw----. 1 root dialout   4,  64 Sep  1 11:54 ttyS0
crw-rw----. 1 root dialout   4,  65 Sep  1 11:54 ttyS1
crw-rw----. 1 root dialout   4,  66 Sep  1 11:54 ttyS2
crw-rw----. 1 root dialout   4,  67 Sep  1 11:54 ttyS3
crw-------. 1 root root     10, 239 Sep  1 11:54 uhid
crw-------. 1 root root     10, 223 Sep  1 11:54 uinput
crw-rw-rw-. 1 root root      1,   9 Sep  1 11:54 urandom
crw-------. 1 root root    247,   0 Sep  1 11:54 usbmon0
crw-rw----. 1 root tty       7,   0 Sep  1 11:54 vcs
```

```
crw-rw----. 1 root tty      7,   1 Sep  1 11:54 vcs1
crw-rw----. 1 root tty      7,   2 Sep  1 11:54 vcs2
crw-rw----. 1 root tty      7,   3 Sep  1 11:54 vcs3
crw-rw----. 1 root tty      7,   4 Sep  1 11:54 vcs4
crw-rw----. 1 root tty      7,   5 Sep  1 11:54 vcs5
crw-rw----. 1 root tty      7,   6 Sep  1 11:54 vcs6
crw-rw----. 1 root tty      7, 128 Sep  1 11:54 vcsa
crw-rw----. 1 root tty      7, 129 Sep  1 11:54 vcsa1
crw-rw----. 1 root tty      7, 130 Sep  1 11:54 vcsa2
crw-rw----. 1 root tty      7, 131 Sep  1 11:54 vcsa3
crw-rw----. 1 root tty      7, 132 Sep  1 11:54 vcsa4
crw-rw----. 1 root tty      7, 133 Sep  1 11:54 vcsa5
crw-rw----. 1 root tty      7, 134 Sep  1 11:54 vcsa6
drwxr-xr-x. 2 root root        60 Sep  1 11:54 vfio
crw-------. 1 root root    10,  63 Sep  1 11:54 vga_arbiter
crw-------. 1 root root    10, 137 Sep  1 11:54 vhci
crw-------. 1 root root    10, 238 Sep  1 11:54 vhost-net
crw-rw-rw-. 1 root root     1,   5 Sep  1 11:54 zero
[vagrant@centos ~]$ mount
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime,seclabel)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
devtmpfs on /dev type devtmpfs (rw,nosuid,seclabel,size=112408k,nr_inodes=28102,mode=755)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,seclabel)
devpts on /dev/pts type devpts
(rw,nosuid,noexec,relatime,seclabel,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,nodev,seclabel,mode=755)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,seclabel,mode=755)
cgroup on /sys/fs/cgroup/systemd type cgroup
(rw,nosuid,nodev,noexec,relatime,seclabel,xattr,release_agent=/usr/lib/systemd/systemd-cgroups-
agent,name=systemd)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup
(rw,nosuid,nodev,noexec,relatime,seclabel,net_prio,net_cls)
cgroup on /sys/fs/cgroup/hugetlb
 type cgroup (rw,nosuid,nodev,noexec,relatime,seclabel,hugetlb)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,seclabel,memory)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup
(rw,nosuid,nodev,noexec,relatime,seclabel,cpuacct,cpu)
cgroup on /sys/fs/cgroup/perf_event type cgroup
(rw,nosuid,nodev,noexec,relatime,seclabel,perf_event)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,seclabel,freezer)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,seclabel,pids)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,seclabel,devices)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,seclabel,blkio)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,seclabel,cpuset)
configfs on /sys/kernel/config type configfs (rw,relatime)
/dev/sda1 on / type xfs (rw,relatime,seclabel,attr2,inode64,noquota)
selinuxfs on /sys/fs/selinux type selinuxfs (rw,relatime)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs
(rw,relatime,fd=29,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=14600)
mqueue on /dev/mqueue type mqueue (rw,relatime,seclabel)
```

hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,seclabel)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw,relatime)
tmpfs on /run/user/1000 type tmpfs
(rw,nosuid,nodev,relatime,seclabel,size=24088k,mode=700,uid=1000,gid=1000)
[vagrant@centos ~]$ mount -o rw /dev/sdb /mnt
mount: only root can use "--options" option
[vagrant@centos ~]$ sudo!!
sudomount -o rw /dev/sdb /mnt
-bash: sudomount: command not found
[vagrant@centos ~]$ ls -l /dev/disk/by-uuid
total 0
lrwxrwxrwx. 1 root root 10 Sep 1 11:54 8ac075e3-1124-4bb6-bef7-a6811bf8b870 -> ../../sda1
[vagrant@centos ~]$ cat /etc/fstab

#
/etc/fstab
Created by anaconda on Sat Jun 1 17:13:31 2019
#
Accessible filesystems, by reference, are maintained under '/dev/disk'
See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=8ac075e3-1124-4bb6-bef7-a6811bf8b870 /   xfs   defaults   0 0
/swapfile none swap defaults 0 0
[vagrant@centos ~]$ cat /etc/groups
cat: /etc/groups: No such file or directory
[vagrant@centos ~]$ cat /etc/group
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:
cdrom:x:11:
mail:x:12:postfix
man:x:15:
dialout:x:18:
floppy:x:19:
games:x:20:
tape:x:33:
video:x:39:
ftp:x:50:
lock:x:54:
audio:x:63:
nobody:x:99:
users:x:100:
utmp:x:22:

utempter:x:35:
input:x:999:
systemd-journal:x:190:
systemd-network:x:192:
dbus:x:81:
polkitd:x:998:
rpc:x:32:
printadmin:x:997:
ssh_keys:x:996:
rpcuser:x:29:
nfsnobody:x:65534:
sshd:x:74:
postdrop:x:90:
postfix:x:89:
chrony:x:995:
vagrant:x:1000:vagrant
otus:x:1001:
otus2:x:1002:
otus3:x:1003:

2. добавил группу red
[vagrant@centos ~]$ sudo groupadd red
проверил появилась ли она
[vagrant@centos ~]$ cat /etc/group
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:
cdrom:x:11:
mail:x:12:postfix
man:x:15:
dialout:x:18:
floppy:x:19:
games:x:20:
tape:x:33:
video:x:39:
ftp:x:50:
lock:x:54:
audio:x:63:
nobody:x:99:
users:x:100:
utmp:x:22:
utempter:x:35:
input:x:999:
systemd-journal:x:190:

systemd-network:x:192:
dbus:x:81:
polkitd:x:998:
rpc:x:32:
printadmin:x:997:
ssh_keys:x:996:
rpcuser:x:29:
nfsnobody:x:65534:
sshd:x:74:
postdrop:x:90:
postfix:x:89:
chrony:x:995:
vagrant:x:1000:vagrant
otus:x:1001:
otus2:x:1002:
otus3:x:1003:
red:x:1004:

3. добавил пользователя otus в группу red:

[vagrant@centos ~]$ sudo usermod -aG red otus

[vagrant@centos ~]$ sudo vi /etc/polkit-1/rules.d/30-udisk2.rules

написал правило вида:
```
polkit.addRule(function(action, subject) {
   if (action.id == "org.freedesktop.udisks2.filesystem-mount-system" &&
   subject.isInGroup("red") && subject.active) {
   return polkit.Result.YES;
   }
});
```

сохранил в файл 30-udisk2.rules

создал файл 10-udisk2-filesystem-mount.pkla:

```
[Mount a system-internal device]
Identity=*
Action=org.freedesktop.udisks2*
ResultActive=yes
```

4. разметил новый диск, которым далее должен оперировать otus:

```
Command (m for help): m
Command action
  a   toggle a bootable flag
  b   edit bsd disklabel
  c   toggle the dos compatibility flag
  d   delete a partition
  g   create a new empty GPT partition table
  G   create an IRIX (SGI) partition table
```

```
  l   list known partition types
  m   print this menu
  n   add a new partition
  o   create a new empty DOS partition table
  p   print the partition table
  q   quit without saving changes
  s   create a new empty Sun disklabel
  t   change a partition's system id
  u   change display/entry units
  v   verify the partition table
  w   write table to disk and exit
  x   extra functionality (experts only)
```

Command (m for help): g
Building a new GPT disklabel (GUID: 2C7F528B-B8D0-4A87-82E7-230976D4FDC5)

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.

```
[root@centos ~]# parted /dev/sdb
GNU Parted 3.1
Using /dev/sdb
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted) mkpart primary ext4 5GiB 100%
Warning: You requested a partition from 5047MB to 5369MB (sectors 9856614..10485759).
The closest location we can manage is 5047MB to 5047MB (sectors 9856613..9856613).
Is this still acceptable to you?
Yes/No? y
Warning: The resulting partition is not properly aligned for best performance.
Ignore/Cancel? i
(parted) quit
Information: You may need to update /etc/fstab.

[root@centos ~]# mkfs.ext4 /dev/sdb1
mke2fs 1.42.9 (28-Dec-2013)
Filesystem label=
OS type: Linux
Block size=1024 (log=0)
Fragment size=1024 (log=0)
Stride=0 blocks, Stripe width=0 blocks
78936 inodes, 314556 blocks
15727 blocks (5.00%) reserved for the super user
First data block=1
Maximum filesystem blocks=33947648
39 block groups
8192 blocks per group, 8192 fragments per group
2024 inodes per group
Superblock backups stored on blocks:
```

8193, 24577, 40961, 57345, 73729, 204801, 221185

Allocating group tables: done
Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done

5. создал директорию, в которую будет монтироваться hdd sdb1
[root@centos ~]# mkdir /media/sdb1

6. назначил права на каталог для монтирования sdb1:

[root@centos ~]# chown otus /media/sdb1
[vagrant@centos etc]$ sudo yum install mc -y
[vagrant@centos etc]$ sudo -u otus mc

[otus@centos sdb1]$ touch readme.txt

[otus@centos sdb1]$ mcedit readme.txt

[otus@centos media]$ umount /dev/sdb1
umount: /dev/sdb1: umount failed: Operation not permitted

[vagrant@centos ~]$ sudo usermod -G red otus
ещё раз убедился, что пользователь в группе red

[vagrant@centos ~]$ sudo -u otus groups
otus red
попытка монтирования
[vagrant@centos ~]$ sudo -u otus mount /dev/sdb1 /media/sdb1
***mount: only root can do that* неудача.**
проверил разрешения:
[root@centos rules.d]# ls -l *.rules
-rw-r--r--. 1 root root 237 Sep 2 16:45 30-mount-udisk2.rules
-rw-r--r--. 1 root root 974 Jun 9 2014 49-polkit-pkla-compat.rules
-rw-r--r--. 1 root root 326 Apr 29 2013 50-default.rules

7. Убедился, Что права на каталог, в который собираемся выполнять монтирование, подходящие:
[vagrant@centos ~]$ sudo chown otus:red /dev/sdb1
[vagrant@centos ~]$ ls -l /dev/sdb1
brw-rw----. 1 otus red 8, 17 Sep 2 15:50 /dev/sdb1
[vagrant@centos ~]$ sudo -u otus mount /dev/sdb1 /media/sdb1
mount: only root can do that
-- не удалось.

Почему?
8. Проверил pkaction
[vagrant@centos ~]$ pkaction
com.redhat.tuned.active_profile
com.redhat.tuned.auto_profile

com.redhat.tuned.disable
com.redhat.tuned.is_running
com.redhat.tuned.log_capture_finish
com.redhat.tuned.log_capture_start
com.redhat.tuned.profile_info
com.redhat.tuned.profile_mode
com.redhat.tuned.profiles
com.redhat.tuned.profiles2
com.redhat.tuned.recommend_profile
com.redhat.tuned.reload
com.redhat.tuned.start
com.redhat.tuned.stop
com.redhat.tuned.switch_profile
com.redhat.tuned.verify_profile
com.redhat.tuned.verify_profile_ignore_missing
org.fedoraproject.FirewallD1.all
org.fedoraproject.FirewallD1.config
org.fedoraproject.FirewallD1.config.info
org.fedoraproject.FirewallD1.direct
org.fedoraproject.FirewallD1.direct.info
org.fedoraproject.FirewallD1.info
org.fedoraproject.FirewallD1.policies
org.fedoraproject.FirewallD1.policies.info
org.fedoraproject.setroubleshootfixit.write
org.freedesktop.NetworkManager.checkpoint-rollback
org.freedesktop.NetworkManager.enable-disable-connectivity-check
org.freedesktop.NetworkManager.enable-disable-network
org.freedesktop.NetworkManager.enable-disable-statistics
org.freedesktop.NetworkManager.enable-disable-wifi
org.freedesktop.NetworkManager.enable-disable-wimax
org.freedesktop.NetworkManager.enable-disable-wwan
org.freedesktop.NetworkManager.network-control
org.freedesktop.NetworkManager.reload
org.freedesktop.NetworkManager.settings.modify.global-dns
org.freedeskt
op.NetworkManager.settings.modify.hostname
org.freedesktop.NetworkManager.settings.modify.own
org.freedesktop.NetworkManager.settings.modify.system
org.freedesktop.NetworkManager.sleep-wake
org.freedesktop.NetworkManager.wifi.share.open
org.freedesktop.NetworkManager.wifi.share.protected
org.freedesktop.hostname1.set-hostname
org.freedesktop.hostname1.set-machine-info
org.freedesktop.hostname1.set-static-hostname
org.freedesktop.import1.pull
org.freedesktop.locale1.set-keyboard
org.freedesktop.locale1.set-locale
org.freedesktop.login1.attach-device
org.freedesktop.login1.flush-devices
org.freedesktop.login1.hibernate
org.freedesktop.login1.hibernate-ignore-inhibit
org.freedesktop.login1.hibernate-multiple-sessions

org.freedesktop.login1.inhibit-block-idle
org.freedesktop.login1.inhibit-block-shutdown
org.freedesktop.login1.inhibit-block-sleep
org.freedesktop.login1.inhibit-delay-shutdown
org.freedesktop.login1.inhibit-delay-sleep
org.freedesktop.login1.inhibit-handle-hibernate-key
org.freedesktop.login1.inhibit-handle-lid-switch
org.freedesktop.login1.inhibit-handle-power-key
org.freedesktop.login1.inhibit-handle-suspend-key
org.freedesktop.login1.power-off
org.freedesktop.login1.power-off-ignore-inhibit
org.freedesktop.login1.power-off-multiple-sessions
org.freedesktop.login1.reboot
org.freedesktop.login1.reboot-ignore-inhibit
org.freedesktop.login1.reboot-multiple-sessions
org.freedesktop.login1.set-user-linger
org.freedesktop.login1.suspend
org.freedesktop.login1.suspend-ignore-inhibit
org.freedesktop.login1.suspend-multiple-sessions
org.freedesktop.machine1.login
org.freedesktop.policykit.exec
org.freedesktop.systemd1.manage-unit-files
org.freedesktop.systemd1.manage-units
org.freedesktop.systemd1.reload-daemon
org.freedesktop.systemd1.reply-password
org.freedesktop.timedate1.set-local-rtc
org.freedesktop.timedate1.set-ntp
org.freedesktop.timedate1.set-time
org.freedesktop.timedate1.set-timezone
[vagrant@centos ~]$ pkaction --action-id org.freedesktop.udisks2.filesystem-mount-system --verbose
No action with action id org.freedesktop.udisks2.filesystem-mount-system

убедился, что нужный мне action в списке pkaction отсутствует.

