Unit 3: Password Cracking and Brute-Force Tools

3

Unit Structure

3.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Crack the password using tools and penetration into the system.
- Usage of brute-force tools

3.2 INTRODUCTION

This block is focus to discuss password and user account exploitation is one of largest issues in network security. In this section we will look at password cracking: the how and why of it. We will look at just how easy it is to penetrate a network, how attackers get in, the tools they use, and ways to combat it.

3.3PASSWORD CRACKING AND BRUTE-FORCE TOOLS

In general an attacker has two choices when trying to ascertain a password:

- Obtain a copy of the plaintext password or its encrypted hash and then use brute-force tools to guess what password produced the hash.
- Target a login prompt and try to guess a password.

Password cracking is an old technique that is successful mostly because humans arenot very good random-sequence generators.

A Brute-force technique is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through exhaustive effort (using brute-force) rather than employing intellectual strategies.

3.3.1 JOHN THE RIPPER

John the Ripper is one of the speedy password cracker, presently for many known operating systems like Windows, Unix, Mac, etc. Basically its main objective is to discover weak password in operating system.

John the Ripper autodetects the encryption on the hashed data and compares it against a large plain-text file that contains popular passwords, hashing each password, and then stopping it when it finds a match.

It also includes its own wordlists of common passwords for 20+ languages. These wordlists provide John the Ripper with thousands of possible passwords from which it can generate the corresponding hash values to make a high value guess of the target password. Since most people choose easy-to-remember passwords, It is often very effective even with its out-of-the-box wordlists of passwords.

What is John the Ripper Used for?

It is primarily a password cracker used during pentesting exercises that can help IT staff spot weak passwords and poor password policies.

Here is the list of encryption technologies found in John the Ripper:

- UNIX crypt(3)
- Traditional DES-based
- “bigcrypt”
- BSDI extended DES-based
- FreeBSD MD5-based (linux and Cisco IOS)
- OpenBSD Blowfish-based
- Kerberos/AFS
- Windows LM (DES-based)
- DES-based tripcodes
- SHA-crypt hashes (newer versions of Fedora and Ubuntu)
- SHA-crypt and SUNMD5 hashes (Solaris)

How to Download John the Ripper

It is an open-source project, so you can download and compile the source on your own, download the executable binaries, or find it as part of a penetration testing package.

The official website for John the Ripper is on https://www.openwall.com/john/. You can grab the source code and binaries there, and you can join the GitHub to contribute to the project.

John the Ripper is available on Kali Linux as part of their password cracking metapackages.

Cracking Password

John the Ripper's primary modes to crack passwords are single crack mode, wordlist mode, and incremental.

The *single crack mode* is the fastest and best mode if you have a full password file to crack.

The *wordlist mode* compares the hash to a known list of potential password matches.

The *incremental mode* is the most powerful and possibly won't complete. This is your classic brute force mode that tries every possible character combination until you have a possible result.

The easiest way to try cracking a password is to let John the Ripper go through a series of common cracking modes. This command below tells it to try "simple" mode, then the default wordlists containing likely passwords, and then "incremental" mode.

```
.\john.exe passwordfile
```

You can also download different wordlists from the Internet, and you can create your own new wordlists for John the Ripper to use with the –wordlist parameter.

```
.\john.exe passwordfile–wordlist=”wordlist.txt”
```

If you want to specify a cracking mode use the exact parameter for the mode.

```
.\john.exe --single passwordfile
.\john.exe --incremental passwordfile
```

When you want to see the list of passwords that you have cracked, use the –show parameter.

