

## Lab 1 - Cracking Passwords

# 1 Preparation

## 1.1 Your PC

Before beginning the exercises in this lab you will first need to ensure that your PC has virtualisation enabled. If you are not sure how to do this please consult the video tutorial provided. This is "How to enable Virtualisation" and it is available under week three on the wikipage: <https://secure.ecs.soton.ac.uk/noteswiki/w/COMP6224-2223>.

## 1.2 Software

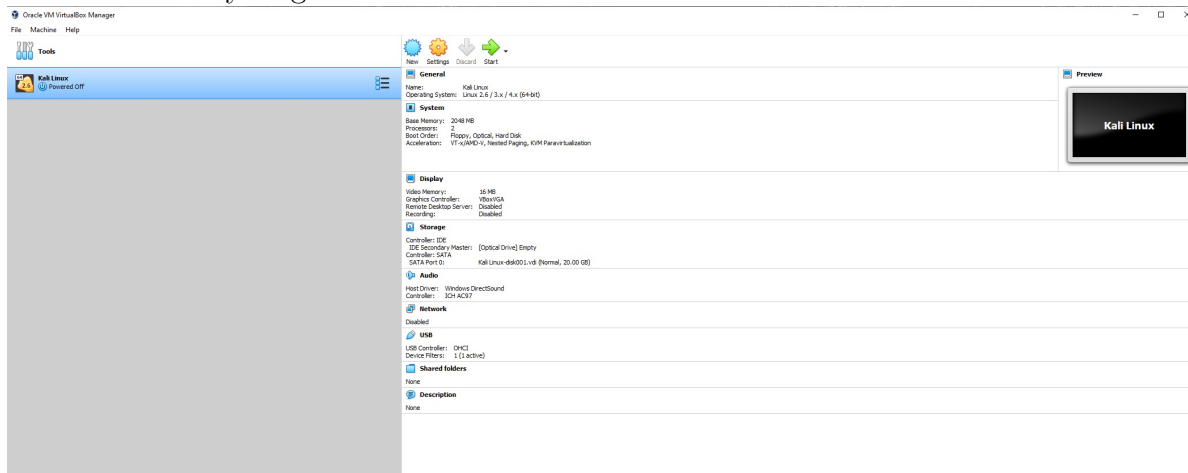
VirtualBox should be installed by default on university computers. If you are using your own system you can download the software here: [virtualbox.org](https://www.virtualbox.org). Please download the correct version for your operating system and install it.

## 1.3 Setting up the Environment

For the following series of exercises we will use a Kali Linux Virtual Machine (VM) which you can find under C:\Apps\CyberLabFiles\COMP6224 or download here: <https://software.soton.ac.uk/software/128> Please use this VM only, but **do not update it** even if prompted to do so! Make a note of where you saved the OVA file on your machine.

## 1.4 Import the VM in VirtualBox

Open VirtualBox, click on "file" and then on "import appliance". The virtual machine should now be ready to go as shown below:



## 1.5 Run the VM and Login

To run the VM just double click on its name, then wait a second or two and log in when prompted. *The username is root, while the password is foundations.*

As you progress through the exercise, please take regular screenshots to record your work. You should practice this habit as you will need it for the coursework to follow.

### Tips:

1. If your mouse appears stuck inside the screen containing the virtual machine, simply hit the right Ctrl button to undo this.
2. If you have the window containing the VM as the active window on your system and you hit the PRTSC button then the screenshot will be saved to the Pictures folder on the VM. If not, then the screenshot will be on your host system (Windows or Mac) and treated accordingly.
3. Do not update the VM.
4. If you copy and paste a command into the command line and it does not work, try typing it out by hand.
5. Exercise 1 below contains a detailed breakdown of the syntax for each command. You can always refer back to it later.
6. If you are unsure about a command, you can always use the "help" and "man" commands to find out more. Please refer to Tutorial 4 for more on this.

## 2 Exercise 1

In this exercise you are presented with a file called sensitive.txt. It was exfiltrated from a target system and it is your task to crack the passwords contained in the file. You will crack the passwords using John the Ripper's dictionary attack mode.

John the Ripper 1.0 was released in 1996 as a drop-in replacement for Cracker Jack under DOS. Initially, it was called Cracker John, but someone suggested the name John the Ripper. This also explains the john.pot filename - obviously, it was jack.pot in Cracker Jack.

The OVA file format stands for Open Virtual Applications. An OVA file is a virtual appliance used by virtualisation applications such as VMware and Virtualbox.