9. Разместил файл org.freedesktop.udisks2.policy в каталоге /usr/share/polkit-1/actions/

[root@centos ~]# pkaction
com.redhat.tuned.active_profile
com.redhat.tuned.auto_profile
com.redhat.tuned.disable
com.redhat.tuned.is_running
com.redhat.tuned.log_capture_finish
com.redhat.tuned.log_capture_start
com.redhat.tuned.profile_info
com.redhat.tuned.profile_mode
com.redhat.tuned.profiles
com.redhat.tuned.profiles2
com.redhat.tuned.recommend_profile
com.redhat.tuned.reload
com.redhat.tuned.start
com.redhat.tuned.stop

com.redhat.tuned.switch_profile
com.redhat.tuned.verify_profile
com.redhat.tuned.verify_profile_ignore_missing
org.fedoraproject.FirewallD1.all
org.fedoraproject.FirewallD1.config
org.fedoraproject.FirewallD1.config.info
org.fedoraproject.FirewallD1.direct
org.fedoraproject.FirewallD1.direct.info
org.fedoraproject.FirewallD1.info
org.fedoraproject.FirewallD1.policies
org.fedoraproject.FirewallD1.policies.info
org.fedoraproject.setroubleshootfixit.write
org.freedesktop.NetworkManager.checkpoint-rollback
org.freedesktop.NetworkManager.enable-disable-connectivity-check
org.freedesktop.NetworkManager.enable-disable-network
org.freedesktop.NetworkManager.enable-disable-statistics
org.freedesktop.NetworkManager.enable-disable-wifi
org.freedesktop.NetworkManager.enable-disable-wimax
org.freedesktop.NetworkManager.enable-disable-wwan
org.freedesktop.NetworkManager.network-control
org.freedesktop.NetworkManager.reload
org.freedesktop.NetworkManager.settings.modify.global-dns
org.freedesktop.NetworkManager.settings.modify.hostname
org.freedesktop.NetworkManager.settings.modify.own
org.freedesktop.NetworkManager.settings.modify.system
org.freedesktop.NetworkManager.sleep-wake
org.freedesktop.NetworkManager.wifi.share.open
org.freedesktop.NetworkManager.wifi.share.protected
org.freedesktop.hostname1.set-hostname
org.freedesktop.hostname1.set-machine-info
org.freedesktop.hostname1.set-static-hostname
org.freedesktop.import1.pull
org.freedesktop.locale1.set-keyboard
org.freedesktop.locale1.set-locale
org.freedesktop.login1.attach-device
org.freedesktop.login1.flush-devices
org.freedesktop.login1.hibernate
org.freedesktop.login1.hibernate-ignore-inhibit
org.freedesktop.login1.hibernate-multiple-sessions
org.freedesktop.login1.inhibit-block-idle
org.freedesktop.login1.inhibit-block-shutdown
org.freedesktop.login1.inhibit-block-sleep
org.freedesktop.login1.inhibit-delay-shutdown
org.freedesktop.login1.inhibit-delay-sleep
org.freedesktop.login1.inhibit-handle-hibernate-key
org.freedesktop.login1.inhibit-handle-lid-switch
org.freedesktop.login1.inhibit-handle-power-key
org.freedesktop.login1.inhibit-handle-suspend-key
org.freedesktop.login1.power-off
org.freedesktop.login1.power-off-ignore-inhibit
org.freedesktop.login1.power-off-multiple-sessions
org.freedesktop.login1.reboot

org.freedesktop.login1.reboot-ignore-inhibit
org.freedesktop.login1.reboot-multiple-sessions
org.freedesktop.login1.set-user-linger
org.freedesktop.login1.suspend
org.freedesktop.login1.suspend-ignore-inhibit
org.freedesktop.login1.suspend-multiple-sessions
org.freedesktop.machine1.login
org.freedesktop.policykit.exec
org.freedesktop.systemd1.manage-unit-files
org.freedesktop.systemd1.manage-units
org.freedesktop.systemd1.reload-daemon
org.freedesktop.systemd1.reply-password
org.freedesktop.timedate1.set-local-rtc
org.freedesktop.timedate1.set-ntp
org.freedesktop.timedate1.set-time
org.freedesktop.timedate1.set-timezone
org.freedesktop.udisks2.ata-check-power
org.freedesktop.udisks2.ata-secure-erase
org.freedesktop.udisks2.ata-smart-enable-disable
org.freedesktop.udisks2.ata-smart-selftest
org.freedesktop.udisks2.ata-smart-simulate
org.freedesktop.udisks2.ata-smart-update
org.freedesktop.udisks2.ata-standby
org.freedesktop.udisks2.ata-standby-other-seat
org.freedesktop.udisks2.ata-standby-system
org.freedesktop.udisks2.cancel-job
org.freedesktop.udisks2.cancel-job-other-user
org.freedesktop.udisks2.eject-media
org.freedesktop.udisks2.eject-media-other-seat
org.freedesktop.udisks2.eject-media-system
org.freedesktop.udisks2.encrypted-change-passphrase
org.freedesktop.udisks2.encrypted-change-passphrase-system
org.freedesktop.udisks2.encrypted-lock-others
org.freedesktop.udisks2.encrypted-unlock
org.freedesktop.udisks2.encrypted-unlock-crypttab
org.freedesktop.udisks2.encrypted-unlock-other-seat
org.freedesktop.udisks2.encrypted-unlock-system
org.freedesktop.udisks2.filesystem-fstab
org.freedesktop.udisks2.filesystem-mount
org.freedesktop.udisks2.filesystem-mount-other-seat
org.freedesktop.udisks2.filesystem-mount-system
org.freedesktop.udisks2.filesystem-unmount-others
org.freedesktop.udisks2.loop-delete-others
org.freedesktop.udisks2.loop-modify-others
org.freedesktop.udisks2.loop-setup
org.freedesktop.udisks2.manage-md-raid
org.freedesktop.udisks2.manage-swapspace
org.freedesktop.udisks2.modify-device
org.freedesktop.udisks2.modify-device-other-seat
org.freedesktop.udisks2.modify-device-system
org.freedesktop.udisks2.modify-drive-settings
org.freedesktop.udisks2.modify-system-configuration

org.freedesktop.udisks2.open-device
org.freedesktop.udisks2.open-device-system
org.freedesktop.udisks2.power-off-drive
org.freedesktop.udisks2.power-off-drive-other-seat
org.freedesktop.udisks2.power-off-drive-system
org.freedesktop.udisks2.read-system-configuration-secrets
org.freedesktop.udisks2.rescan

[root@centos ~]# pkaction
com.redhat.tuned.active_profile
com.redhat.tuned.auto_profile
com.redhat.tuned.disable
com.redhat.tuned.is_running
com.redhat.tuned.log_capture_finish
com.redhat.tuned.log_capture_start
com.redhat.tuned.profile_info
com.redhat.tuned.profile_mode
com.redhat.tuned.profiles
com.redhat.tuned.profiles2
com.redhat.tuned.recommend_profile
com.redhat.tuned.reload
com.redhat.tuned.start
com.redhat.tuned.stop
com.redhat.tuned.switch_profile
com.redhat.tuned.verify_profile
com.redhat.tuned.verify_profile_ignore_missing
org.fedoraproject.FirewallD1.all
org.fedoraproject.FirewallD1.config
org.fedoraproject.FirewallD1.config.info
org.fedoraproject.FirewallD1.direct
org.fedoraproject.FirewallD1.direct.info
org.fedoraproject.FirewallD1.info
org.fedoraproject.FirewallD1.policies
org.fedoraproject.FirewallD1.policies.info
org.fedoraproject.setroubleshootfixit.write
org.freedesktop.NetworkManager.checkpoint-rollback
org.freedesktop.NetworkManager.enable-disable-connectivity-check
org.freedesktop.NetworkManager.enable-disable-network
org.freedesktop.NetworkManager.enable-disable-statistics
org.freedesktop.NetworkManager.enable-disable-wifi
org.freedesktop.NetworkManager.enable-disable-wimax
org.freedesktop.NetworkManager.enable-disable-wwan
org.freedesktop.NetworkManager.network-control
org.freedesktop.NetworkManager.reload
org.freedesktop.NetworkManager.settings.modify.global-dns
org.freedesktop.NetworkManager.settings.modify.hostname
org.freedesktop.NetworkManager.settings.modify.own
org.freedesktop.NetworkManager.settings.modify.system
org.freedesktop.NetworkManager.sleep-wake
org.freedesktop.NetworkManager.wifi.share.open
org.freedesktop.NetworkManager.wifi.share.protected

org.freedesktop.hostname1.set-hostname
org.freedesktop.hostname1.set-machine-info
org.freedesktop.hostname1.set-static-hostname
org.freedesktop.import1.pull
org.freedesktop.locale1.set-keyboard
org.freedesktop.locale1.set-locale
org.freedesktop.login1.attach-device
org.freedesktop.login1.flush-devices
org.freedesktop.login1.hibernate
org.freedesktop.login1.hibernate-ignore-inhibit
org.freedesktop.login1.hibernate-multiple-sessions
org.freedesktop.login1.inhibit-block-idle
org.freedesktop.login1.inhibit-block-shutdown
org.freedesktop.login1.inhibit-block-sleep
org.freedesktop.login1.inhibit-delay-shutdown
org.freedesktop.login1.i
nhibit-delay-sleep
org.freedesktop.login1.inhibit-handle-hibernate-key
org.freedesktop.login1.inhibit-handle-lid-switch
org.freedesktop.login1.inhibit-handle-power-key
org.freedesktop.login1.inhibit-handle-suspend-key
org.freedesktop.login1.power-off
org.freedesktop.login1.power-off-ignore-inhibit
org.freedesktop.login1.power-off-multiple-sessions
org.freedesktop.login1.reboot
org.freedesktop.login1.reboot-ignore-inhibit
org.freedesktop.login1.reboot-multiple-sessions
org.freedesktop.login1.set-user-linger
org.freedesktop.login1.suspend
org.freedesktop.login1.suspend-ignore-inhibit
org.freedesktop.login1.suspend-multiple-sessions
org.freedesktop.machine1.login
org.freedesktop.policykit.exec
org.freedesktop.systemd1.manage-unit-files
org.freedesktop.systemd1.manage-units
org.freedesktop.systemd1.reload-daemon
org.freedesktop.systemd1.reply-password
org.freedesktop.timedate1.set-local-rtc
org.freedesktop.timedate1.set-ntp
org.freedesktop.timedate1.set-time
org.freedesktop.timedate1.set-timezone
org.freedesktop.udisks2.ata-check-power
org.freedesktop.udisks2.ata-secure-erase
org.freedesktop.udisks2.ata-smart-enable-disable
org.freedesktop.udisks2.ata-smart-selftest
org.freedesktop.udisks2.ata-smart-simulate
org.freedesktop.udisks2.ata-smart-update
org.freedesktop.udisks2.ata-standby
org.freedesktop.udisks2.ata-standby-other-seat
org.freedesktop.udisks2.ata-standby-system
org.freedesktop.udisks2.cancel-job
org.freedesktop.udisks2.cancel-job-other-user

org.freedesktop.udisks2.eject-media
org.freedesktop.udisks2.eject-media-other-seat
org.freedesktop.udisks2.eject-media-system
org.freedesktop.udisks2.encrypted-change-passphrase
org.freedesktop.udisks2.encrypted-change-passphrase-system
org.freedesktop.udisks2.encrypted-lock-others
org.freedesktop.udisks2.encrypted-unlock
org.freedesktop.udisks2.encrypted-unlock-crypttab
org.freedesktop.udisks2.encrypted-unlock-other-seat
org.freedesktop.udisks2.encrypted-unlock-system
org.freedesktop.udisks2.filesystem-fstab
org.freedesktop.udisks2.filesystem-mount
org.freedesktop.udisks2.filesystem-mount-other-seat
org.freedesktop.udisks2.filesystem-mount-system
org.freedesktop.udisks2.filesystem-unmount-others
org.freedesktop.udisks2.loop-delete-others
org.freedesktop.udisks2.loop-modify-others
org.freedesktop.udisks2.loop-setup
org.freedesktop.udisks2.manage-md-raid
org.freedesktop.udisks2.manage-swapspace
org.freedesktop.udisks2.modify-device
org.freedesktop.udisks2.modify-device-other-seat
org.freedesktop.udisks2.modify-device-system
org.freedesktop.udisks2.modify-drive-settings
org.freedesktop.udisks2.modify-system-configuration
org.freedesktop.udisks2.open-device
org.freedesktop.udisks2.open-device-system
org.freedesktop.udisks2.power-off-drive
org.freedesktop.udisks2.power-off-drive-other-seat
org.freedesktop.udisks2.power-off-drive-system
org.freedesktop.udisks2.read-system-configuration-secrets
org.freedesktop.udisks2.rescan
[root@centos ~]#

11. убедился, что нужные мне action в список pkaction добавились.

12. просмотр журнала с отбором по polkitd показал, что завершена загрузка, компиляция и выполнение 4 правил.
копии наработок выкладываю архивами.
[root@centos rules.d]# tail -n 100 /var/log/secure | grep polkitd
Sep 2 18:07:16 centos polkitd[1556]: Registered Authentication Agent for unix-process:6688:824436 (system bus name :1.68 [/usr/bin/pkttyagent --notify-fd 5 --fallback], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Sep 3 14:57:51 centos polkitd[1556]: Loading rules from directory /etc/polkit-1/rules.d
Sep 3 14:57:51 centos polkitd[1556]: Loading rules from directory /usr/share/polkit-1/rules.d
Sep 3 14:57:51 centos polkitd[1556]: Finished loading, compiling and executing 4 rules
Sep 3 14:57:51 centos polkitd[1556]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
Sep 3 17:23:29 centos polkitd[1556]: Reloading rules
Sep 3 17:23:29 centos polkitd[1556]: Collecting garbage unconditionally...