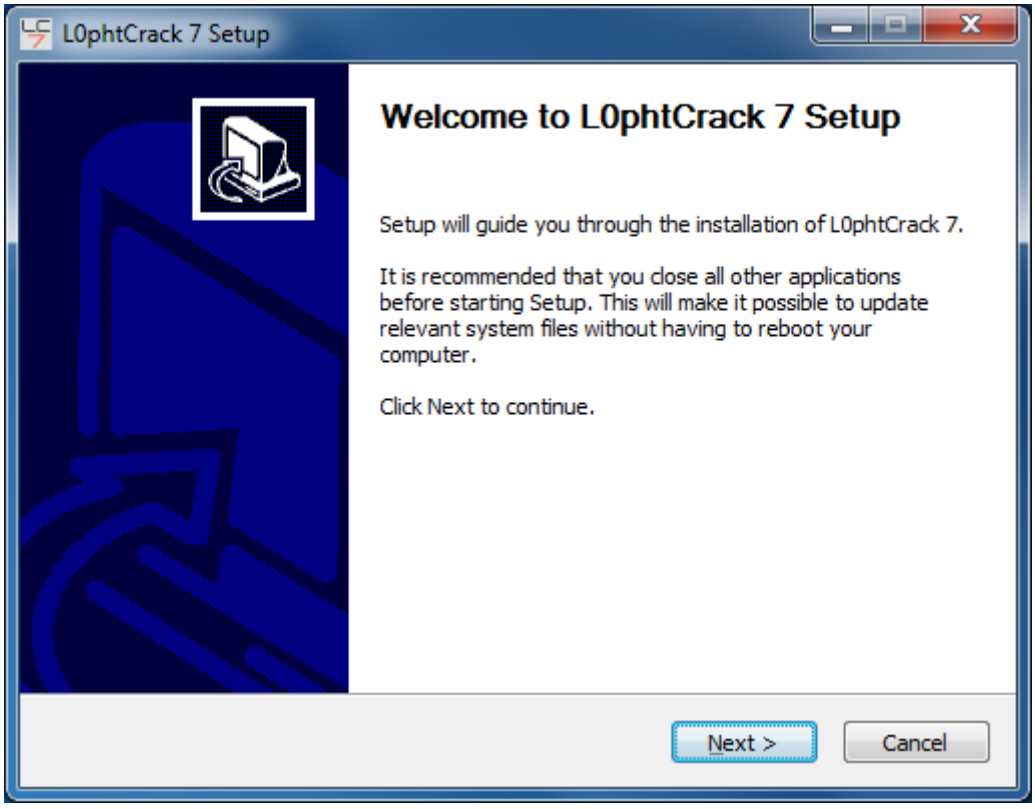
```
.\john.exe –show passwordfile
```

3.3.2 L0PHTCRACK

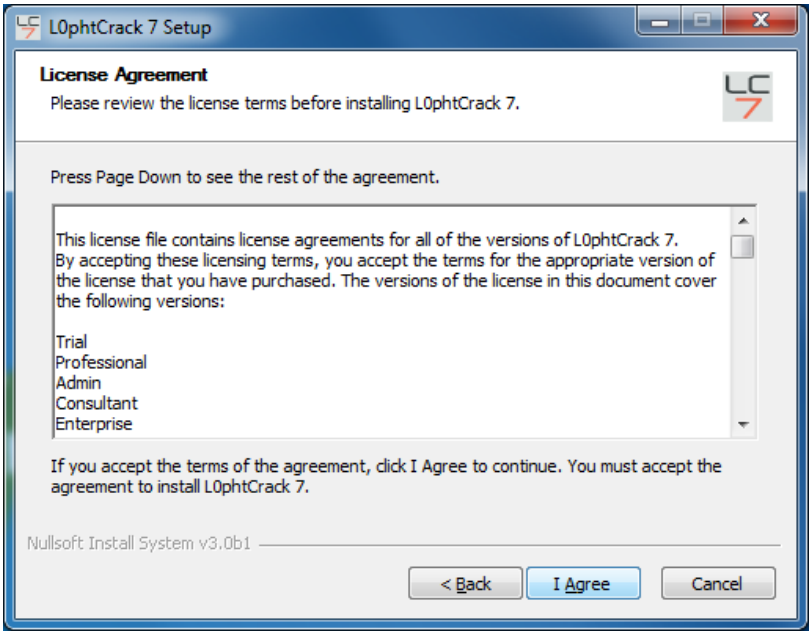
L0phtCrack is known as best windows password auditing tool. It can be used by network/system administrator for auditing weak passwords and can also help a hacker to recover password from password hashes.

To install L0phtCrack 7:

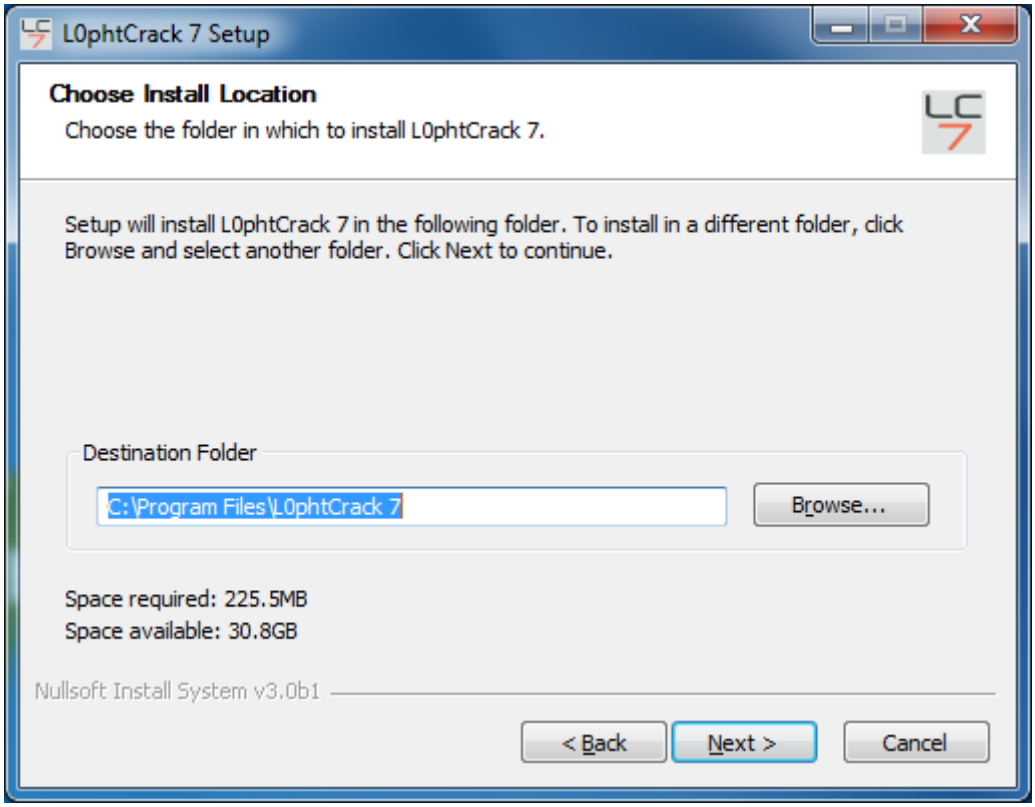
1. L0phtCrack 7 is distributed in a self-installing executable distribution file that can be downloaded for free at http://www.l0phtcrack.com/download.html.
2. Save the .exe file to your download directory.
3. In the download directory, double click the lc7setup.exe file. The installer starts a standard installation process. At the Welcome screen, click Next.



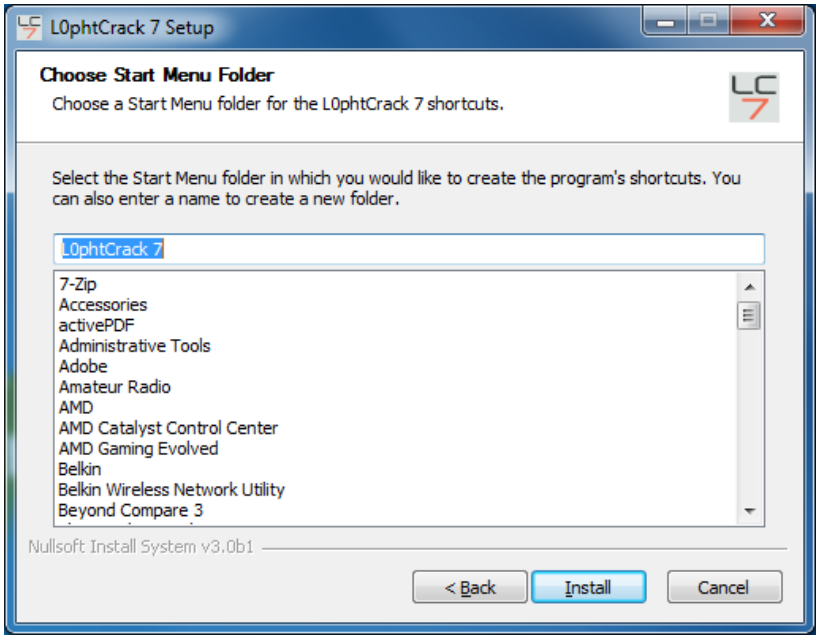
4. Read the License Agreement screen, then click I Agree to agree.



