CYBERSECURITY

EXPLOITATION: SSH

We try to get access via ssh to a machine. The machine needs to be reachable/pingeable.

CREATE (WEAK) USER

On KALI create a user.
Give this user a (weak) password from the rockyou.txt wordlist.
Document how you did this.

On your KALI, make sure ssh is running: service ssh status, service ssh start, …

HYDRA

From another KALI machine, or from a hydra-installation on your windows machine we will try to crack the ssh.
Try to find the command yourself.
The following questions will help you.
What do these options do?
-l

-p

-t

-P

-L

-M

-s

-V

-e nsr

Document the result.

Extra: can hydra only crack ssh? Which other protocols can it try to break?
Document this.

TEST

Install a terminal tool that can connect over ssh to test the connection with the found user & password.
Document this.