Sep 3 17:23:29 centos polkitd[1556]: Loading rules from directory /etc/polkit-1/rules.d
Sep 3 17:23:29 centos polkitd[1556]: Loading rules from directory /usr/share/polkit-1/rules.d

Sep 3 17:23:29 centos polkitd[1556]: Finished loading, compiling and executing 4 rules
[root@centos rules.d]#

13. проверил разрешения на выполнение команды mount в системе:
13.1 какие системные утилиты и службы отвечают за выполнение процедуры монтирования устройств в операционной системе, путь их размещения:
[vagrant@centos ~]$ whereis mount
mount: /usr/bin/mount /usr/sbin/mount.fuse /usr/sbin/mount.nfs /usr/sbin/mount.nfs4 /usr/sbin/mount.cifs /usr/share/man/man8/mount.8.gz /usr/share/man/man2/mount.2.gz
13.2 разрешения:
[vagrant@centos ~]$ ll /usr/bin/mount /usr/sbin/mount.fuse /usr/sbin/mount.nfs /usr/sbin/mount.nfs4 /usr/sbin/mount.cifs /usr/share/man/man8/mount.8.gz /usr/share/man/man2/mount.2.gz
-rwxr-xr-x. 1 root root 44320 Mar 14 10:37 /usr/bin/mount
-rwxr-xr-x. 1 root root 41016 Aug 3 2017 /usr/sbin/mount.cifs
-rwxr-xr-x. 1 root root 11368 Oct 30 2018 /usr/sbin/mount.fuse
-rwsr-xr-x. 1 root root 117504 Nov 7 2018 /usr/sbin/mount.nfs
lrwxrwxrwx. 1 root root   9 Jun 1 17:15 /usr/sbin/mount.nfs4 -> mount.nfs
-rw-r--r--. 1 root root   5937 Jun 9 2014 /usr/share/man/man2/mount.2.gz
-rw-r--r--. 1 root root 30554 Mar 14 10:37 /usr/share/man/man8/mount.8.gz

13.3 меняем на нужные нам разрешения:
[root@centos ~]# chmod a+s /usr/bin/mount* /usr/sbin/mount.cifs
проверка себя:
[root@centos ~]# ll /usr/bin/mount /usr/sbin/mount.fuse /usr/sbin/mount.nfs /usr/sbin/mount.nfs4 /usr/sbin/mount.cifs /usr/share/man/man8/mount.8.gz /usr/share/man/man2/mount.2.gz
-rwsr-sr-x. 1 root root 44320 Mar 14 10:37 /usr/bin/mount
-rwsr-sr-x. 1 root root 41016 Aug 3 2017 /usr/sbin/mount.cifs
-rwxr-xr-x. 1 root root 11368 Oct 30 2018 /usr/sbin/mount.fuse
-rwsr-xr-x. 1 root root 117504 Nov 7 2018 /usr/sbin/mount.nfs
lrwxrwxrwx. 1 root root   9 Jun 1 17:15 /usr/sbin/mount.nfs4 -> mount.nfs
-rw-r--r--. 1 root root   5937 Jun 9 2014 /usr/share/man/man2/mount.2.gz
-rw-r--r--. 1 root root 30554 Mar 14 10:37 /usr/share/man/man8/mount.8.gz
13.3.1 позднее выяснил, что менять разрешения можно было и таким образом:
[root@centos ~]# chmod +s `which mount`
[root@centos ~]# ls -la `which mount`
-rwsr-sr-x. 1 root root 44320 Mar 14 10:37 /bin/mount

pam.d
подготовка к реализации примера начатого в лекции, по запрету с помощью time_conf логиниться пользователю otus2 через ssh

vagrant ssh-config
Host centos
* HostName 127.0.0.1*
* User vagrant*
* Port 2222*
* UserKnownHostsFile /dev/null*
* StrictHostKeyChecking no*

PasswordAuthentication no
IdentityFile /home/labuzhskiy/.vagrant.d/boxes/4lesson-dz/.vagrant/machines/centos/virtualbox/private_key
IdentitiesOnly yes
LogLevel FATAL

The provider for this Vagrant-managed machine is reporting that it is not yet ready for SSH. Depending on your provider this can carry different meanings. Make sure your machine is created and running and try again. Additionally, check the output of `vagrant status` to verify that the machine is in the state that you expect. If you continue to get this error message, please view the documentation for the provider you're using.

labuzhskiy@MINT-LIN-CIN-X64 ~/.vagrant.d/boxes/4lesson-dz/.vagrant/machines/centos/virtualbox $ ***ssh -i ~/.vagrant.d/boxes/4lesson-dz/.vagrant/machines/centos/virtualbox/private_key otus2@127.0.0.1 -p 2222***
The authenticity of host '[127.0.0.1]:2222 ([127.0.0.1]:2222)' can't be established.
ECDSA key fingerprint is SHA256:Xug6/UVvxvyJ+CJEAZgyY1ndhSS0FaNWH2Fae9CbFWc.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': ***yes***
Warning: Permanently added '[127.0.0.1]:2222' (ECDSA) to the list of known hosts.
Last login: Tue Sep 3 15:55:08 2019
[otus2@centos ~]$

1. Отредактировал файл /etc/pam.d/sshd, добавив в него pam_time.so
[root@centos ~]# vi /etc/pam.d/sshd

```
#%PAM-1.0
auth       required     pam_sepermit.so
auth       substack     password-auth
auth       include      postlogin
# Used with polkit to reauthorize users in remote sessions
-auth      optional     pam_reauthorize.so prepare
account    required     pam_time.so
account    required     pam_nologin.so
account    include      password-auth
password   include      password-auth
# pam_selinux.so close should be the first session rule
session    required     pam_selinux.so close
session    required     pam_loginuid.so
# pam_selinux.so open should only be followed by sessions to be executed in the user context
session    required     pam_selinux.so open env_params
session    required     pam_namespace.so
session    optional     pam_keyinit.so force revoke
session    include      password-auth
session    include      postlogin
# Used with polkit to reauthorize users in remote sessions
-session   optional     pam_reauthorize.so prepare
~
```

~
~
~
~
~
"/etc/pam.d/sshd" 20L, 904C

2. отредактировал и перезапустил конфигурационный файл cat /etc/security/time.conf

[root@centos security]# cat /etc/security/time.conf
 # this is an example configuration file for the pam_time module. Its syntax
 # was initially based heavily on that of the shadow package (shadow-960129).
#
 # the syntax of the lines is as follows:
#
 # services;ttys;users;times
#
 # white space is ignored and lines maybe extended with '\\n' (escaped
 # newlines). As should be clear from reading these comments,
 # text following a '#' is ignored to the end of the line.
#
 # the combination of individual users/terminals etc is a logic list
 # namely individual tokens that are optionally prefixed with '!' (logical
 # not) and separated with '&' (logical and) and '|' (logical or).
#
 # services
 # is a logic list of PAM service names that the rule applies to.
#
 # ttys
 # is a logic list of terminal names that this rule applies to.
#
 # users
 # is a logic list of users or a netgroup of users to whom this
 # rule applies.
#
 # NB. For these items the simple wildcard '' may be used only once.*
#
 # times
 # the format here is a logic list of day/time-range
 # entries the days are specified by a sequence of two character
 # entries, MoTuSa for example is Monday Tuesday and Saturday. Note
 # that repeated days are unset MoMo = no day, and MoWk = all weekdays
 # bar Monday. The two character combinations accepted are
#
 # Mo Tu We Th Fr Sa Su Wk Wd Al
#
 # the last two being week-end days and all 7 days of the week
 # respectively. As a final example, AlFr means all days except Friday.
#
 # each day/time-range can be prefixed with a '!' to indicate "anything
 # but"
#

 # The time-range part is two 24-hour times HHMM separated by a hyphen
 # indicating the start and finish time (if the finish time is smaller
 # than the start time it is deemed to apply on the following day).
#
 # for a rule to be active, ALL of service+ttys+users must be satisfied
 # by the applying process.
#

#
 # Here is a simple example: running blank on tty (any ttyXXX device),*
 # the users 'you' and 'me' are denied service all of the time
#

#blank;tty & !ttyp*;you|me;!Al0000-2400*

 # Another silly example, user 'root' is denied xsh access
 # from pseudo terminals at the weekend and on mondays.

#xsh;ttyp;root;!WdMo0000-2400*
sshd;tty*;otus2;!Al0000-2400
#
 # End of example file.
#

3. изучил записи по безопасности системного журнала:

[root@centos security]# tail -n 100 /var/log/secure
Sep 3 15:53:05 centos unix_chkpwd[2487]: password check failed for user (otus2)
Sep 3 15:53:05 centos passwd: pam_unix(passwd:chauthtok): authentication failure; logname= uid=1002 euid=0 tty=pts/2 ruser= rhost= user=otus2
Sep 3 15:53:07 centos sudo: pam_unix(sudo:session): session closed for user otus2
Sep 3 15:54:19 centos passwd: pam_pwquality(passwd:chauthtok): pam_get_authtok_verify returned error: Failed preliminary check by password service
Sep 3 15:54:37 centos passwd: pam_unix(passwd:chauthtok): password changed for otus2
Sep 3 15:55:08 centos su: pam_unix(su-l:session): session opened for user otus2 by vagrant(uid=0)
Sep 3 15:55:15 centos su: pam_unix(su-l:session): session closed for user otus2
Sep 3 16:04:59 centos sshd[2567]: Accepted publickey for vagrant from 10.0.2.2 port 42104 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 3 16:04:59 centos sshd[2567]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 3 16:05:03 centos sshd[2570]: Received disconnect from 10.0.2.2 port 42104:11: disconnected by user
Sep 3 16:05:03 centos sshd[2570]: Disconnected from 10.0.2.2 port 42104
Sep 3 16:05:03 centos sshd[2567]: pam_unix(sshd:session): session closed for user vagrant
Sep 3 17:23:29 centos polkitd[1556]: Reloading rules
Sep 3 17:23:29 centos polkitd[1556]: Collecting garbage unconditionally...
Sep 3 17:23:29 centos polkitd[1556]: Loading rules from directory /etc/polkit-1/rules.d
Sep 3 17:23:29 centos polkitd[1556]: Loading rules from directory /usr/share/polkit-1/rules.d
Sep 3 17:23:29 centos polkitd[1556]: Finished loading, compiling and executing 4 rules
Sep 3 17:24:07 centos sudo: root : TTY=pts/2 ; PWD=/home/vagrant ; USER=otus ; COMMAND=/bin/mount /dev/sdb1 /media/sdb1

Sep 3 17:24:07 centos sudo: pam_unix(sudo:session): session opened for user otus by vagrant(uid=0)
Sep 3 17:24:07 centos sudo: pam_unix(sudo:session): session closed for user otus
Sep 3 17:44:55 centos sshd[2279]: Received disconnect from 10.0.2.2 port 41566:11: disconnected by user
Sep 3 17:44:55 centos sshd[2279]: Disconnected from 10.0.2.2 port 41566
Sep 3 17:44:55 centos sshd[2276]: pam_unix(sshd:session): session closed for user vagrant
Sep 3 17:44:55 centos su: pam_unix(su-l:session): session closed for user root
Sep 3 17:44:55 centos sudo: pam_unix(sudo:session): session closed for user root
Sep 3 18:03:36 centos polkitd[1556]: Registered Authentication Agent for unix-process:2721:1116224 (system bus name :1.52 [/usr/bin/pkttyagent --notify-fd 5 --fallback], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Sep 4 15:56:07 centos polkitd[1561]: Loading rules from directory /etc/polkit-1/rules.d
Sep 4 15:56:07 centos polkitd[1561]: Loading rules from directory /usr/share/polkit-1/rules.d
Sep 4 15:56:07 centos polkitd[1561]: Finished loading, compiling and executing 4 rules
Sep 4 15:56:07 centos polkitd[1561]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
Sep 4 15:56:11 centos sshd[1947]: Server listening on 0.0.0.0 port 22.
Sep 4 15:56:11 centos sshd[1947]: Server listening on :: port 22.
Sep 4 15:56:38 centos sshd[2195]: Accepted publickey for vagrant from 10.0.2.2 port 39000 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 15:56:39 centos sshd[2195]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 15:57:20 centos sudo: vagrant : TTY=pts/0 ; PWD=/home/vagrant ; USER=otus3 ; COMMAND=/bin/groups
Sep 4 15:57:20 centos sudo: pam_unix(sudo:session): session opened for user otus3 by vagrant(uid=0)
Sep 4 15:57:20 centos sudo: pam_unix(sudo:session): session closed for user otus3
Sep 4 15:57:34 centos sudo: vagrant : TTY=pts/0 ; PWD=/home/vagrant ; USER=root ; COMMAND=/bin/su -l
Sep 4 15:57:34 centos sudo: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 4 15:57:34 centos su: pam_unix(su-l:session): session opened for user root by vagrant(uid=0)
Sep 4 16:16:12 centos polkitd[1561]: Registered Authentication Agent for unix-process:2372:121900 (system bus name :1.29 [/usr/bin/pkttyagent --notify-fd 5 --fallback], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Sep 4 16:16:35 centos polkitd[1595]: Loading rules from directory /etc/polkit-1/rules.d
Sep 4 16:16:35 centos polkitd[1595]: Loading rules from directory /usr/share/polkit-1/rules.d
Sep 4 16:16:35 centos polkitd[1595]: Finished loading, compiling and executing 4 rules
Sep 4 16:16:35 centos polkitd[1595]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
Sep 4 16:16:36 centos sshd[1842]: Server listening on 0.0.0.0 port 22.
Sep 4 16:16:36 centos sshd[1842]: Server listening on :: port 22.
Sep 4 16:16:48 centos sshd[2202]: Accepted publickey for vagrant from 10.0.2.2 port 40094 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 16:16:48 centos sshd[2202]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 16:17:36 centos sshd[2231]: Connection closed by 127.0.0.1 port 40106 [preauth]
Sep 4 16:18:35 centos sshd[2205]: Received disconnect from 10.0.2.2 port 40094:11: disconnected by user
Sep 4 16:18:35 centos sshd[2205]: Disconnected from 10.0.2.2 port 40094
Sep 4 16:18:35 centos sshd[2202]: pam_unix(sshd:session): session closed for user vagrant

Sep 4 16:32:16 centos sshd[2237]: Accepted publickey for otus2 from 10.0.2.2 port 40326 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 16:32:16 centos sshd[2237]: pam_unix(sshd:session): session opened for user otus2 by (uid=0)
Sep 4 17:33:51 centos sshd[2241]: Received disconnect from 10.0.2.2 port 40326:11: disconnected by user
Sep 4 17:33:51 centos sshd[2241]: Disconnected from 10.0.2.2 port 40326
Sep 4 17:33:51 centos sshd[2237]: pam_unix(sshd:session): session closed for user otus2
Sep 4 17:34:09 centos sshd[2305]: Accepted publickey for vagrant from 10.0.2.2 port 40730 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 17:34:09 centos sshd[2305]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 17:34:14 centos sudo: vagrant : TTY=pts/0 ; PWD=/home/vagrant ; USER=root ; COMMAND=/bin/su -l
Sep 4 17:34:14 centos sudo: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 4 17:34:14 centos su: pam_unix(su-l:session): session opened for user root by vagrant(uid=0)
Sep 4 17:34:21 centos polkitd[1595]: Registered Authentication Agent for unix-process:2353:467871 (system bus name :1.34 [/usr/bin/pkttyagent --notify-fd 5 --fallback], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Sep 4 18:28:11 centos polkitd[1615]: Loading rules from directory /etc/polkit-1/rules.d
Sep 4 18:28:11 centos polkitd[1615]: Loading rules from directory /usr/share/polkit-1/rules.d
Sep 4 18:28:11 centos polkitd[1615]: Finished loading, compiling and executing 4 rules
Sep 4 18:28:11 centos polkitd[1615]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
Sep 4 18:28:12 centos sshd[1841]: Server listening on 0.0.0.0 port 22.
