EPAM University Programs

DevOps external course

Module 4 Linux & Bash Essentials

TASK 4.5

1. To discover files with active sticky bits, use the following version of the **find** command:

sudo find / -perm /6000 -type f -exec ls -ld {} \;>setuid.txt

Put into your report a fragment of setuid.txt file. Explain meaning of parameters of the above **find** command (hint: use find's man page).

```
user@user-VirtualBox:~/tmp/dir1$ cat setuid.txt |more
-rwsr-xr-x 1 root root 44664 бер 22  2019 /bin/su
-rwsr-xr-x 1 root root 64424 чер 28  2019 /bin/ping
-rwsr-xr-x 1 root root 26696 січ  8 20:31 /bin/umount
-rwsr-xr-x 1 root root 43088 січ  8 20:31 /bin/mount
-rwsr-xr-x 1 root root 30800 сер 11  2016 /bin/fusermount
-rwsr-xr-x 1 root root 40152 жов 10  2019 /snap/core/8268/bin/mount
-rwsr-xr-x 1 root root 44168 тра  7  2014 /snap/core/8268/bin/ping
-rwsr-xr-x 1 root root 44680 тра  7  2014 /snap/core/8268/bin/ping6
-rwsr-xr-x 1 root root 40128 бер 25  2019 /snap/core/8268/bin/su
-rwsr-xr-x 1 root root 27608 жов 10  2019 /snap/core/8268/bin/umount
-rwxr-sr-x 1 root shadow 35632 кві  9  2018 /snap/core/8268/sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root shadow 35600 кві  9  2018 /snap/core/8268/sbin/unix_chkpwd
-rwxr-sr-x 1 root shadow 62336 бер 25  2019 /snap/core/8268/usr/bin/chage
-rwsr-xr-x 1 root root 71824 бер 25  2019 /snap/core/8268/usr/bin/chfn
-rwsr-xr-x 1 root root 40432 бер 25  2019 /snap/core/8268/usr/bin/chsh
-rwxr-sr-x 1 root systemd-network 36080 кві  6  2016 /snap/core/8268/usr/bin/crontab
-rwxr-sr-x 1 root mail 14856 гру  7  2013 /snap/core/8268/usr/bin/dotlockfile
-rwxr-sr-x 1 root shadow 22768 бер 25  2019 /snap/core/8268/usr/bin/expiry
-rwsr-xr-x 1 root root 75304 бер 25  2019 /snap/core/8268/usr/bin/gpasswd
-rwxr-sr-x 3 root mail 14592 гру  4  2012 /snap/core/8268/usr/bin/mail-lock
-rwxr-sr-x 3 root mail 14592 гру  4  2012 /snap/core/8268/usr/bin/mail-touchlock
-rwxr-sr-x 3 root mail 14592 гру  4  2012 /snap/core/8268/usr/bin/mail-unlock
-rwsr-xr-x 1 root root 39904 бер 25  2019 /snap/core/8268/usr/bin/newgrp
-rwsr-xr-x 1 root root 54256 бер 25  2019 /snap/core/8268/usr/bin/passwd
-rwxr-sr-x 1 root crontab 358624 бер  4  2019 /snap/core/8268/usr/bin/ssh-agent
-rwsr-xr-x 1 root root 136808 жов 11  2019 /snap/core/8268/usr/bin/sudo
-rwxr-sr-x 1 root tty 27368 жов 10  2019 /snap/core/8268/usr/bin/wall
-rwsr-xr-- 1 root systemd-resolve 42992 чер 10  2019 /snap/core/8268/usr/lib/dbus-1.0/dbus-daemon-
-rwsr-xr-x 1 root root 428240 бер  4  2019 /snap/core/8268/usr/lib/openssh/ssh-keysign
```

The explanation for the parameters:

/ -- starting point

-perm /mode -- Any of the permission bits mode are set for the file. Symbolic modes are accepted in this form. You must specify `u', `g' or `o' if you use a symbolic mode.

-type f -- File is of type: regular file

-exec command ;

Execute command; true if 0 status is returned. All following arguments to find are taken to be arguments to the command until an argument consisting of `;' is encountered. The string `{}' is replaced by the current file name being processed everywhere it occurs in the arguments to the command, not just in arguments where it is alone, as in some versions of find. Both of these constructions might need to be escaped (with a `\') or quoted to protect them from expansion by the shell. The specified command is run once for each matched file. The command is executed in the starting directory.

