**Experimenting with Password Cracking**

In this lab, you will be getting used to password cracking, basic fuzzing, and reverse engineering binaries/executables.

**Lab Set-up**

For password cracking (Part 1), you can work on your **Kali Linux**.

**Part 1: Password Cracking**

The objective of the first part of the lab is to try [John the Ripper](https://www.openwall.com/john/), a popular tool for cracking passwords. John the Ripper is already pre-installed in Kali.

**Tasks**

1. First, we will investigate how **passwords are stored** in Linux system.

Open your favourite terminal and print out the content of /etc/passwd and /etc/shadow files. Also check the access permissions of the two files and your own user privilege.

* 1. What can you see as root?
  2. What can be seen by non-privileged users?

1. You may find that some tools in Kali are unavailable if you log in as   
   a non-root user. Hence, if needed, use su command to switch to root   
   so that you can proceed with the subsequent steps below.

$ sudo su

1. Create a new user named test, and set the password for this user to testtest (i.e. double ‘test’). Then, check whether the password and password-shadow files contain a new line for the newly-added user.

# useradd -m test

1. You may want to **unshadow** your password and password-shadow files by running:

# unshadow /etc/passwd /etc/shadow > combined.txt

1. Run John, but limit the usernames to be cracked to test only:

# john --users=test combined.txt

Check how much time did John need to crack the password?

1. Change the password of user test to testtesttest (triple ‘test’)   
   and run John again with the same parameters. Can you see any difference?
2. Now, add a new user admin and set its password to a single English word. Run John with your selected wordlist shipped with Kali, which can be found in /usr/share/wordlists.

# john --users=admin --wordlist*=<path-to-wordlist>*  combined.txt

1. Share the results of your John within your group.
2. Print out all the passwords that have been cracked by John:

# john --show combined.txt

1. Once you finish the lab, delete the newly-added users with weak passwords:

# deluser test

# deluser admin

1. Lasly, don’t forget to remove John’s $JOHN/john.pot file:

# rm ~/.john/john.pot