Sep 4 18:28:12 centos sshd[1841]: Server listening on :: port 22.
Sep 4 18:28:41 centos sshd[2191]: Accepted publickey for vagrant from 10.0.2.2 port 40932 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 18:28:41 centos sshd[2191]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 18:29:03 centos sudo: vagrant : TTY=pts/0 ; PWD=/home/vagrant ; USER=root ; COMMAND=/bin/su
-l
Sep 4 18:29:03 centos sudo: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 4 18:29:03 centos su: pam_unix(su-l:session): session opened for user root by vagrant(uid=0)
Sep 4 18:40:32 centos sshd[2194]: Received disconnect from 10.0.2.2 port 40932:11: disconnected by user
Sep 4 18:40:32 centos sshd[2194]: Disconnected from 10.0.2.2 port 40932
Sep 4 18:40:32 centos sshd[2191]: pam_unix(sshd:session): session closed for user vagrant
Sep 4 18:40:32 centos su: pam_unix(su-l:session): session closed for user root
Sep 4 18:40:32 centos sudo: pam_unix(sudo:session): session closed for user root
Sep 4 18:41:22 centos sshd[2245]: Accepted publickey for vagrant from 10.0.2.2 port 40978 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 18:41:22 centos sshd[2245]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 18:41:30 centos sudo: vagrant : TTY=pts/0 ; PWD=/home/vagrant ; USER=root ; COMMAND=/bin/su -l
Sep 4 18:41:30 centos sudo: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 4 18:41:30 centos su: pam_unix(su-l:session): session opened for user root by vagrant(uid=0)

Sep 4 19:08:08 centos sshd[2248]: Received disconnect from 10.0.2.2 port 40978:11: disconnected by user
Sep 4 19:08:08 centos sshd[2248]: Disconnected from 10.0.2.2 port 40978
Sep 4 19:08:08 centos sshd[2245]: pam_unix(sshd:session): session closed for user vagrant
Sep 4 19:08:08 centos su: pam_unix(su-l:session): session closed for user root
Sep 4 19:08:08 centos sudo: pam_unix(sudo:session): session closed for user root
Sep 4 19:08:45 centos sshd[2364]: Accepted publickey for vagrant from 10.0.2.2 port 41054 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 19:08:45 centos sshd[2364]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 19:09:12 centos sudo: vagrant : TTY=pts/0 ; PWD=/home/vagrant ; USER=root ; COMMAND=/bin/su -l
Sep 4 19:09:12 centos sudo: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 4 19:09:12 centos su: pam_unix(su-l:session): session opened for user root by vagrant(uid=0)
Sep 4 19:24:27 centos sshd[2479]: Accepted publickey for otus2 from 10.0.2.2 port 41108 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 19:24:27 centos sshd[2479]: pam_unix(sshd:session): session opened for user otus2 by (uid=0)
Sep 4 19:24:36 centos sshd[2482]: Received disconnect from 10.0.2.2 port 41108:11: disconnected by user
Sep 4 19:24:36 centos sshd[2482]: Disconnected from 10.0.2.2 port 41108
Sep 4 19:24:36 centos sshd[2479]: pam_unix(sshd:session): session closed for user otus2
[root@centos security]#

Это странно, но grep по pam_time говорит, что pam_time вообще в лог не записывается...
[root@centos security]# tail -n 100 /var/log/secure | grep pam_time
[root@centos security]#

[root@centos security]# tail -n 100 /var/log/secure | grep pam
Sep 3 15:53:05 centos passwd: pam_unix(passwd:chauthtok): authentication failure; logname= uid=1002 euid=0 tty=pts/2 ruser= rhost= user=otus2
Sep 3 15:53:07 centos sudo: pam_unix(sudo:session): session closed for user otus2
Sep 3 15:54:19 centos passwd: pam_pwquality(passwd:chauthtok): pam_get_authtok_verify returned error: Failed preliminary check by password service
Sep 3 15:54:37 centos passwd: pam_unix(passwd:chauthtok): password changed for otus2
Sep 3 15:55:08 centos su: pam_unix(su-l:session): session opened for user otus2 by vagrant(uid=0)
Sep 3 15:55:15 centos su: pam_unix(su-l:session): session closed for user otus2
Sep 3 16:04:59 centos sshd[2567]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 3 16:05:03 centos sshd[2567]: pam_unix(sshd:session): session closed for user vagrant
Sep 3 17:24:07 centos sudo: pam_unix(sudo:session): session opened for user otus by vagrant(uid=0)
Sep 3 17:24:07 centos sudo: pam_unix(sudo:session): session closed for user otus
Sep 3 17:44:55 centos sshd[2276]: pam_unix(sshd:session): session closed for user vagrant
Sep 3 17:44:55 centos su: pam_unix(su-l:session): session closed for user root
Sep 3 17:44:55 centos sudo: pam_unix(sudo:session): session closed for user root
Sep 4 15:56:39 centos sshd[2195]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 15:57:20 centos sudo: pam_unix(sudo:session): session opened for user otus3 by vagrant(uid=0)

Sep 4 15:57:20 centos sudo: pam_unix(sudo:session): session closed for user otus3
Sep 4 15:57:34 centos sudo: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 4 15:57:34 centos su: pam_unix(su-l:session): session opened for user root by vagrant(uid=0)
Sep 4 16:16:48 centos sshd[2202]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 16:18:35 centos sshd[2202]: pam_unix(sshd:session): session closed for user vagrant
Sep 4 16:32:16 centos sshd[2237]: pam_unix(sshd:session): session opened for user otus2 by (uid=0)
Sep 4 17:33:51 centos sshd[2237]: pam_unix(sshd:session): session closed for user otus2
Sep 4 17:34:09 centos sshd[2305]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 17:34:14 centos sudo: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 4 17:34:14 centos su: pam_unix(su-l:session): session opened for user root by vagrant(uid=0)
Sep 4 18:28:41 centos sshd[2191]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 18:29:03 centos sudo: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 4 18:29:03 centos su: pam_unix(su-l:session): session opened for user root by vagrant(uid=0)
Sep 4 18:40:32 centos sshd[2191]: pam_unix(sshd:session): session closed for user vagrant
Sep 4 18:40:32 centos su: pam_unix(su-l:session): session closed for user root
Sep 4 18:40:32 centos sudo: pam_unix(sudo:session): session closed for user root
Sep 4 18:41:22 centos sshd[2245]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 18:41:30 centos sudo: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 4 18:41:30 centos su: pam_unix(su-l:session): session opened for user root by vagrant(uid=0)
Sep 4 19:08:08 centos sshd[2245]: pam_unix(sshd:session): session closed for user vagrant
Sep 4 19:08:08 centos su: pam_unix(su-l:session): session closed for user root
Sep 4 19:08:08 centos sudo: pam_unix(sudo:session): session closed for user root
Sep 4 19:08:45 centos sshd[2364]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 19:09:12 centos sudo: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 4 19:09:12 centos su: pam_unix(su-l:session): session opened for user root by vagrant(uid=0)
Sep 4 19:24:27 centos sshd[2479]: pam_unix(sshd:session): session opened for user otus2 by (uid=0)
Sep 4 19:24:36 centos sshd[2479]: pam_unix(sshd:session): session closed for user otus2

4. Поставил запись pam_time.so на первое место.
[root@centos pam.d]# cat /etc/pam.d/sshd
#%PAM-1.0
account   required   pam_time.so
auth   required   pam_sepermit.so
auth   substack   password-auth
auth   include   postlogin
 # Used with polkit to reauthorize users in remote sessions
-auth   optional   pam_reauthorize.so prepare
account   required   pam_nologin.so
account   include   password-auth
password   include   password-auth

 # pam_selinux.so close should be the first session rule
session required pam_selinux.so close
session required pam_loginuid.so
 # pam_selinux.so open should only be followed by sessions to be executed in the user context
session required pam_selinux.so open env_params
session required pam_namespace.so
session optional pam_keyinit.so force revoke
session include password-auth
session include postlogin
 # Used with polkit to reauthorize users in remote sessions
-session optional pam_reauthorize.so prepare
[root@centos pam.d]#

5. Исправил конфигурационный файл так, чтобы правило запрета во входе в систему через SSH для учётной записи otus2 срабатывало всегда.
[root@centos etc]# vi /etc/security/time.conf

 # this is an example configuration file for the pam_time module. Its syntax
 # was initially based heavily on that of the shadow package (shadow-960129).
#
 # the syntax of the lines is as follows:
#
 # services;ttys;users;times
#
 # white space is ignored and lines maybe extended with '\\n' (escaped
 # newlines). As should be clear from reading these comments,
 # text following a '#' is ignored to the end of the line.
#
 # the combination of individual users/terminals etc is a logic list
 # namely individual tokens that are optionally prefixed with '!' (logical
 # not) and separated with '&' (logical and) and '|' (logical or).
#
 # services
 # is a logic list of PAM service names that the rule applies to.
#
 # ttys
 # is a logic list of terminal names that this rule applies to.
#
 # users
 # is a logic list of users or a netgroup of users to whom this
 # rule applies.
#
 # NB. For these items the simple wildcard '' may be used only once.*
#
 # times
 # the format here is a logic list of day/time-range
 # entries the days are specified by a sequence of two character
 # entries, MoTuSa for example is Monday Tuesday and Saturday. Note
 # that repeated days are unset MoMo = no day, and MoWk = all weekdays
 # bar Monday. The two character combinations accepted are
#
 # Mo Tu We Th Fr Sa Su Wk Wd Al

#
 # the last two being week-end days and all 7 days of the week
 # respectively. As a final example, AlFr means all days except Friday.
#
 # each day/time-range can be prefixed with a '!' to indicate "anything
 # but"
#
 # The time-range part is two 24-hour times HHMM separated by a hyphen
 # indicating the start and finish time (if the finish time is smaller
 # than the start time
it is deemed to apply on the following day).
#
 # for a rule to be active, ALL of service+ttys+users must be satisfied
 # by the applying process.
#

#
 # Here is a simple example: running blank on tty (any ttyXXX device),*
 # the users 'you' and 'me' are denied service all of the time
#

#blank;tty & !ttyp*;you|me;!Al0000-2400*

 # Another silly example, user 'root' is denied xsh access
 # from pseudo terminals at the weekend and on mondays.

#xsh;ttyp;root;!WdMo0000-2400*
sshd;*;otus2;!Al0000-2400
#
 # End of example file.
#

labuzhskiy@MINT-LIN-CIN-X64 ~/.vagrant.d/boxes/4lesson-dz $ ssh -i ~/.vagrant.d/boxes/4lesson-dz/.vagrant/machines/centos/virtualbox/private_key otus2@127.0.0.1 -p 2222
Connection closed by 127.0.0.1 port 2222 ###-- **Теперь работает.**

5. Смотрим журнал:
[vagrant@centos ~]$ tail -n 100 /var/log/secure
tail: cannot open '/var/log/secure' for reading: Permission denied
[vagrant@centos ~]$ sudo !!