### 2.1 Cracking passwords using password.lst

We will now run John The Ripper in dictionary attack mode. This functionality uses a list of words in a dictionary (wordlist) and tries each as a password. It does this by hashing each word in the dictionary and then comparing the result to the hash of the password you are trying to crack. John The Ripper comes with a pre-installed small dictionary password.lst located in /usr/share/john/password.lst.

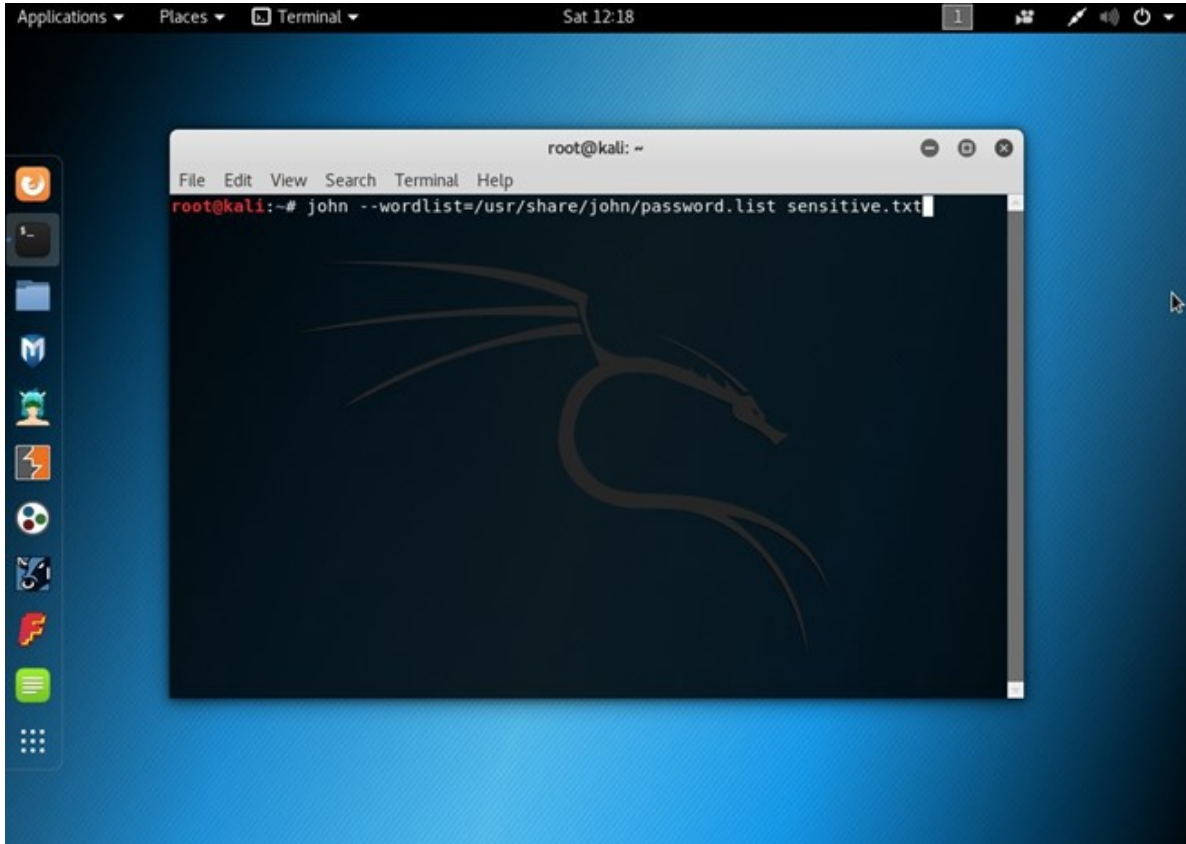
Please click on the terminal from the dock to the right:



Run John The Ripper in dictionary attack mode to try to crack the passwords in sensitive.txt. Type the following command:

```
john --wordlist=/usr/share/john/password.lst sensitive.txt
```

john	--wordlist=	/usr/share/john/	password.lst	sensitive.txt
Command	Parameter	Directory	Dictionary file	Target file



To see what the hashed passwords look like in their raw form, run the Bash command "cat" as follows:

*cat sensitive.txt*

cat	sensitive	.txt
Command	Filename	Extension

To see which hashes contained which passwords, run the following command:

*cat .john/john.pot*

cat	.john/	john	.pot
Command	Directory	Filename	Extension

**TASK 1 : WHICH PASSWORDS WERE YOU ABLE TO CRACK AND WHY IS THIS THE CASE?**

Now please remove ("rm" bash command) the john.pot file before you continue.

