Information systems security
Linux terminal basics

Linux terminal is the environment that, sooner or later, all the IT experts will have to work in (heard that sentence before? :)). To get acquainted with this environment, this laboratory exercise was developed, whose goal is to introduce students to the basics of working with a Linux terminal, as well as to some more advanced commands. The assumption is that the student already knows how to use commands to list the folder contents, change the folder, etc. *PowerShell* in a windows environment can be compared with a Linux terminal because of its advanced capabilities. However, there are similarities to the commands used in Windows command line and Linux environments. The basics learned in the previous exercise will be helpful in today's exercise (especially the trick of using the | (pipe) operator).
Note: Write down all the commands you will use during the exercise (in this document or additional notes document); you will need it for short exams.
IMPORTANT.: Before starting to work on the exercise, make sure to check the document 2_Linux_Shell_Basics.pdf

Linux terminal basics

You can use your own Linux distribution if you like. Recommendation is Kali Linux, since we will be using it later on this semester.

First, install the Apache web server if not installed already (make sure to press ENTER after the command):

`sudo apt update`
`sudo apt install apache2` and follow the instructions on the screen

NOTE: Linux has excellent autocomplete. Use it! How? Type the first few letters of the command and then press TAB. If the autocomplete does not work after that, there are more possible candidates to complete the command, or there is no single candidate – don't panic; press TAB twice, and you will see which candidates they are.
TRY IT:
To change in the `/var/www` folder in the terminal, type `ls /va` and press TAB (autocomplete will type the rest of the path (`r/`).
Press 2x TAB (autocomplete will show you all the options that you can use to continue the command.
Type `ww` and press TAB (autocomplete will type the rest of the path (`w/`).
Press ENTER to position yourself in the directory `/var/www/`.

Viewing files

The `cat` command can display the contents of the files, e.g. `cat [filename]`

Task: display the contents of the `passwd` file in the folder `/etc`/.(Use autocomplete!)

The command that does this independently of the current folder: ________________

Content search is possible with the grep command. The | (pipe) operator allows us to search the text string in the result of the second command. E.g. `cat` *file* `| grep` "*text*" searches for the string "*text*" in the file named "*file*".

Note: The requested string submitted to the grep command should be enclosed in quotation marks if there is a space within the string. Special characters like \, $, etc. have to be escaped (for example, \ will be escaped like this \\, & like this \&).

Task: Using the `grep` command, find the `shadow` string in the result of the `ls /etc/` command.

Answer: ____

Task: If we want to search the string using the `grep` command regardless of uppercase and lowercase letters, it is necessary to use a specific flag with the `grep` command. Check the `grep` command help by using `man grep` or `grep -h`.

Which flag ignores case: _______________

Environment variables

Environment variables define the different parameters that the Linux terminal and its applications use. Environment variables are helpful when scripting at the command line.

To see all the environment variables, we can use a variety of commands (not just a `set` command we used in Windows!).

For example, we can use `printenv` and `env` commands to display all variables, `export` command that allows us to enter, a `set` command that will show the complete program code used to adjust the environment, and `show` command which shows defined variables, etc.

Task: Display all environment variables using the `env` command.

____

Note: Linux is *a case-sensitive* OS, which means that `grep` and `Grep` are NOT the same commands!

What is the content of the USER variable (use the `grep` command to filter only the specified variable)?

____

If we write the variable's name with `printenv`, we will only see the content of that variable, e.g. `printenv USER`. What is the content of the COMPUTER variable:

____

What is the PATH variable used for?

____

What is the content of the PATH variable (Unlike Windows, where we used the `path` command, on Linux OS, we will look for the content of the path variable using the `env` command)?

Watch out for the CASE sensitivity of Linux OS!

____

`service` command

`service` command allows to start and stop of the service. What other commands can we use to achieve this in Linux OS? (If you have studied the presentation 2_Linux_Shell_Basics.pdf, answering this question should be no problem). To start the service, you must use `sudo` before the command because

root privileges are required. You will have to provide a user password, and the user must have sudoers privileges assigned for this to work.
Which command will you use to run apache2 services?