sudo tail -n 100 /var/log/secure
Sep 4 19:08:45 centos sshd[2364]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 19:09:12 centos sudo: vagrant : TTY=pts/0 ; PWD=/home/vagrant ; USER=root ; COMMAND=/bin/su -l
Sep 4 19:09:12 centos sudo: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 4 19:09:12 centos su: pam_unix(su-l:session): session opened for user root by vagrant(uid=0)
Sep 4 19:24:27 centos sshd[2479]: Accepted publickey for otus2 from 10.0.2.2 port 41108 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 19:24:27 centos sshd[2479]: pam_unix(sshd:session): session opened for user otus2 by

(uid=0)
Sep 4 19:24:36 centos sshd[2482]: Received disconnect from 10.0.2.2 port 41108:11: disconnected by user
Sep 4 19:24:36 centos sshd[2482]: Disconnected from 10.0.2.2 port 41108
Sep 4 19:24:36 centos sshd[2479]: pam_unix(sshd:session): session closed for user otus2
Sep 4 19:32:08 centos sshd[2520]: Accepted publickey for otus2 from 10.0.2.2 port 41128 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 19:32:09 centos sshd[2520]: pam_unix(sshd:session): session opened for user otus2 by (uid=0)
Sep 4 19:32:15 centos sshd[2523]: Received disconnect from 10.0.2.2 port 41128:11: disconnected by user
Sep 4 19:32:15 centos sshd[2523]: Disconnected from 10.0.2.2 port 41128
Sep 4 19:32:15 centos sshd[2520]: pam_unix(sshd:session): session closed for user otus2
Sep 4 19:50:36 centos sshd[2367]: Received disconnect from 10.0.2.2 port 41054:11: disconnected by user
Sep 4 19:50:36 centos sshd[2367]: Disconnected from 10.0.2.2 port 41054
Sep 4 19:50:36 centos sshd[2364]: pam_unix(sshd:session): session closed for user vagrant
Sep 4 19:50:36 centos su: pam_unix(su-l:session): session closed for user root
Sep 4 19:50:36 centos sudo: pam_unix(sudo:session): session closed for user root
Sep 4 19:51:12 centos sshd[2557]: Accepted publickey for vagrant from 10.0.2.2 port 41170 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 19:51:12 centos sshd[2557]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 19:51:21 centos sudo: vagrant : TTY=pts/0 ; PWD=/home/vagrant ; USER=root ; COMMAND=/bin/su -l
Sep 4 19:51:21 centos sudo: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 4 19:51:21 centos su: pam_unix(su-l:session): session opened for user root by vagrant(uid=0)
Sep 4 20:01:50 centos sshd[2560]: Received disconnect from 10.0.2.2 port 41170:11: disconnected by user
Sep 4 20:01:50 centos sshd[2560]: Disconnected from 10.0.2.2 port 41170
Sep 4 20:01:50 centos sshd[2557]: pam_unix(sshd:session): session closed for user vagrant
Sep 4 20:01:50 centos su: pam_unix(su-l:session): session closed for user root
Sep 4 20:01:50 centos sudo: pam_unix(sudo:session): session closed for user root
Sep 4 20:02:10 centos sshd[2649]: Accepted publickey for vagrant from 10.0.2.2 port 41214 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 20:02:10 centos sshd[2649]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 20:02:22 centos sudo: vagrant : TTY=pts/0 ; PWD=/home/vagrant ; USER=root ; COMMAND=/bin/su -l
Sep 4 20:02:22 centos sudo: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 4 20:02:22 centos su: pam_unix(su-l:session): session opened for user root by vagrant(uid=0)
Sep 4 20:03:24 centos sshd[2697]: Accepted publickey for vagrant from 10.0.2.2 port 41232 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 20:03:24 centos sshd[2697]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 20:03:55 centos sudo: vagrant : TTY=pts/1 ; PWD=/home ; USER=root ; COMMAND=/bin/su -
Sep 4 20:03:55 centos sudo: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 4 20:03:55 centos su: pam_unix(su-l:session): session opened for user root by vagrant(uid=0)

Sep 4 20:08:05 centos sshd[2652]: Received disconnect from 10.0.2.2 port 41214:11: disconnected by user
Sep 4 20:08:05 centos sshd[2652]: Disconnected from 10.0.2.2 port 41214
Sep 4 20:08:05 centos sshd[2649]: pam_unix(sshd:session): session closed for user vagrant
Sep 4 20:08:05 centos su: pam_unix(su-l:session): session closed for user root
Sep 4 20:08:05 centos sudo: pam_unix(sudo:session): session closed for user root
Sep 4 20:08:23 centos sshd[2796]: Accepted publickey for vagrant from 10.0.2.2 port 41252 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 20:08:23 centos sshd[2796]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 20:08:31 centos sudo: vagrant : TTY=pts/0 ; PWD=/home/vagrant ; USER=root ; COMMAND=/bin/su -
Sep 4 20:08:31 centos sudo: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 4 20:08:31 centos su: pam_unix(su-l:session): session opened for user root by vagrant(uid=0)
Sep 4 20:12:37 centos sshd[2799]: Received disconnect from 10.0.2.2 port 41252:11: disconnected by user
Sep 4 20:12:37 centos sshd[2799]: Disconnected from 10.0.2.2 port 41252
Sep 4 20:12:37 centos sshd[2796]: pam_unix(sshd:session): session closed for user vagrant
Sep 4 20:12:38 centos su: pam_unix(su-l:session): session closed for user root
Sep 4 20:12:38 centos sudo: pam_unix(sudo:session): session closed for user root
Sep 4 20:12:57 centos sshd[2845]: Accepted publickey for vagrant from 10.0.2.2 port 41268 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 20:12:58 centos sshd[2845]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 20:13:03 centos sudo: vagrant : TTY=pts/0 ; PWD=/home/vagrant ; USER=root ; COMMAND=/bin/su -
Sep 4 20:13:03 centos sudo: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 4 20:13:03 centos su: pam_unix(su-l:session): session opened for user root by vagrant(uid=0)
Sep 4 20:22:21 centos sshd[2848]: Received disconnect from 10.0.2.2 port 41268:11: disconnected by user
Sep 4 20:22:21 centos sshd[2848]: Disconnected from 10.0.2.2 port 41268
Sep 4 20:22:21 centos sshd[2845]: pam_unix(sshd:session): session closed for user vagrant
Sep 4 20:22:21 centos su: pam_unix(su-l:session): session closed for user root
Sep 4 20:22:21 centos sudo: pam_unix(sudo:session): session closed for user root
Sep 4 20:22:39 centos sshd[2928]: Accepted publickey for vagrant from 10.0.2.2 port 41308 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 20:22:39 centos sshd[2928]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 20:22:46 centos sudo: vagrant : TTY=pts/0 ; PWD=/home/vagrant ; USER=root ; COMMAND=/bin/su -
Sep 4 20:22:46 centos sudo: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 4 20:22:46 centos su: pam_unix(su-l:session): session opened for user root by vagrant(uid=0)
Sep 4 20:31:41 centos su: pam_unix(su-l:session): session closed for user root
Sep 4 20:31:41 centos sudo: pam_unix(sudo:session): session closed for user root
Sep 4 20:31:45 centos sshd[2700]: Received disconnect from 10.0.2.2 port 41232:11: disconnected by user
Sep 4 20:31:45 centos sshd[2700]: Disconnected from 10.0.2.2 port 41232
Sep 4 20:31:45 centos sshd[2697]: pam_unix(sshd:session): session closed for user vagrant
Sep 4 20:31:53 centos sshd[3029]: Accepted publickey for otus2 from 10.0.2.2 port 41332 ssh2:

RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 20:31:53 centos sshd[3029]: pam_unix(sshd:session): session opened for user otus2 by (uid=0)
Sep 4 20:31:58 centos sshd[3032]: Received disconnect from 10.0.2.2 port 41332:11: disconnected by user
Sep 4 20:31:58 centos sshd[3032]: Disconnected from 10.0.2.2 port 41332
Sep 4 20:31:58 centos sshd[3029]: pam_unix(sshd:session): session closed for user otus2
Sep 4 20:46:14 centos sshd[3117]: Accepted publickey for otus2 from 10.0.2.2 port 41388 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 20:46:14 centos sshd[3117]: pam_unix(sshd:session): session opened for user otus2 by (uid=0)
Sep 4 20:46:41 centos sshd[3120]: Received disconnect from 10.0.2.2 port 41388:11: disconnected by user
Sep 4 20:46:41 centos sshd[3120]: Disconnected from 10.0.2.2 port 41388
Sep 4 20:46:41 centos sshd[3117]: pam_unix(sshd:session): session closed for user otus2
Sep 4 20:54:56 centos sshd[3153]: fatal: Access denied for user otus2 by PAM account configuration [preauth]
Sep 4 20:55:22 centos sshd[3156]: fatal: Access denied for user otus2 by PAM account configuration [preauth]
Sep 4 21:10:21 centos sshd[3235]: Connection closed by 10.0.2.2 port 41456 [preauth]
Sep 4 21:13:17 centos sshd[3238]: fatal: Access denied for user otus2 by PAM account configuration [preauth]
Sep 4 21:16:09 centos polkitd[1615]: Registered Authentication Agent for unix-process:3241:1008839 (system bus name :1.74 [/usr/bin/pkttyagent --notify-fd 5 --fallback], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Sep 4 21:25:59 centos polkitd[1551]: Loading rules from directory /etc/polkit-1/rules.d
Sep 4 21:25:59 centos polkitd[1551]: Loading rules from directory /usr/share/polkit-1/rules.d
Sep 4 21:25:59 centos polkitd[1551]: Finished loading, compiling and executing 4 rules
Sep 4 21:25:59 centos polkitd[1551]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
Sep 4 21:26:03 centos sshd[1945]: Server listening on 0.0.0.0 port 22.
Sep 4 21:26:03 centos sshd[1945]: Server listening on :: port 22.
Sep 4 21:27:12 centos sshd[2197]: fatal: Access denied for user otus2 by PAM account configuration [preauth]
Sep 4 21:27:22 centos sshd[2200]: Accepted publickey for vagrant from 10.0.2.2 port 45150 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 21:27:22 centos sshd[2200]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 21:28:36 centos sudo: vagrant : TTY=pts/0 ; PWD=/home/vagrant ; USER=root ; COMMAND=/bin/tail -n 100 /var/log/secure
Sep 4 21:28:36 centos sudo: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
[vagrant@centos ~]$ sudo tail -n 100 /var/log/secure
Sep 4 19:24:27 centos sshd[2479]: Accepted publickey for otus2 from 10.0.2.2 port 41108 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 19:24:27 centos sshd[2479]: pam_unix(sshd:session): session opened for user otus2 by (uid=0)
Sep 4 19:24:36 centos sshd[2482]: Received disconnect from 10.0.2.2 port 41108:11: disconnected by user
Sep 4 19:24:36 centos sshd[2482]: Disconnected from 10.0.2.2 port 41108
Sep 4 19:24:36 centos sshd[2479]: pam_unix(sshd:session): session closed for user otus2
Sep 4 19:32:08 centos sshd[2520]: Accepted publickey for otus2 from 10.0.2.2 port 41128 ssh2:

RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 19:32:09 centos sshd[2520]: pam_unix(sshd:session): session opened for user otus2 by (uid=0)
Sep 4 19:32:15 centos sshd[2523]: Received disconnect from 10.0.2.2 port 41128:11: disconnected by user
Sep 4 19:32:15 centos sshd[2523]: Disconnected from 10.0.2.2 port 41128
Sep 4 19:32:15 centos sshd[2520]: pam_unix(sshd:session): session closed for user otus2
Sep 4 19:50:36 centos sshd[2367]: Received disconnect from 10.0.2.2 port 41054:11: disconnected by user
Sep 4 19:50:36 centos sshd[2367]: Disconnected from 10.0.2.2 port 41054
Sep 4 19:50:36 centos sshd[2364]: pam_unix(sshd:session): session closed for user vagrant
Sep 4 19:50:36 centos su: pam_unix(su-l:session): session closed for user root
Sep 4 19:50:36 centos sudo: pam_unix(sudo:session): session closed for user root
Sep 4 19:51:12 centos sshd[2557]: Accepted publickey for vagrant from 10.0.2.2 port 41170 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 19:51:12 centos sshd[2557]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 19:51:21 centos sudo: vagrant : TTY=pts/0 ; PWD=/home/vagrant ; USER=root ; COMMAND=/bin/su -l
Sep 4 19:51:21 centos sudo: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 4 19:51:21 centos su: pam_unix(su-l:session): session opened for user root by vagrant(uid=0)
Sep 4 20:01:50 centos sshd[2560]: Received disconnect from 10.0.2.2 port 41170:11: disconnected by user
Sep 4 20:01:50 centos sshd[2560]: Disconnected from 10.0.2.2 port 41170
Sep 4 20:01:50 centos sshd[2557]: pam_unix(sshd:session): session closed for user vagrant
Sep 4 20:01:50 centos su: pam_unix(su-l:session): session closed for user root
Sep 4 20:01:50 centos sudo: pam_unix(sudo:session): session closed for user root
Sep 4 20:02:10 centos sshd[2649]: Accepted publickey for vagrant from 10.0.2.2 port 41214 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 20:02:10 centos sshd[2649]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 20:02:22 centos sudo: vagrant : TTY=pts/0 ; PWD=/home/vagrant ; USER=root ; COMMAND=/bin/su -l
Sep 4 20:02:22 centos sudo: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 4 20:02:22 centos su: pam_unix(su-l:session): session opened for user root by vagrant(uid=0)
Sep 4 20:03:24 centos sshd[2697]: Accepted publickey for vagrant from 10.0.2.2 port 41232 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 20:03:24 centos sshd[2697]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 20:03:55 centos sudo: vagrant : TTY=pts/1 ; PWD=/home ; USER=root ; COMMAND=/bin/su -
Sep 4 20:03:55 centos sudo: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 4 20:03:55 centos su: pam_unix(su-l:session): session opened for user root by vagrant(uid=0)
Sep 4 20:08:05 centos sshd[2652]: Received disconnect from 10.0.2.2 port 41214:11: disconnected by user
Sep 4 20:08:05 centos sshd[2652]: Disconnected from 10.0.2.2 port 41214
Sep 4 20:08:05 centos sshd[2649]: pam_unix(sshd:session): session closed for user vagrant
Sep 4 20:08:05 centos su: pam_unix(su-l:session): session closed for user root
Sep 4 20:08:05 centos sudo: pam_unix(sudo:session): session closed for user root

Sep 4 20:08:23 centos sshd[2796]: Accepted publickey for vagrant from 10.0.2.2 port 41252 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 20:08:23 centos sshd[2796]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 20:08:31 centos sudo: vagrant : TTY=pts/0 ; PWD=/home/vagrant ; USER=root ; COMMAND=/bin/su -
Sep 4 20:08:31 centos sudo: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 4 20:08:31 centos su: pam_unix(su-l:session): session opened for user root by vagrant(uid=0)
Sep 4 20:12:37 centos sshd[2799]: Received disconnect from 10.0.2.2 port 41252:11: disconnected by user
Sep 4 20:12:37 centos sshd[2799]: Disconnected from 10.0.2.2 port 41252
Sep 4 20:12:37 centos sshd[2796]: pam_unix(sshd:session): session closed for user vagrant
Sep 4 20:12:38 centos su: pam_unix(su-l:session): session closed for user root
Sep 4 20:12:38 centos sudo: pam_unix(sudo:session): session closed for user root
Sep 4 20:12:57 centos sshd[2845]: Accepted publickey for vagrant from 10.0.2.2 port 41268 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 20:12:58 centos sshd[2845]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 20:13:03 centos sudo: vagrant : TTY=pts/0 ; PWD=/home/vagrant ; USER=root ; COMMAND=/bin/su -
Sep 4 20:13:03 centos sudo: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 4 20:13:03 centos su: pam_unix(su-l:session): session opened for user root by vagrant(uid=0)
Sep 4 20:22:21 centos sshd[2848]: Received disconnect from 10.0.2.2 port 41268:11: disconnected by user
Sep 4 20:22:21 centos sshd[2848]: Disconnected from 10.0.2.2 port 41268
Sep 4 20:22:21 centos sshd[2845]: pam_unix(sshd:session): session closed for user vagrant
Sep 4 20:22:21 centos su: pam_unix(su-l:session): session closed for user root
Sep 4 20:22:21 centos sudo: pam_unix(sudo:session): session closed for user root
Sep 4 20:22:39 centos sshd[2928]: Accepted publickey for vagrant from 10.0.2.2 port 41308 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 20:22:39 centos sshd[2928]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 20:22:46 centos sudo: vagrant : TTY=pts/0 ; PWD=/home/vagrant ; USER=root ; COMMAND=/bin/su -
Sep 4 20:22:46 centos sudo: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 4 20:22:46 centos su: pam_unix(su-l:session): session opened for user root by vagrant(uid=0)
Sep 4 20:31:41 centos su: pam_unix(su-l:session): session closed for user root
Sep 4 20:31:41 centos sudo: pam_unix(sudo:session): session closed for user root
Sep 4 20:31:45 centos sshd[2700]: Received disconnect from 10.0.2.2 port 41232:11: disconnected by user
Sep 4 20:31:45 centos sshd[2700]: Disconnected from 10.0.2.2 port 41232
Sep 4 20:31:45 centos sshd[2697]: pam_unix(sshd:session): session closed for user vagrant
Sep 4 20:31:53 centos sshd[3029]: Accepted publickey for otus2 from 10.0.2.2 port 41332 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 20:31:53 centos sshd[3029]: pam_unix(sshd:session): session opened for user otus2 by (uid=0)
Sep 4 20:31:58 centos sshd[3032]: Received disconnect from 10.0.2.2 port 41332:11: disconnected by user
Sep 4 20:31:58 centos sshd[3032]: Disconnected from 10.0.2.2 port 41332

Sep 4 20:31:58 centos sshd[3029]: pam_unix(sshd:session): session closed for user otus2
Sep 4 20:46:14 centos sshd[3117]: Accepted publickey for otus2 from 10.0.2.2 port 41388 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 20:46:14 centos sshd[3117]: pam_unix(sshd:session): session opened for user otus2 by (uid=0)
Sep 4 20:46:41 centos sshd[3120]: Received disconnect from 10.0.2.2 port 41388:11: disconnected by user
Sep 4 20:46:41 centos sshd[3120]: Disconnected from 10.0.2.2 port 41388
Sep 4 20:46:41 centos sshd[3117]: pam_unix(sshd:session): session closed for user otus2
Sep 4 20:54:56 centos sshd[3153]: fatal: Access denied for user otus2 by PAM account configuration [preauth]
Sep 4 20:55:22 centos sshd[3156]: fatal: Access denied for user otus2 by PAM account configuration [preauth]
Sep 4 21:10:21 centos sshd[3235]: Connection closed by 10.0.2.2 port 41456 [preauth]
Sep 4 21:13:17 centos sshd[3238]: fatal: Access denied for user otus2 by PAM account configuration [preauth]
Sep 4 21:16:09 centos polkitd[1615]: Registered Authentication Agent for unix-process:3241:1008839 (system bus name :1.74 [/usr/bin/pkttyagent --notify-fd 5 --fallback], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Sep 4 21:25:59 centos
polkitd[1551]: Loading rules from directory /etc/polkit-1/rules.d
Sep 4 21:25:59 centos polkitd[1551]: Loading rules from directory /usr/share/polkit-1/rules.d
Sep 4 21:25:59 centos polkitd[1551]: Finished loading, compiling and executing 4 rules
Sep 4 21:25:59 centos polkitd[1551]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
Sep 4 21:26:03 centos sshd[1945]: Server listening on 0.0.0.0 port 22.