> -- output redirection

2. Discovering soft and hard links.

Comment on results of these commands (place the output into your report):

cd

mkdir test

cd test

touch test1.txt

echo “test1.txt” > test1.txt

ls -l .

(a hard link)

ln test1.txt test2.txt

ls -l .

(pay attention to the number of links to test1.txt and test2.txt)

echo “test2.txt” > test2.txt

cat test1.txt test2.txt

rm test1.txt

ls -l .

(now a soft link)

ln -s test2.txt test3.txt

ls -l .

(pay attention to the number of links to the created files)

rm test2.txt; **ls** -l .

```
user@user-VirtualBox:~/test$ touch test1.txt
user@user-VirtualBox:~/test$ echo 'test1.txt' > test1.txt
user@user-VirtualBox:~/test$ cat test1.txt
test1.txt
user@user-VirtualBox:~/test$ ls -l .
total 4
-rw-r--r-- 1 user user 10 кві 21 23:53 test1.txt
-rw-r--r-- 1 user user  0 кві 16 23:50 test2.txt
-rw-r--r-- 1 user user  0 кві 16 23:50 test.txt
user@user-VirtualBox:~/test$ rm test2.txt
user@user-VirtualBox:~/test$ rm test.txt
user@user-VirtualBox:~/test$ ls -l .
total 4
-rw-r--r-- 1 user user 10 кві 21 23:53 test1.txt
user@user-VirtualBox:~/test$ ln test1.txt test2.txt
user@user-VirtualBox:~/test$ ls -l .
total 8
-rw-r--r-- 2 user user 10 кві 21 23:53 test1.txt
-rw-r--r-- 2 user user 10 кві 21 23:53 test2.txt
user@user-VirtualBox:~/test$ echo 'test2.txt' > test2.txt
user@user-VirtualBox:~/test$ cat test1.txt test2.txt
test2.txt
test2.txt
user@user-VirtualBox:~/test$ rm test1.txt
user@user-VirtualBox:~/test$ ls -l .
total 4
-rw-r--r-- 1 user user 10 кві 21 23:57 test2.txt
user@user-VirtualBox:~/test$ ln -s test2.txt test3.txt
```

```
user@user-VirtualBox:~/test$ ln -s test2.txt test3.txt
user@user-VirtualBox:~/test$ ls -l .
total 4
-rw-r--r-- 1 user user 10 кві 21 23:57 test2.txt
lrwxrwxrwx 1 user user  9 кві 22 00:09 test3.txt -> test2.txt
user@user-VirtualBox:~/test$ rm test2.txt
user@user-VirtualBox:~/test$ ls -l .
total 0
lrwxrwxrwx 1 user user 9 кві 22 00:09 test3.txt -> test2.txt
user@user-VirtualBox:~/test$
```

The above commands serve as an example for soft and hard links, we were able to create both types of links and see the difference between them.

3. I/O redirect.

Execute these commands; comment on the output.

mount

```
user@user-VirtualBox:~/test$
user@user-VirtualBox:~/test$ mount
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,nosuid,relatime,size=1507976k,nr_inodes=376994,mode=755)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,noexec,relatime,size=306464k,mode=755)
/dev/sda1 on / type ext4 (rw,relatime,errors=remount-ro)
```

The **mount** command instructs the operating system that a file system is ready to use, and associates it with a particular point in the overall file system hierarchy (its *mount point*) and sets options relating to its access. Mounting makes file systems, files, directories, devices and special files available for use and available to the user. Its counterpart **umount** instructs the operating system that the file system should be disassociated from its mount point, making it no longer accessible and may be removed from the computer. It is important to **umount** a device before removing it since changes to files may have only partially been written and are completed as part of the **umount**.

The 'mount' with no options displays all currently mounted FS, their type/mount point and associated options.

blkid

```
user@user-VirtualBox:~/test$ blkid
/dev/sda1: UUID="4acf8985-7b5d-4d43-a671-9743d734105c" TYPE="ext4" PARTUUID="b962fac8-01"
/dev/sr0: UUID="2020-02-18-17-20-05-35" LABEL="VBox_GAs_6.1.4" TYPE="iso9660"
user@user-VirtualBox:~/test$
```

The **blkid** program is the command-line interface to working with **libuuid**(3) library. It can determine the type of content (e.g. filesystem, swap) a block device holds, and also attributes (tokens, NAME=value pairs) from the content metadata (e.g. LABEL or UUID fields).