*rm .john/john.pot*

rm	.john/	john	.pot
Command	Directory	Filename	Extension

## 2.2 Cracking passwords using a downloaded dictionary

Run John The Ripper in dictionary attack mode against sensitive.txt. This time you will use a dictionary downloaded online e.g <https://wiki.skullsecurity.org/Passwords>. Here you will find a list of dictionaries which you will have to download and extract to use. It could be good practice for you to try out a couple of these, but to move things along we have already downloaded and extracted the Cain and Abel list for you. Run the following command:

```
john --wordlist=Downloads/cain.txt sensitive.txt
```

john	--wordlist=	Downloads/	cain	.txt	sensitive	.txt
Command	Paramater	Directory	Filename	Extension	Filename	Extension

Task2: Which passwords were you able to crack? Why do they differ from task 1?

As before, you need to remove john.pot before continuing. Next we will use the rockyou dictionary, which you will have to move to the correct dictionary and unzip. It is currently saved as: /usr/share/wordlists/rockyou.txt.gz. To use rockyou.txt you have to copy ("cp" bash command) the file rockyou.txt.gz to your curent directory and unzip ("gunzip" bash command) it:

```
cp /usr/share/wordlists/rockyou.txt.gz .
```

cp	/usr/share/wordlists/	rockyou	txt.gz	.
Command	Directory	Filename	Extension	Current directory

```
gunzip rockyou.txt.gz
```

gunzip	rockyou	.txt.gz
Command	Filename	Extension

Then run John The Ripper:

```
john --wordlist=rockyou.txt sensitive.txt
```

john	--wordlist=	rockyou	.txt	sensitive	.txt
Command	Paramater	Filename	Extension	Filename	Extension

Task3: Did you crack all the password hashes using rockyou and why?

Task 4: Can you think of a way to improve your results?

If so, please present your findings. Hint: you can use the "cat" command to see what the other wordlists look like. You can use the Leafpad utility or any other text editor to create your own wordlist and you might look online for popular passwords to include in your own wordlist.

*Remove the john.pot file before you move to the Exercise 2*

### 3 Exercise 2: Cracking account passwords

In this exercise you will have to grab password hashes from the Kali Linux system and crack them using John the Ripper. We have created six users accounts on Kali Linux.ova: user1, user2, user3, user4, users, and user6.

*You will crack the passwords of all six accounts*

#### 3.1 Copy the password files to your current directory

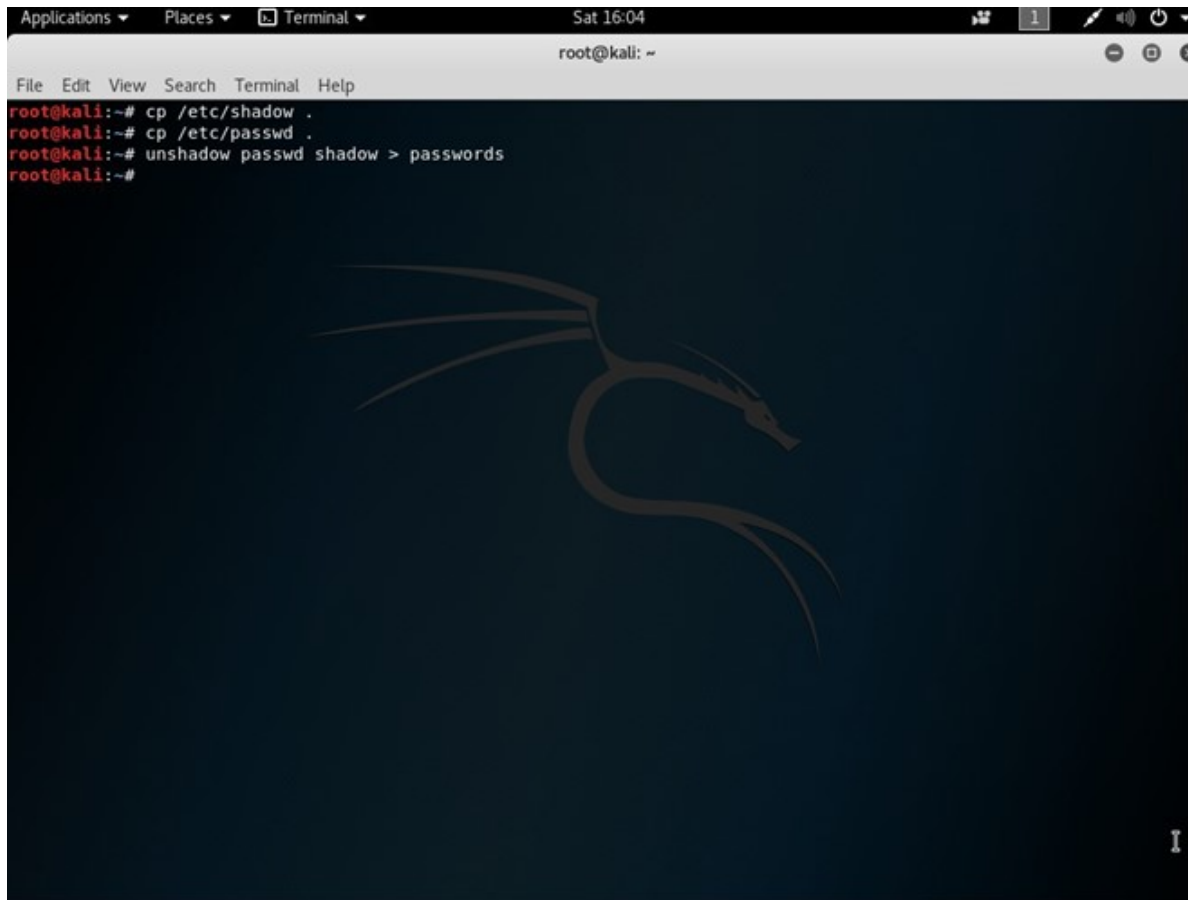
Linux stores its passwords in `/etc/shadow`, so what we want to do is copy this file to the home directory along with the `/etc/passwd` file, then "unshadow" them and store them in a file we'll call `passwords`. The `passwd` file contains user data but not the actual hashed passwords which are stored separately in the shadow file for added security. In the terminal, type the following commands:

1. `cp /etc/shadow .`
2. `cp /etc/passwd .`

#### 3.2 Unshadow the files

Next we need to combine the information in the `/etc/shadow` and the `/etc/passwd` files, so that John can do its magic. To do this we use the "unshadow" command along with ">". The ">" operator writes to a file while ">>" appends to a file. Please run:

*`unshadow passwd shadow >passwords`*

A terminal window titled 'Terminal' with a menu bar (File, Edit, View, Search, Terminal, Help) and a status bar (Sat 16:04, root@kali: ~). The terminal shows the following commands and output:

```
root@kali:~# cp /etc/shadow .
root@kali:~# cp /etc/passwd .
root@kali:~# unshadow passwd shadow > passwords
root@kali:~#
```

The background of the terminal is dark blue with a faint, stylized dragon logo.

We are now ready to crack the Kali Linux user accounts' passwords. John the Ripper supports different attack modes and in this exercise we will use the incremental brute force attack in addition to the dictionary attack mode already used in exercise 1.

### 3.3 Cracking the password using brute force

We will first run John the Ripper in brute force attack mode. This functionality tries different passwords and computes their hashes till it finds a hash that matches the hash of the password that you are trying to crack. To run John The Ripper in brute force attack mode, type the following command:

*john --incremental passwords*

Give this about 5 minutes to run and then stop the process by hitting "CTRL + C". The breached passwords are in the john.pot file again but this time we can use the "show" parameter to view them:

*john --show passwords*

This command displays the broken password in the john.pot file.

Task 5: Which passwords were you able to crack?

### 3.4 Cracking user passwords using a dictionary

To run John The Ripper in dictionary attack mode against user passwords, type the following command:

```
john --wordlist=/usr/share/john/password.lst passwords
```

Task 6: Which users' passwords were you able to crack? Please also elaborate on the differing results from questions 1 and 2.

Now you should have cracked all the passwords for all the Kali Linux user accounts. Try to login in the user accounts.

## 4 Final thoughts

If you were able to complete all 6 tasks, 4 for exercise 1 and 2 for exercise 2, then you should be prepared for the coursework to come. For the coursework though, taking screenshots will be an important factor, so please practice doing that. Please also remember that you can use a text editor to create your own dictionary. The more adventurous amongst you might want to look at tools such CeWL which is included in Kali, but this is not necessary to complete the coursework. One online resource that everybody should have a look at though is the list of top 20 most common passwords year by year. It is at: [https://en.wikipedia.org/wiki/List\\_of\\_the\\_most\\_common\\_passwords](https://en.wikipedia.org/wiki/List_of_the_most_common_passwords)