Sep 4 21:26:03 centos sshd[1945]: Server listening on :: port 22.
Sep 4 21:27:12 centos sshd[2197]: fatal: Access denied for user otus2 by PAM account configuration [preauth]
Sep 4 21:27:22 centos sshd[2200]: Accepted publickey for vagrant from 10.0.2.2 port 45150 ssh2: RSA SHA256:BErUF8VRD3qCxqFA1JM7Ao2giT3pTUpUnrPxGfmhYzA
Sep 4 21:27:22 centos sshd[2200]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
Sep 4 21:28:36 centos sudo: vagrant : TTY=pts/0 ; PWD=/home/vagrant ; USER=root ; COMMAND=/bin/tail -n 100 /var/log/secure
Sep 4 21:28:36 centos sudo: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 4 21:28:36 centos sudo: pam_unix(sudo:session): session closed for user root
Sep 4 21:28:45 centos sshd[2237]: fatal: Access denied for user otus2 by PAM account configuration [preauth]
Sep 4 21:28:49 centos sudo: vagrant : TTY=pts/0 ; PWD=/home/vagrant ; USER=root ; COMMAND=/bin/tail -n 100 /var/log/secure
Sep 4 21:28:49 centos sudo: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
[vagrant@centos ~]$

Ещё раз убеждаемся, глядя на строки журнала:
Sep 4 21:13:17 centos sshd[3238]: fatal: Access denied for user otus2 by PAM account configuration [preauth]
Sep 4 20:46:41 centos sshd[3117]: pam_unix(sshd:session): session closed for user otus2
Sep 4 20:54:56 centos sshd[3153]: fatal: Access denied for user otus2 by PAM account configuration [preauth]

Sep 4 20:55:22 centos sshd[3156]: fatal: Access denied for user otus2 by PAM account configuration [preauth]

Sep 4 21:13:17 centos sshd[3238]: fatal: Access denied for user otus2 by PAM account configuration [preauth]
Да, доступ закрыт.

chroot

1. Настраиваем Chroot окружение по статье, описанной по следующей ссылке:
https://www.tecmint.com/restrict-ssh-user-to-directory-using-chrooted-jail/

labuzhskiy@MINT-LIN-CIN-X64 ~ $ mc

labuzhskiy@MINT-LIN-CIN-X64 ~/.vagrant.d/boxes/4lesson-dz $ vagrant ssh centos
Last login: Sat Sep 7 19:39:29 2019 from 10.0.2.2
[vagrant@centos ~]$ sudo su -
Last login: Sat Sep 7 19:39:39 UTC 2019 on pts/0
[root@centos ~]# mkdir -p /home/o3
[root@centos ~]# mc

[root@centos ssh]# ls -l /dev/{null,zero,stdin,stdout,stderr,random,tty}
crw-rw-rw-. 1 root root 1, 3 Sep 8 08:30 /dev/null
crw-rw-rw-. 1 root root 1, 8 Sep 8 08:30 /dev/random
lrwxrwxrwx. 1 root root   15 Sep 8 08:30 /dev/stderr -> /proc/self/fd/2
lrwxrwxrwx. 1 root root   15 Sep 8 08:30 /dev/stdin -> /proc/self/fd/0
lrwxrwxrwx. 1 root root   15 Sep 8 08:30 /dev/stdout -> /proc/self/fd/1
crw-rw-rw-. 1 root tty 5, 0 Sep 8 08:30 /dev/tty
crw-rw-rw-. 1 root root 1, 5 Sep 8 08:30 /dev/zero

[root@centos ssh]# mkdir -p /home/o3/dev/
[root@centos ssh]# cd /home/o3/dev/
[root@centos dev]# mknod -m 666 null c 1 3
[root@centos dev]# mknod -m 666 tty c 5 0
[root@centos dev]# mknod -m 666 zero c 1 5
[root@centos dev]# mknod -m 666 random c 1 8
[root@centos dev]# chown root:root /home/o3
[root@centos dev]# chmod 0755 /home/o3
[root@centos dev]# ls -ld /home/o3
drwxr-xr-x. 3 root root 17 Sep 8 08:37 /home/o3
[root@centos dev]# mkdir -p /home/o3/bin

[root@centos o3]# cp -v /bin/bash /home/o3/bin/
‘/bin/bash’ -> ‘/home/o3/bin/bash’
[root@centos o3]# cp -v /bin/bash /home/o3/bin/
‘/bin/bash’ -> ‘/home/o3/bin/bash’
[root@centos o3]# ldd /bin/bash
linux-vdso.so.1 => (0x00007fffa0180000)
libtinfo.so.5 => /lib64/libtinfo.so.5 (0x00007f6a52666000)
libdl.so.2 => /lib64/libdl.so.2 (0x00007f6a52462000)
libc.so.6 => /lib64/libc.so.6 (0x00007f6a52095000)

/lib64/ld-linux-x86-64.so.2 (0x00007f6a52890000)
[root@centos o3]# mkdir -p /home/o3/lib64
[root@centos o3]# cp -v /lib64/{libtinfo.so.5,libdl.so.2,libc.so.6,ld-linux-x86-64.so.2}
/home/o3/lib64/
‘/lib64/libtinfo.so.5’ -> ‘/home/o3/lib64/libtinfo.so.5’
‘/lib64/libdl.so.2’ -> ‘/home/o3/lib64/libdl.so.2’
‘/lib64/libc.so.6’ -> ‘/home/o3/lib64/libc.so.6’
‘/lib64/ld-linux-x86-64.so.2’ -> ‘/home/o3/lib64/ld-linux-x86-64.so.2’

[root@centos o3]# passwd otus3
Changing password for user otus3.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@centos o3]# mkdir /home/o3/etc
[root@centos o3]# cp -vf /etc/{passwd,group} /home/o3/etc/
‘/etc/passwd’ -> ‘/home/o3/etc/passwd’
‘/etc/group’ -> ‘/home/o3/etc/group’

[root@centos otus3]# chown -R otus3:otus3 /home/otus3/.ssh
[root@centos otus3]# ll /home/otus3/.ssh
total 4
-rw-------. 1 otus3 otus3 389 Sep 1 09:41 authorized_keys
[root@centos o3]# ll /home/o3/.ssh
total 4
-rw-------. 1 otus3 otus3 389 Sep 1 09:41 authorized_keys
[root@centos /]# su - otus3
Last login: Sun Sep 8 13:40:40 UTC 2019 on pts/1
[otus3@centos ~]$

Приводим конфигурационный файл sshd_config к следующему виду:

[root@centos /]# cat /etc/ssh/sshd_config
*#	$OpenBSD: sshd_config,v 1.100 2016/08/15 12:32:04 naddy Exp $*

 # This is the sshd server system-wide configuration file. See
 # sshd_config(5) for more information.

 # This sshd was compiled with PATH=/usr/local/bin:/usr/bin

 # The strategy used for options in the default sshd_config shipped with
 # OpenSSH is to specify options with their default value where
 # possible, but leave them commented. Uncommented options override the
 # default value.

 # If you want to change the port on a SELinux system, you have to tell
 # SELinux about this change.
 # semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0

#ListenAddress ::

HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

 # Ciphers and keying
#RekeyLimit default none

 # Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

 # Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

AllowUsers otus2 otus3 vagrant
DenyUsers root

#PubkeyAuthentication yes

 # The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
 # but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile .ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

 # For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
 # Change to yes if you don't trust ~/.ssh/known_hosts for
 # HostbasedAuthentication
#IgnoreUserKnownHosts no
 # Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

 # To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
PasswordAuthentication no

 # Change to no to disable s/key passwords

#ChallengeResponseAuthentication yes
ChallengeResponseAuthentication no

 # Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
#KerberosUseKuserok yes

 # GSSAPI options
GSSAPIAuthentication yes
GSSAPICleanupCredentials no
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no
#GSSAPIEnablek5users no

 # Set this to 'yes' to enable PAM authentication, account processing,
 # and session processing. If this is enabled, PAM authentication will
 # be allowed through the ChallengeResponseAuthentication and
 # PasswordAuthentication. Depending on your PAM configuration,
 # PAM authentication via ChallengeResponseAuthentication may bypass
 # the setting of "PermitRootLogin without-password".
 # If you just want the PAM account and session checks to run without
 # PAM authentication, then enable this but set PasswordAuthentication
 # and ChallengeResponseAuthentication to 'no'.
 # WARNING: 'UsePAM no' is not supported in Red Hat Enterprise Linux and may cause several
 # problems.
UsePAM yes

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
#PrintMotd yes
#PrintLastLog yes
#TCPKeepAlive yes
#UseLogin no
#UsePrivilegeSeparation sandbox
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#ShowPatchLevel no
#UseDNS yes
UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no

#ChrootDirectory /home/o3
#VersionAddendum none

 # no default banner path
#Banner none

 # Accept locale-related environment variables
AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MESSAGES
AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
AcceptEnv LC_IDENTIFICATION LC_ALL LANGUAGE
AcceptEnv XMODIFIERS

 # override default of no subsystems
Subsystem sftp /usr/libexec/openssh/sftp-server

 # Example of overriding settings on a per-user basis
####порядок строк имеет значение и обязательно располагаем их в конце файла.
Match User otus3
ChrootDirectory /home/o3
 # X11Forwarding no
 # AllowTcpForwarding no
 # PermitTTY no
 # ForceCommand cvs server

Проверяем себя:

labuzhskiy@MINT-LIN-CIN-X64 ~/.vagrant.d/boxes/4lesson-dz $ ssh -i ~/.vagrant.d/boxes/4lesson-dz/.vagrant/machines/centos/virtualbox/private_key vagrant@127.0.0.1 -p 2222
Last login: Sun Sep 8 14:02:55 2019 from 10.0.2.2
***[vagrant@centos ~]$** exit*
logout
Connection to 127.0.0.1 closed.
labuzhskiy@MINT-LIN-CIN-X64 ~/.vagrant.d/boxes/4lesson-dz $ ssh -i ~/.vagrant.d/boxes/4lesson-dz/.vagrant/machines/centos/virtualbox/private_key otus3@127.0.0.1 -p 2222
Last login: Sun Sep 8 14:02:12 2019 from 10.0.2.2
***-bash-4.2$** exit*
logout
Connection to 127.0.0.1 closed.
labuzhskiy@MINT-LIN-CIN-X64 ~/.vagrant.d/boxes/4lesson-dz $

* реализовать apparmor профайл для nginx

1. Убедился, что в операционной системе отсутствует предустановленный nginx, но присутствует apparmor:

root@ubuntu:~# more /etc/nginx
more: stat of /etc/nginx failed: No such file or directory
root@ubuntu:~# whereis nginx

nginx:
root@ubuntu:~# whereis apparmor
apparmor: /etc/apparmor /etc/apparmor.d /lib/apparmor /usr/share/man/man7/apparmor.7.gz
2. Обновил список доступных пакетов.
root@ubuntu:~# apt-get update
Hit:1 http://archive.ubuntu.com/ubuntu bionic InRelease
Get:2 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Get:3 http://archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]

Get:4 http://archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]

Fetched 252 kB in 1s (247 kB/s)
Reading package lists... Done

3. Установил nginx.

root@ubuntu:~# apt install nginx -y

Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
fontconfig-config fonts-dejavu-core libfontconfig1 libgd3 libjbig0 libjpeg-turbo8 libjpeg8 libnginx-mod-http-geoip libnginx-mod-http-image-filter
libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream libtiff5 libwebp6 libxpm4 nginx-common nginx-core
Suggested packages:
libgd-tools fcgiwrap nginx-doc ssl-cert
The following NEW packages will be installed:
fontconfig-config fonts-dejavu-core libfontconfig1 libgd3 libjbig0 libjpeg-turbo8 libjpeg8 libnginx-mod-http-geoip libnginx-mod-http-image-filter
libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream libtiff5 libwebp6 libxpm4 nginx nginx-common nginx-core
0 upgraded, 18 newly installed, 0 to remove and 0 not upgraded.
Need to get 2461 kB of archives.
