Security in Mobile Systems - UE/EX

FH Hagenberg, WS 2017
DI Dr. Erik Sonnleitner

Exercise 2: Linux Shell Basics I

Exercise 2: Basic Linux Shell

(1) Explain the meaning and syntactic representation of the third and fifth fields of the `/etc/shadow` file. With what shell program can these fields be altered (without manually editing the shadow file)? Give an example command which changes the fifth field.

(2) In your home directory, create a sub-directory for backing up the contents of `/etc/`. Make sure, that the copied files show the exact same a) file permissions and b) file modification time stamps.

(3) You would like to mount an external hard-drive located at `/dev/sdd1` to `/mnt/myhdd` with the following constraints:

- The file-access timestamp of all file-system objects located on the HDD should never be altered.
- Executing programs located on this HDD should not be allowed.
- Disallow setting SUID ot GUID bits.

(4) Find a way to establish a disk usage quota on per-user basis (i.e., as administrator, you define that a particular user *bob* must not use more than e.g. 3 gigabytes of storage).

(5) What exactly does the following command do?

```
time find / -type d >/dev/null 2>&1
```

Exercise 2: Basic Linux Shell

(6) Create an `ls` command with proper arguments, to make the last-modified timestamp appear like in the following example (note recently modified objects show exact time, while older ones show full date including year):

```
-rw-r--r-- 1 eso users 161  2016-09-08  Makefile
-rw-r--r-- 1 eso users 4.6K 2016-10-31  cheatsheet.txt
-rw-r--r-- 1 eso users 132K 08-28 13:57 ex2.pdf
-rw-r--r-- 1 eso users 7.0K 08-28 13:57 ex2.tex
-rw-r--r-- 1 eso users 907  2014-10-24  solution
```

(7) Use the `find` command to search for...

- (a) all directories in `/usr/` up to a maximum depth of 3, and store the output in a textfile in your home directory.
- (b) all files on your system without actual content (i.e. zero bytes in size).
- (c) all executable files on the entire system for which either SUID or GUID is set, while suppressing any error messages on the console.

Exercise 2: Basic Linux Shell

(8) Create a new file in your home directory, and change its permissions in octal notation to reflect the following permission triplets:

- (a) `-rw-r--r--`
- (b) `-rwxr-xr-x`
- (c) `-r-xr-----`
- (d) `-r-sr-x---`

Also, describe what those permissions actually mean (who can do what with a file having a particular permission set).

(9) Explain the meaning of Linux signals `SIGHUP`, `SIGCONT`, `SIGALRM`, `SIGSEGV`, `SIGUSR2`.

(10) Utilize text-processing commands in conjunction with pipelining, in order to search your username in the `/etc/passwd` file and subsequently extract the numeric user ID. Your username must not appear in command line statement, use the `whoami` program instead.

(11) Use the `find` and `md5sum` commands in conjunction, in order to create a command which calculates the MD5 hash sum of each executable file on your system.

(12) Find a way to read 100 bytes from the entropy source `/dev/urandom`, and create an MD5 hash from these bytes.

Exercise 2: Basic Linux Shell

(13) Suppose you have a textfile with URLs, one per line. Create a command using the `cat`, `wget` and `xargs` programs, which downloads each URL to the `Downloads` directory in your home folder.

(14) Get to know regular expressions and understand how to effectively use them. In order to do so, visit **`https://regexone.com`**. Make sure to successfully accomplish **all exercises** (consisting of 15 tutorial *lessions* and 8 *problems*).

(15) Download **`http://sms.delta-xi.net/sample_access_log.txt`**, which resembles a sample log-file from the Apache web-server, and construct the correct command lines to answer the following questions (one-liners only):

(a) How many distinct IP source addresses or hostnames are contained in the logfile?
(b) How many HTTP requests other than GET requests have reached the web-server on 08.03.2004 between 20:00 and 23:59?
(c) What size was the largest web-server response answer of all non-GET requests?
(d) How many clients requested the **`robots.txt`** file using HTTP version 1.0, whose source host does not originate from a **`.com`** domain?
(e) How many HTTP **`Not Modified`** responses have been issued?
(f) How many different distinct HTTP status codes except for 200 (OK) and 404 (Not Found) have been issued?