____

What command will you use to check the status of the service (whether it is running or not)?

____

What command will you use to stop apache2 services?

____

DNS is one of the critical services of today's networks. It is almost impossible to surf the Internet without a DNS service. Imagine what happens when you type www.google.hr into the Internet browser – how did you end up on the right website? The answer is (in short) the DNS client service on your computer contacted the DNS servers, learned the corresponding IP address for the specified name, and "converted" the name of www.google.hr into an IP address. Based on that, the Internet browser is directed to www.gooogle.hr. Also, the DNS server can find the name (www.google.hr) based on the IP address (if the so-called reverse lookup zone on the DNS server is configured). The end user does not need to think about DNS service because everything works transparently without user interaction. Sometimes it is necessary to deal with the DNS resolving problems and test DNS operation and configuration. The tool we can use on Linux OS for this purpose is `dig` (`nslookup` is an old command that will be obsolete in future versions of Linux OS).

Task: Get to know how to use the `dig` command. On Windows OS, we used the `nslookup` command. Nslookup is an outdated command on Linux OS, and it is not installed by default on all distributions. Help on Linux can be asked by typing `man` and then the command name or command name and then `--help`.
How can we find the name corresponding to the IP address 1.1.1.1 with the dig tool? How about an IP address corresponding to www.hr?

____
____

Manage usernames and group memberships.

Since this course will deal with (among other things) hacking, it is necessary to know some basic commands for managing users.
On the Linux OS of the new user will be created with the `useradd` command.
Type the `useradd` command and see what parameters can be used with it.
The most straightforward command to create a new user is `useradd` USERNAME (where the USERNAME is the name of the user one wants to create).
Create a user (enter your name instead of USERNAME). What command did you use?

____

Use the `cat` command to display the contents of the `/etc/passwd` file to verify that you have successfully created a new user. What is the content of the last line in the `/etc/passwd` file:

____

Note the figures that follow the username (after the string of characters :x:). They define group membership. If we want to create a new user with root privileges on Linux OS, we need to define the root group affiliation for that user, which is 0. WE SHOULD NEVER be logged on as OS administrators, but this is the simplest way a hacker can create a user with admin privileges. So what is the command to create a new user called "test" with the same rights as the root user on Linux? Google is your friend.

____

Can you change the group membership for the user you created in the previous step (the user you assigned your name to)? How can you achieve this? For example, set the user with the same privileges as the root.
HINT: passwd file, digits, 0 is the root group...

____

Users you have created or tried to create using the above commands must have the password defined. Hence, one cannot log in to Linux OS with these users. Generate the password with the `passwd` command. Before you do, check the contents of the `/etc/shadow` file. Only the `student` user has the password defined, and only the student user account can log in interactively.

Create the new password for your user account (account with your name) using the `passwd` command.
NOTE! MAKE SURE TO CRETE A COMPLEX PASSWORD to prevent someone from breaking into the computer by guessing the password. Use this password: **Th1sIsComplex,Right?**
Check the contents of the shadow file again and answer these questions:
What type of hash is used to store a password? (Write down the part of the line where the hash type is defined).

____

Write down the salt with which the hash is additionally protected:

____

What is the role of salt-ing (salting) passwords when creating a hashing?

____

Change the password for your username again, USE THE SAME PASSWORD AS PREVIOUSLY!
Check that the salt value was changed (hash value too) – what is the hash value? (Check the slides to find which portion is the hash value)

____

If time permits:
This part of the exercise requires your own computer with Linux OS with root privileges (if completed @home)!
Using the presentation that came with the exercise (or your knowledge or googling, or AI-ing), set up the ssh server on a Linux computer as follows:

1. Set up public and private keys
2. Set up ssh service
3. transfer the private key to a Windows computer
4. download the putty client from the Internet
5. change the private key so it can be used with the putty client

6. set up the profile in the putty client that will connect to the ssh server using the private key you converted
7. set up the ssh server to accept connections only using a private key and allow the root user to connect only if they DO NOT use the password.