After this operation, 8210 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libjpeg-turbo8 amd64 1.5.2-0ubuntu5.18.04.1 [110 kB]
Get:2 http://archive.ubuntu.com/ubuntu bionic/main amd64 fonts-dejavu-core all 2.37-1 [1041 kB]
Get:3 http://archive.ubuntu.com/ubuntu bionic/main amd64 fontconfig-config all 2.12.6-0ubuntu2 [55.8 kB]
Get:4 http://archive.ubuntu.com/ubuntu bionic/main amd64 libfontconfig1 amd64 2.12.6-0ubuntu2 [137 kB]
Get:5 http://archive.ubuntu.com/ubuntu bionic/main amd64 libjpeg8 amd64 8c-2ubuntu8 [2194 B]
Get:6 http://archive.ubuntu.com/ubuntu bionic/main amd64 libjbig0 amd64 2.1-3.1build1 [26.7 kB]
Get:7 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libtiff5 amd64 4.0.9-5ubuntu0.2 [153 kB]
Get:8 http://archive.ubuntu.com/ubuntu bionic/main amd64 libwebp6 amd64 0.6.1-2 [185 kB]
Get:9 http://archive.ubuntu.com/ubuntu bionic/main amd64 libxpm4 amd64 1:3.5.12-1 [34.0 kB]
Get:10 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libgd3 amd64 2.2.5-4ubuntu0.3 [119 kB]
Get:11 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 nginx-common all 1.14.0-

0ubuntu1.6 [37.3 kB]
Get:12 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libnginx-mod-http-geoip amd64 1.14.0-0ubuntu1.6 [11.2 kB]
Get:13 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libnginx-mod-http-image-filter amd64 1.14.0-0ubuntu1.6 [14.5 kB]
Get:14 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libnginx-mod-http-xslt-filter amd64 1.14.0-0ubuntu1.6 [12.9 kB]
Get:15 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libnginx-mod-mail amd64 1.14.0-0ubuntu1.6 [41.7 kB]
Get:16 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libnginx-mod-stream amd64 1.14.0-0ubuntu1.6 [63.6 kB]
Get:17 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 nginx-core amd64 1.14.0-0ubuntu1.6 [413 kB]
Get:18 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 nginx all 1.14.0-0ubuntu1.6 [3596 B]
Fetched 2461 kB in 6s (414 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libjpeg-turbo8:amd64.
(Reading database ... 90216 files and directories currently installed.)
Preparing to unpack .../00-libjpeg-turbo8_1.5.2-0ubuntu5.18.04.1_amd64.deb ...
Unpacking libjpeg-turbo8:amd64 (1.5.2-0ubuntu5.18.04.1) ...
Selecting previously unselected package fonts-dejavu-core.
Preparing to unpack .../01-fonts-dejavu-core_2.37-1_all.deb ...
Unpacking fonts-dejavu-core (2.37-1) ...
Selecting previously unselected package fontconfig-config.
Preparing to unpack .../02-fontconfig-config_2.12.6-0ubuntu2_all.deb ...
Unpacking fontconfig-config (2.12.6-0ubuntu2) ...
Selecting previously unselected package libfontconfig1:amd64.
Preparing to unpack .../03-libfontconfig1_2.12.6-0ubuntu2_amd64.deb ...
Unpacking libfontconfig1:amd64 (2.12.6-0ubuntu2) ...
Selecting previously unselected package libjpeg8:amd64.
Preparing to unpack .../04-libjpeg8_8c-2ubuntu8_amd64.deb ...
Unpacking libjpeg8:amd64 (8c-2ubuntu8) ...
Selecting previously unselected package libjbig0:amd64.
Preparing to unpack .../05-libjbig0_2.1-3.1build1_amd64.deb ...
Unpacking libjbig0:amd64 (2.1-3.1build1) ...
Selecting previously unselected package libtiff5:amd64.
Preparing to unpack .../06-libtiff5_4.0.9-5ubuntu0.2_amd64.deb ...
Unpacking libtiff5:amd64 (4.0.9-5ubuntu0.2) ...
Selecting previously unselected package libwebp6:amd64.
Preparing to unpack .../07-libwebp6_0.6.1-2_amd64.deb ...
Unpacking libwebp6:amd64 (0.6.1-2) ...
Selecting previously unselected package libxpm4:amd64.
Preparing to unpack .../08-libxpm4_1%3a3.5.12-1_amd64.deb ...
Unpacking libxpm4:amd64 (1:3.5.12-1) ...
Selecting previously unselected package libgd3:amd64.
Preparing to unpack .../09-libgd3_2.2.5-4ubuntu0.3_amd64.deb ...
Unpacking libgd3:amd64 (2.2.5-4ubuntu0.3) ...
Selecting previously unselected package nginx-common.
Preparing to unpack .../10-nginx-common_1.14.0-0ubuntu1.6_all.deb ...
Unpacking nginx-common (1.14.0-0ubuntu1.6) ...
Selecting previously unselected package libnginx-mod-http-geoip.

Preparing to unpack .../11-libnginx-mod-http-geoip_1.14.0-0ubuntu1.6_amd64.deb ...
Unpacking libnginx-mod-http-geoip (1.14.0-0ubuntu1.6) ...
Selecting previously unselected package libnginx-mod-http-image-filter.
Preparing to unpack .../12-libnginx-mod-http-image-filter_1.14.0-0ubuntu1.6_amd64.deb ...
Unpacking libnginx-mod-http-image-filter (1.14.0-0ubuntu1.6) ...
Selecting previously unselected package libnginx-mod-http-xslt-filter.
Preparing to unpack .../13-libnginx-mod-http-xslt-filter_1.14.0-0ubuntu1.6_amd64.deb ...
Unpacking libnginx-mod-http-xslt-filter (1.14.0-0ubuntu1.6) ...
Selecting previously unselected package libnginx-mod-mail.
Preparing to unpack .../14-libnginx-mod-mail_1.14.0-0ubuntu1.6_amd64.deb ...
Unpacking libnginx-mod-mail (1.14.0-0ubuntu1.6) ...
Selecting previously unselected package libnginx-mod-stream.
Preparing to unpack .../15-libnginx-mod-stream_1.14.0-0ubuntu1.6_amd64.deb ...
Unpacking libnginx-mod-stream (1.14.0-0ubuntu1.6) ...
Selecting previously unselected package nginx-core.
Preparing to unpack .../16-nginx-core_1.14.0-0ubuntu1.6_amd64.deb ...
Unpacking nginx-core (1.14.0-0ubuntu1.6) ...
Selecting previously unselected package nginx.
Preparing to unpack .../17-nginx_1.14.0-0ubuntu1.6_all.deb ...
Unpacking nginx (1.14.0-0ubuntu1.6) ...
Setting up libjbig0:amd64 (2.1-3.1build1) ...
Setting up fonts-dejavu-core (2.37-1) ...
Setting up nginx-common (1.14.0-0ubuntu1.6) ...
Created symlink /etc/systemd/system/multi-user.target.wants/nginx.service → /lib/systemd/system/nginx.service.
Setting up libjpeg-turbo8:amd64 (1.5.2-0ubuntu5.18.04.1) ...
Setting up libnginx-mod-mail (1.14.0-0ubuntu1.6) ...
Setting up libxpm4:amd64 (1:3.5.12-1) ...
Setting up libnginx-mod-http-xslt-filter (1.14.0-0ubuntu1.6) ...
Setting up libnginx-mod-http-geoip (1.14.0-0ubuntu1.6) ...
Setting up libwebp6:amd64 (0.6.1-2) ...
Setting up libjpeg8:amd64 (8c-2ubuntu8) ...
Setting up fontconfig-config (2.12.6-0ubuntu2) ...
Setting up libnginx-mod-stream (1.14.0-0ubuntu1.6) ...
Setting up libtiff5:amd64 (4.0.9-5ubuntu0.2) ...
Setting up libfontconfig1:amd64 (2.12.6-0ubuntu2) ...
Setting up libgd3:amd64 (2.2.5-4ubuntu0.3) ...
Setting up libnginx-mod-http-image-filter (1.14.0-0ubuntu1.6) ...
Setting up nginx-core (1.14.0-0ubuntu1.6) ...
Setting up nginx (1.14.0-0ubuntu1.6) ...
Processing triggers for systemd (237-3ubuntu10.28) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for ufw (0.36-0ubuntu0.18.04.1) ...
Processing triggers for ureadahead (0.100.0-21) ...
Processing triggers for libc-bin (2.27-3ubuntu1) ...

4. посмотрел состав установленного продукта:

root@ubuntu:~# more /etc/nginx

**** /etc/nginx: directory ****

root@ubuntu:~# ls -l /etc/nginx
total 64
drwxr-xr-x 2 root root 4096 Aug 20 12:46 conf.d
-rw-r--r-- 1 root root 1077 Apr 6 2018 fastcgi.conf
-rw-r--r-- 1 root root 1007 Apr 6 2018 fastcgi_params
-rw-r--r-- 1 root root 2837 Apr 6 2018 koi-utf
-rw-r--r-- 1 root root 2223 Apr 6 2018 koi-win
-rw-r--r-- 1 root root 3957 Apr 6 2018 mime.types
drwxr-xr-x 2 root root 4096 Aug 20 12:46 modules-available
drwxr-xr-x 2 root root 4096 Sep 7 14:58 modules-enabled
-rw-r--r-- 1 root root 1482 Apr 6 2018 nginx.conf
-rw-r--r-- 1 root root 180 Apr 6 2018 proxy_params
-rw-r--r-- 1 root root 636 Apr 6 2018 scgi_params
drwxr-xr-x 2 root root 4096 Sep 7 14:58 sites-available
drwxr-xr-x 2 root root 4096 Sep 7 14:58 sites-enabled
drwxr-xr-x 2 root root 4096 Sep 7 14:58 snippets
-rw-r--r-- 1 root root 664 Apr 6 2018 uwsgi_params
-rw-r--r-- 1 root root 3071 Apr 6 2018 win-utf

root@ubuntu:~# ls /etc/nginx
conf.d fastcgi_params koi-win modules-available nginx.conf scgi_params sites-enabled uwsgi_params
fastcgi.conf koi-utf mime.types modules-enabled proxy_params sites-available snippets win-utf

root@ubuntu:~# ls /etc/nginx
conf.d fastcgi_params koi-win modules-available nginx.conf scgi_params sites-enabled uwsgi_params
fastcgi.conf koi-utf mime.types modules-enabled proxy_params sites-available snippets win-utf

5. Проверил наличие конфигурационных файлов и каталогов, с которыми предстояло работать.

root@ubuntu:~# more /etc/nginx/conf.d/ppp.conf
more: stat of /etc/nginx/conf.d/ppp.conf failed: No such file or directory
root@ubuntu:~# ls -l /data/www
ls: cannot access '/data/www': No such file or directory ## -- **Не обнаружил.**

6. Создал всю необходимую структуру.

root@ubuntu:~# ls -l /data/www/
total 8
drwxr-xr-x 2 root root 4096 Sep 7 15:13 safe
drwxr-xr-x 2 root root 4096 Sep 7 15:14 unsafe
root@ubuntu:~#
root@ubuntu:~# touch /data/www/safe/index.html
root@ubuntu:~# touch /data/www/unsafe/index.html
root@ubuntu:~# ls -l /data/www/safe
total 0
-rw-r--r-- 1 root root 0 Sep 7 15:19 index.html

root@ubuntu:~# ls -l /data/www/unsafe
total 0
-rw-r--r-- 1 root root 0 Sep 7 15:19 index.html

root@ubuntu:~# touch /etc/apparmor.d/usr.bin.nginx

7. Направился по ложному пути, положась на волю случая,
что удастся создать профайл для nginx в ручную:
root@ubuntu:~# vi /etc/apparmor.d/usr.bin.nginx

#include <tunables/global>

/usr/sbin/nginx {
#include <abstractions/base>
#include <abstractions/lxc/container-base>
capability dac_override,
capability dac_read_search,
capability dac_net_bind_service,
capability setgid,
capability setuid,

/data/www/safe/ r,*
deny /data/www/unsafe/ r,*
/etc/group r,
/etc/nginx/conf.d/ r,
/etc/nginx/mime.types r,
/etc/nginx/nginx.conf r,
/etc/nsswitch.conf r,
/etc/passwd r,
/etc/ssl/openssl.cnf r,
/run/nginx.pid rw,
/usr/sbin/nginx mr,
/var/log/nginx/access.log w,
/var/log/nginx/error.log w,
}

8. Узнал свой ip-адрес, для подключения через curl.

root@ubuntu:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 02:a9:3e:be:bb:aa brd ff:ff:ff:ff:ff:ff
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3

valid_lft 80691sec preferred_lft 80691sec
inet6 fe80::a9:3eff:febe:bbaa/64 scope link
valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:26:8f:22 brd ff:ff:ff:ff:ff:ff
inet 192.168.55.12/24 brd 192.168.55.255 scope global enp0s8
valid_lft forever preferred_lft forever
inet6 fe80::a00:27ff:fe26:8f22/64 scope link
valid_lft forever preferred_lft forever

9. Провёл запуск nginx

root@ubuntu:~# systemctl start nginx
root@ubuntu:~# systemctl status nginx

● *nginx.service - A high performance web server and a reverse proxy server*
Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
Active: active (running) since Sat 2019-09-07 14:58:29 UTC; 1h 21min ago
Docs: man:nginx(8)
Main PID: 3546 (nginx)
Tasks: 2 (limit: 4703)
CGroup: /system.slice/nginx.service
├─3546 nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
└─3547 nginx: worker process

Sep 07 14:58:29 ubuntu systemd[1]: Starting A high performance web server and a reverse proxy server...
Sep 07 14:58:29 ubuntu systemd[1]: nginx.service: Failed to parse PID from file /run/nginx.pid: Invalid argument
Sep 07 14:58:29 ubuntu systemd[1]: Started A high performance web server and a reverse proxy server.

10. Посмотрел статус Apparmor:

root@ubuntu:~# systemctl status apparmor

● *apparmor.service - AppArmor initialization*
Loaded: loaded (/lib/systemd/system/apparmor.service; enabled; vendor preset: enabled)
Active: active (exited) since Sat 2019-09-07 14:41:00 UTC; 1h 38min ago
Docs: man:apparmor(7)
http://wiki.apparmor.net/
Main PID: 531 (code=exited, status=0/SUCCESS)
Tasks: 0 (limit: 4703)
CGroup: /system.slice/apparmor.service

Sep 07 14:40:59 ubuntu systemd[1]: Starting AppArmor initialization...
*Sep 07 14:40:59 ubuntu apparmor[531]: * Starting AppArmor profiles*
Sep 07 14:41:00 ubuntu apparmor[531]: Skipping profile in /etc/apparmor.d/disable: usr.sbin.rsyslogd
Sep 07 14:41:00 ubuntu apparmor[531]: ...done.
Sep 07 14:41:00 ubuntu systemd[1]: Started AppArmor initialization.

root@ubuntu:~# systemctl restart apparmor
Job for apparmor.service failed because the control process exited with ***error code.***
See "systemctl status apparmor.service" and "journalctl -xe" for details.

root@ubuntu:~# curl http://192.168.55.12:8080/safe
curl: (7) Failed to connect to 192.168.55.12 port 8080: Connection refused

root@ubuntu:~# curl http://192.168.55.12:80/safe
<html>
<head><title>404 Not Found</title></head>
<body bgcolor="white">
* <h1>404 Not Found</h1> *
*<hr> nginx/1.14.0 (Ubuntu) *
</body>
</html>
root@ubuntu:~#

11. Увидев ошибку, обратился в журнал за деталями.

