Ecole Supérieure
d'Informatique et du Numérique
COLLEGE OF ENGINEERING & ARCHITECTURE

Lab 04: Fundamental Security
Instructor: Prof. Anass Sebbar
Level: Engineering - 3rd Year

Lab 04: Network Attacks and System Security

Objectives

The purpose of this lab is to illustrate various password security analysis techniques and penetration testing strategies. You will learn how to use John the Ripper to perform dictionary, hybrid, and brute-force attacks, analyze password strength and complexity, and evaluate the resilience of password systems against common cracking methods. In this lab, we will focus on:

- Performing password security analysis with John the Ripper**.**

Instructions

- The lab report must be submitted one week after the lab session on the Moodle platform, respecting the deadline mentioned there.
- The lab must be performed individually in class, but the report should be submitted in groups of up to 2 students.
- Lab groups must remain the same for all reports throughout the semester.

Legal and Ethical Precautions:

Brute-force attacks, as well as other penetration tests, are illegal if they are carried out without explicit permission. Please ensure that these tests are conducted in a controlled and ethical environment (e.g., on systems for which you have permission to test for security). This lab must be carried out in a laboratory setting or with dedicated testing machines.

In this lab, we will explore password cracking techniques using John the Ripper, a powerful open-source tool, and a dictionary attack on a Kali Linux virtual machine. The objective is to understand how attackers exploit weak passwords and how security professionals can test system vulnerabilities. We will demonstrate how dictionary attacks can efficiently crack password hashes. This hands-on exercise highlights the importance of strong password policies and defensive measures against brute-force attacks.

Password Analysis with John the Ripper:
Test password strength by using *John the Ripper* to try to crack weak passwords.
1-Create a folder John and download John the Ripper:

```
$ mkdir John
$ cd John
$ wget www.openwall.com/john/j/john-1.8.0.tar.xz
$ tar -xvf john-1.8.0.tar.xz
```

2- Download **crack-these-please** from
https://www.dropbox.com/s/3or7x52xb35kvau/crack-these-please?dl=0
(use a web browser to download). Place the file **crack-these-please** into the directory **john-1.8.0/run**. This file **crack-these-please.txt** contains the passwords of 50 users, named crack01 to crack50. The passwords vary; some are chosen to be simple and easy, and others are complex and difficult.

3- Dictionary attack

A dictionary attack uses a database of words and repeatedly tests them. John the Ripper has this capability. Display the contents of **password.lst** on the screen by executing the following command:

```
$ more password.lst
```

Then, change to the John the Ripper directory and run:

```
$ cd john-1.8.0/run

$ john --wordlist=password.lst crack-these-please
```

4- Combination attack

By default, John the Ripper performs dictionary, hybrid, and brute-force attacks in combination. Launch a combined attack by executing:

```
$ john crack-these-please
```

Let John run long enough to perform additional cracking. Note the time it took and how many additional passwords it was able to crack. Also, observe the nature of the passwords. What proportion of the cracked passwords can be found in the dictionary? And in a foreign language dictionary? How many of these passwords contain varied combinations of letters, symbols, numbers, and case? Do the cracked passwords tend to be long or short? Obtaining all the passwords might take an eternity, so if it takes too long, you can press **CTRL-C** to stop the execution.

5- Testing the attack on the UNIX system

As the root user, create a normal user (for example, **user1** and **user2**) using the `useradd` command:

```
$ useradd user2
$ useradd -c "User" -s /bin/bash -m -g users -k /etc/skel-comm -b
/home/ user1
```

Assign passwords to the users. Then, using the `su` command, log in as these users:

```
$ passwd user1
$ passwd -n 60 -x 90 -w 7 user2
$ su user1
```

On a terminal, display the contents of the files `/etc/shadow` and `/etc/passwords`.

Explain the role of these files:

```
$ more /etc/shadow
$ more /etc/passwords
```

We will use John the Ripper's **unshadow** utility to obtain the classic format of a Linux password file:

```
$ unshadow /etc/passwd /etc/shadow > mypasswd
Or
$ sudo unshadow /etc/passwd /etc/shadow | sudo tee /etc/mypasswd >
/dev/null
```

Launch John the Ripper to try to find the passwords of the targeted users by executing:

```
$ john --format=crypt mypasswd
```

You can also use a dictionary to crack the passwords from the `/etc/shadow` file:

```
$ john --wordlist=password.lst --format=crypt --rules mypasswd
```

Homework: Using DnsSpoof to Hijack DNS Traffic:

Create an IP redirection file to spoof DNS queries and hijack user connections.

```
$ dnsspoof -i eth0 -f hosts.txt
```

Example: `hosts.txt`

```
192.168.1.100   example.com

192.168.1.101   google.com
```