blkid has two main forms of operation: either searching for a device with a specific NAME=value pair, or displaying NAME=value pairs for one or more devices.

mount | **grep** sda

```
user@user-VirtualBox:~/test$ mount | grep sda
/dev/sda1 on / type ext4 (rw,relatime,errors=remount-ro)
user@user-VirtualBox:~/test$
```

Display only those entries from 'mount' command that match the 'sda' pattern

dmesg | **grep** sda

```
user@user-VirtualBox:~/test$ dmesg | grep sda
[    2.736667] sd 2:0:0:0: [sda] 33313888 512-byte logical blocks: (17.1 GB/15.9 GiB)
[    2.736689] sd 2:0:0:0: [sda] Write Protect is off
[    2.736693] sd 2:0:0:0: [sda] Mode Sense: 00 3a 00 00
[    2.736730] sd 2:0:0:0: [sda] Write cache: enabled, read cache: enabled, doesn't support DPO or FUA
[    2.737613]  sda: sda1
[    2.738192] sd 2:0:0:0: [sda] Attached SCSI disk
[    3.596644] EXT4-fs (sda1): mounted filesystem with ordered data mode. Opts: (null)
[    4.165269] EXT4-fs (sda1): re-mounted. Opts: errors=remount-ro
user@user-VirtualBox:~/test$
```

Same as above, only this outputs 'sda'-related entries from message buffer of the kernel

sudo grep -R -e "root" /etc > root_entries.txt

(place only a reasonable fragment of root_entries.txt into your report)

```
/etc/dbus-1/system.d/com.redhat.PrinterDriversInstaller.conf:   <policy user="root">
/etc/dbus-1/system.d/com.redhat.PrinterDriversInstaller.conf:   <policy user="root">
/etc/dbus-1/system.d/org.freedesktop.UDisks2.conf:  <!-- Only root can own the service -->
/etc/dbus-1/system.d/org.freedesktop.UDisks2.conf:  <policy user="root">
/etc/dbus-1/system.d/com.hp.hplip.conf:  <!-- Only root can own the service -->
/etc/dbus-1/system.d/com.hp.hplip.conf:  <policy user="root">
/etc/dbus-1/system.d/org.freedesktop.RealtimeKit1.conf:  <policy user="root">
/etc/dbus-1/system.d/org.freedesktop.RealtimeKit1.conf:  <policy user="root">
/etc/dbus-1/system.d/com.ubuntu.USBCreator.conf:  <!-- Only root can own the service -->
/etc/dbus-1/system.d/com.ubuntu.USBCreator.conf:  <policy user="root">
/etc/dbus-1/system.d/org.freedesktop.NetworkManager.conf:        <policy user="root">
/etc/dbus-1/system.d/gdm.conf:  <!-- Only root can own the service -->
/etc/dbus-1/system.d/gdm.conf:  <policy user="root">
/etc/dbus-1/system.d/nm-pptp-service.conf:      <policy user="root">
/etc/dbus-1/system.d/dnsmasq.conf:      <policy user="root">
/etc/dbus-1/system.d/org.freedesktop.fwupd.conf:  <!-- Only user root can own the fwupd service -->
/etc/dbus-1/system.d/org.freedesktop.fwupd.conf:  <policy user="root">
/etc/dbus-1/system.d/org.freedesktop.PolicyKit1.conf:  <policy user="root">
/etc/dbus-1/system.d/org.freedesktop.PolicyKit1.conf:  <policy user="root">
/etc/dbus-1/system.d/org.freedesktop.bolt.conf:  <policy user="root">
/etc/dbus-1/system.d/org.freedesktop.GeoClue2.Agent.conf:  <policy user="root">
/etc/dbus-1/system.d/com.ubuntu.LanguageSelector.conf:        <policy user="root">
/etc/services:rootd             1094/tcp
/etc/services:rootd             1094/udp
/etc/updatedb.conf:PRUNEPATHS="/tmp /var/spool /media /var/lib/os-prober /var/lib/ceph /home/.ecryptfs /var/lib/schroot"
/etc/containerd/config.toml:#root = "/var/lib/containerd"
/etc/shadow-:root:!:18352:0:99999:7:::
/etc/X11/Xwrapper.config:# again, run the following command as root:
/etc/X11/Xreset.d/README:# Scripts in this directory are executed as root when a user log out from
user@user-VirtualBox:~/test$
```


Search for 'root' pattern in all files recursively starting from /etc, output redirected to a file.