root@ubuntu:~# journalctl -xe
Sep 07 16:20:40 ubuntu audit[4195]: AVC apparmor="STATUS" operation="profile_replace" profile="unconfined" name="lxc-container-default-with-mounting" pid=4195
Sep 07 16:20:40 ubuntu audit[4195]: AVC apparmor="STATUS" operation="profile_replace" profile="unconfined" name="lxc-container-default-with-nesting" pid=4195
Sep 07 16:20:40 ubuntu audit[4197]: AVC apparmor="STATUS" operation="profile_replace" profile="unconfined" name="/sbin/dhclient" pid=4197 comm="apparmor_parse
Sep 07 16:20:40 ubuntu audit[4197]: AVC apparmor="STATUS" operation="profile_replace" profile="unconfined" name="/usr/lib/NetworkManager/nm-dhcp-client.action
Sep 07 16:20:40 ubuntu audit[4197]: AVC apparmor="STATUS" operation="profile_replace" profile="unconfined" name="/usr/lib/NetworkManager/nm-dhcp-helper" pid=4
Sep 07 16:20:40 ubuntu audit[4197]: AVC apparmor="STATUS" operation="profile_replace" profile="unconfined" name="/usr/lib/connman/scripts/dhclient-script" pid
Sep 07 16:20:40 ubuntu audit[4199]: AVC apparmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined" name="/usr
Sep 07 16:20:40 ubuntu audit[4201]: AVC apparmor="STATUS" operation="profile_replace" profile="unconfined" name="/usr/bin/man" pid=4201 comm="apparmor_parser"
Sep 07 16:20:40 ubuntu audit[4201]: AVC apparmor="STATUS" operation="profile_replace" profile="unconfined" name="man_filter" pid=4201 comm="apparmor_parser"
Sep 07 16:20:40 ubuntu audit[4201]: AVC apparmor="STATUS" operation="profile_replace" profile="unconfined" name="man_groff" pid=4201 comm="apparmor_parser"
Sep 07 16:20:40 ubuntu apparmor[4142]: AppArmor parser error for /etc/apparmor.d/usr.bin.nginx in /etc/apparmor.d/usr.bin.nginx at line 8: Invalid capability --
Поняв ошибку, переместил файл профиля в другое местоположение.
Sep 07 16:20:40 ubuntu audit[4205]: AVC apparmor="STATUS" operation="profile_replace" profile="unconfined" name="/usr/lib/snapd/snap-confine" pid=4205 comm="a
Sep 07 16:20:40 ubuntu audit[4205]: AVC apparmor="STATUS" operation="profile_replace" profile="unconfined" name="/usr/lib/snapd/snap-confine//mount-namespace-
Sep 07 16:20:40 ubuntu apparmor[4142]: Skipping profile in /etc/apparmor.d/disable: usr.sbin.rsyslogd
Sep 07 16:20:40 ubuntu audit[4209]: AVC apparmor="STATUS" operation="profile_replace"

info="same as current profile, skipping" profile="unconfined" name="/usr
Sep 07 16:20:40 ubuntu apparmor[4142]: ...fail!
Sep
07 16:20:40 ubuntu systemd[1]: apparmor.service: Main process exited, code=exited, status=123/n/a
Sep 07 16:20:40 ubuntu systemd[1]: apparmor.service: Failed with result 'exit-code'.
Sep 07 16:20:40 ubuntu systemd[1]: Failed to start AppArmor initialization.
-- Subject: Unit apparmor.service has failed
-- Defined-By: systemd
-- Support: http://www.ubuntu.com/support
--
-- Unit apparmor.service has failed.
--
-- The result is RESULT.

12. Установил утилиты, требуемые apparmor для генерирования корректного профайла:

root@ubuntu:~# sudo apt-get install apparmor-utils

Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
python3-apparmor python3-libapparmor
Suggested packages:
vim-addon-manager
The following NEW packages will be installed:
apparmor-utils python3-apparmor python3-libapparmor
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 157 kB of archives.
After this operation, 961 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 python3-libapparmor amd64 2.12-4ubuntu5.1 [26.8 kB]
Get:2 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 python3-apparmor amd64 2.12-4ubuntu5.1 [79.5 kB]
Get:3 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 apparmor-utils amd64 2.12-4ubuntu5.1 [50.6 kB]
Fetched 157 kB in 1s (147 kB/s)
Selecting previously unselected package python3-libapparmor.
(Reading database ... 90849 files and directories currently installed.)
Preparing to unpack .../python3-libapparmor_2.12-4ubuntu5.1_amd64.deb ...
Unpacking python3-libapparmor (2.12-4ubuntu5.1) ...
Selecting previously unselected package python3-apparmor.
Preparing to unpack .../python3-apparmor_2.12-4ubuntu5.1_amd64.deb ...
Unpacking python3-apparmor (2.12-4ubuntu5.1) ...
Selecting previously unselected package apparmor-utils.
Preparing to unpack .../apparmor-utils_2.12-4ubuntu5.1_amd64.deb ...
Unpacking apparmor-utils (2.12-4ubuntu5.1) ...
Setting up python3-libapparmor (2.12-4ubuntu5.1) ...
Setting up python3-apparmor (2.12-4ubuntu5.1) ...

Setting up apparmor-utils (2.12-4ubuntu5.1) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) …

13. Сгенерировал корректный профайл.

root@ubuntu:~# sudo aa-autodep nginx
Writing updated profile for /usr/sbin/nginx.

root@ubuntu:~# ls -l /etc/apparmor.d

total 80
drwxr-xr-x 5 root root 4096 Aug 28 15:50 abstractions
drwxr-xr-x 2 root root 4096 Sep 7 16:20 cache
drwxr-xr-x 2 root root 4096 Aug 28 15:49 disable
drwxr-xr-x 2 root root 4096 Apr 24 2018 force-complain
drwxr-xr-x 2 root root 4096 Aug 28 15:50 local
drwxr-xr-x 2 root root 4096 Aug 28 15:50 lxc
-rw-r--r-- 1 root root   198 Nov 23 2018 lxc-containers
-rw-r--r-- 1 root root 3194 Mar 26 2018 sbin.dhclient
drwxr-xr-x 5 root root 4096 Aug 28 15:50 tunables
-rw-r--r-- 1 root root   125 Nov 23 2018 usr.bin.lxc-start
-rw-r--r-- 1 root root 2857 Apr 7 2018 usr.bin.man
-rw-r--r-- 1 root root 23754 Jul 12 08:40 usr.lib.snapd.snap-confine.real
-rw------- 1 root root   198 Sep 7 17:16 usr.sbin.nginx Не те разрешения!!!
-rw-r--r-- 1 root root 1550 Apr 24 2018 usr.sbin.rsyslogd
-rw-r--r-- 1 root root 1353 Mar 31 2018 usr.sbin.tcpdump

13. Убедился в корректности разрешений:

root@ubuntu:~# chmod 755 /etc/apparmor.d
root@ubuntu:~# chmod 755 /etc/apparmor.d/usr.sbin.nginx
root@ubuntu:~# chmod -x /etc/apparmor.d/usr.sbin.nginx
root@ubuntu:~# ls -l /etc/apparmor.d

total 80
drwxr-xr-x 5 root root 4096 Aug 28 15:50 abstractions
drwxr-xr-x 2 root root 4096 Sep 7 16:20 cache
drwxr-xr-x 2 root root 4096 Aug 28 15:49 disable
drwxr-xr-x 2 root root 4096 Apr 24 2018 force-complain
drwxr-xr-x 2 root root 4096 Aug 28 15:50 local
drwxr-xr-x 2 root root 4096 Aug 28 15:50 lxc
-rw-r--r-- 1 root root   198 Nov 23 2018 lxc-containers
-rw-r--r-- 1 root root 3194 Mar 26 2018 sbin.dhclient
drwxr-xr-x 5 root root 4096 Aug 28 15:50 tunables
-rw-r--r-- 1 root root   125 Nov 23 2018 usr.bin.lxc-start
-rw-r--r-- 1 root root 2857 Apr 7 2018 usr.bin.man
-rw-r--r-- 1 root root 23754 Jul 12 08:40 usr.lib.snapd.snap-confine.real
-rw-r--r-- 1 root root   198 Sep 7 17:16 usr.sbin.nginx
-rw-r--r-- 1 root root 1550 Apr 24 2018 usr.sbin.rsyslogd
-rw-r--r-- 1 root root 1353 Mar 31 2018 usr.sbin.tcpdump

14. Отредактировал профиль, добавив необходимые настройки из профайла пункта 7.

root@ubuntu:~# vi /etc/apparmor.d/usr.sbin.nginx

15. Попытка перезагрузки профилья увенчалась ошибкой

root@ubuntu:~# sudo aa-genprof /etc/apparmor.d/usr.sbin.nginx

Writing updated profile for /etc/apparmor.d/usr.sbin.nginx.
Setting /usr.sbin.nginx to complain mode.

***ERROR**: /etc/apparmor.d/usr.sbin.nginx contains no profile*
root@ubuntu:~#

16. Попытка перекомпиляции указала номер ошибочной строки в профайле.

root@ubuntu:~# sudo aa-complain /etc/apparmor.d/usr.sbin.nginx

Setting /etc/apparmor.d/usr.sbin.nginx to complain mode.

ERROR:** AppArmor parser error for /etc/apparmor.d/usr.sbin.nginx in /etc/apparmor.d/usr.sbin.nginx **at line 9: Invalid capability dac_net_bind_service.

root@ubuntu:~# vi /etc/apparmor.d/usr.sbin.nginx

17. Отладив ошибку, получили следущее:

```
# Last Modified: Sat Sep  7 17:16:03 2019
#include <tunables/global>

/usr/sbin/nginx flags=(complain) {
  #include <abstractions/base>
  #include <abstractions/lxc/container-base>
 capability dac_override,
 capability dac_read_search,
 #capability dac_net_bind_service, -- Ошибочная строка!!!
 capability setgid,
 capability setuid,


  /lib/x86_64-linux-gnu/ld-*.so mr,
  /usr/sbin/nginx mr,
  /data/www/safe/* r,
deny /data/www/unsafe/* r,
/etc/group r,
/etc/nginx/conf.d/ r,
/etc/nginx/mime.types r,
/etc/nginx/nginx.conf r,
/etc/nsswitch.conf r,
/etc/passwd r,
/etc/ssl/openssl.cnf r,
/run/nginx.pid rw,
/usr/sbin/nginx mr,
/var/log/nginx/access.log w,
```

/var/log/nginx/error.log w,

}

root@ubuntu:~# sudo aa-complain /etc/apparmor.d/usr.sbin.nginx
Setting /etc/apparmor.d/usr.sbin.nginx to complain mode.
root@ubuntu:~# sudo service apparmor reload
apparmor.service is not active, cannot reload.
root@ubuntu:~#

root@ubuntu:~# journalctl -xe
Sep 07 17:16:03 ubuntu audit[4551]: AVC apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/sbin/nginx" pid=4551 comm="apparmor_parser"
Sep 07 17:16:03 ubuntu kernel: kauditd_printk_skb: 20 callbacks suppressed
Sep 07 17:16:03 ubuntu kernel: audit: type=1400 audit(1567876563.190:49): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/sbin/ngin
Sep 07 17:16:03 ubuntu sudo[4420]: pam_unix(sudo:session): session closed for user root
Sep 07 17:17:01 ubuntu CRON[4566]: pam_unix(cron:session): session opened for user root by (uid=0)
Sep 07 17:17:01 ubuntu CRON[4567]: (root) CMD (cd / && run-parts --report /etc/cron.hourly)
Sep 07 17:17:01 ubuntu CRON[4566]: pam_unix(cron:session): session closed for user root
Sep 07 17:28:31 ubuntu sudo[4580]:   root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/usr/sbin/aa-genprof /etc/apparmor.d/usr.sbin.nginx
Sep 07 17:28:31 ubuntu sudo[4580]: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 07 17:28:31 ubuntu sudo[4580]: pam_unix(sudo:session): session closed for user root
Sep 07 17:31:44 ubuntu sudo[4586]:   root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/usr/sbin/service apparmor reload
Sep 07 17:31:44 ubuntu sudo[4586]: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 07 17:31:45 ubuntu systemd[1]: apparmor.service: Unit cannot be reloaded because it is inactive.
Sep 07 17:31:45 ubuntu sudo[4586]: pam_unix(sudo:session): session closed for user root
Sep 07 17:33:53 ubuntu sudo[4594]:   root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/usr/sbin/aa-complain /etc/apparmor.d/usr.sbin.nginx
Sep 07 17:33:53 ubuntu sudo[4594]: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 07 17:33:53 ubuntu sudo[4594]: pam_unix(sudo:session): session closed for user root
Sep 07 17:35:46 ubuntu sudo[4600]:   root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/usr/sbin/aa-complain /etc/apparmor.d/usr.sbin.nginx
Sep 07 17:35:46 ubuntu sudo[4600]: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)
Sep 07 17:35:46 ubuntu audit[4603]: AVC apparmor="STATUS" operation="profile_replace" profile="unconfined" name="/usr/sbin/nginx" pid=4603 comm="apparmor_pars
Sep 07 17:35:46 ubuntu kernel: audit: type=1400 audit(1567877746.970:50): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="/usr/sbin/n
Sep 07 17:35:46 ubuntu sudo[4600]: pam_unix(sudo:session): session closed for user root
Sep 07 17:36:05 ubuntu sudo[4604]:   root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/usr/sbin/service apparmor reload
Sep 07 17:36:05 ubuntu sudo[4604]: pam_unix(sudo:session): session opened for user root by vagrant(uid=0)

Sep 07 17:36:05 ubuntu systemd[1]: apparmor.service: Unit cannot be reloaded because it is inactive.
Sep 07 17:36:05 ubuntu sudo[4604]: pam_unix(sudo:session): session closed for user root

18. перезагрузили ПК, для применения всех изменений:
root@ubuntu:~# shutdown -h now

19. Проверили выполнение всех наших настроек после перезагрузки.

labuzhskiy@MINT-LIN-CIN-X64 ~/.vagrant.d/boxes/4lesson-dz $ curl http://192.168.55.12:8080/safe/
<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<centre><h1>301 Moved Permanently</h1></centre>
<hr><centre>nginx/1.14.0 (Ubuntu)</centre>
</body>
</html>

Работает. *Копии конфигов прилагаю. архивами o2.tar.gz (для Pam.d), polkitd.tar.gz (для PolicyKit-1), usr.sbin.nginx.tar.gz (для Apparmor), SSH_Chroot.tar.gz(Chroot для учётной записи Otus3).*