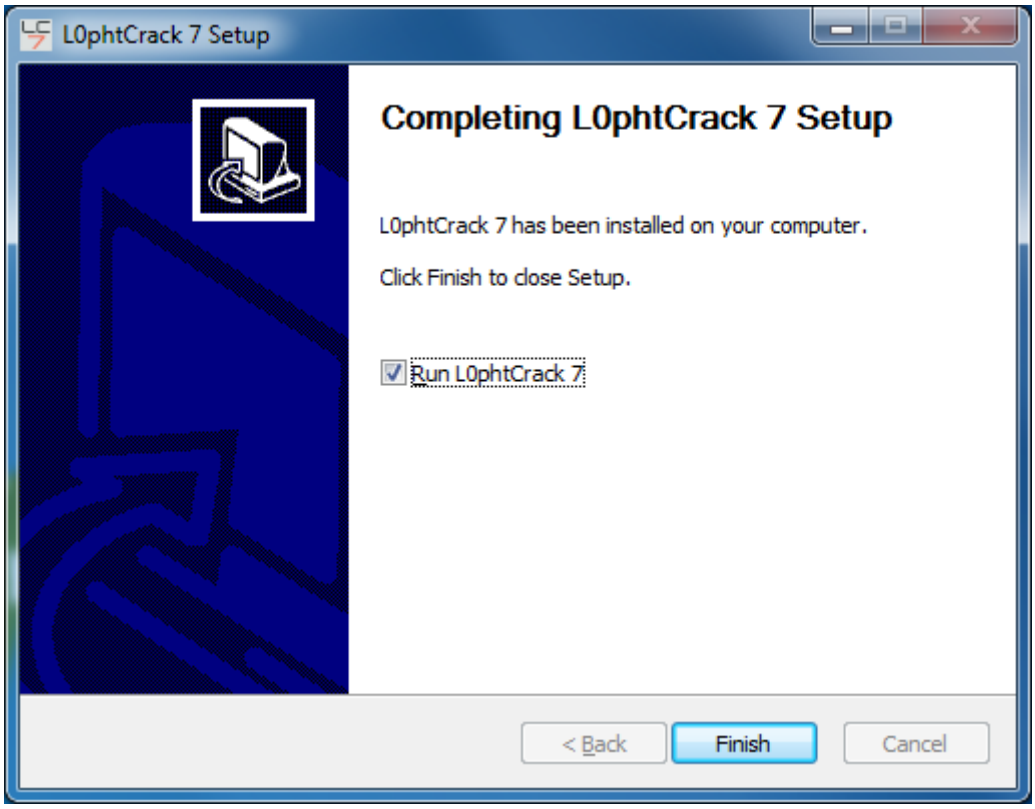
5. The installer installs L0phtCrack 7 in a default installation location: "C:\Program Files\L0phtCrack 7" or you may Browse to choose a different location. Click Next when ready.



6. A shortcut to the L0phtCrack 7 executable is installed in the Programs folder under the Start menu. The default folder name is L0phtCrack 7. You may choose a different name. Click Install when ready.



7. Click Finish when the L0phtCrack installer completes the installation. L0phtCrack will launch by default. If you don't want to run the program at this time, uncheck Run L0phtCrack 7.



8. L0phtCrack 7 is now installed on your system. You may now click the Start button, and go to the Programs folder to run L0phtCrack 7.

Importing Password Hashes

Approaches to importing password hashes differ depending on where the password resides on the computer and your ability to access them.

L0phtCrack 7 can import password hashes directly from remote machines, from the local file system, from SAM, pwdump, or shadow files, and from Active Directory. Obtaining passwords over the network requires network access and administrator privileges to the target machine.

To begin the import process select Import from the Passwords Menu Sidebar on the left hand side of the main screen. When Import is selected you will see the main window display the Import Mechanisms. When you select an Import Mechanism you will see the right side of the main window change to a dialog for the inputs required such as file and machine names.

After you input the required filenames, hostnames and options for an Import Mechanism you will see the action buttons Run Import Immediately and Add Import To Queue ungray and become active. At this point you will likely press Run Import Immediately to perform the import action. Optionally you can press Add Import to Queue to build a queue.

Import from Local Machine

To import password hashes from a local machine, you must be logged in with administrator rights or have an administrator/password pair. The local machine import works regardless of whether passwords are stored in a SAM file or in an Active Directory.

First, select Import from local Windows system. You can select to Keep Currently Imported Accounts if you are adding this import to accounts (hashes) you have already imported. If this option is not selected the import will overwrite any previously imported accounts. If you want to audit all system accounts, not just user accounts, you can select to Include Machine Accounts.

Next, specify the credentials that will be used to access the password hashes. You can choose Use Logged-In User Credentials. If you previously saved credentials for the local machine you can Use Saved Credentials. You can also select Use Specific

User Credentials. If specific user credentials is selected you need to specify Username, Password, and optionally a Domain. You can select Save These Credentials to save the username, password, and domain to the Windows protected store for use in future audits.

Import from Remote Machine

L0phtCrack 7 incorporates remote password hash retrieval, simplifying the process of obtaining password hashes, and reducing the need to use a third-party retrieval/dumping tool.

To import from remote machines select either Import from Linux/BSD/Solaris/AIX system over SSH if your target system is Unix-like or select Import from remote Windows system if your target system is Windows. Credentials with Root or Administrator privileges are required. If a security tool or some other element in the network environment is preventing remote hash retrieval, then you may have to use a third party tool to obtain the hashes and then follow the instructions for importing hashes from a pwdump file, SAM/System file (Windows), or shadow file (Unix).

3.3.3 PWDUMP

The original pwdump program was written by Jeremy Allison in 1997 to demonstratehow to extract password hashes from the Windows Registry. Since then,other developers have created many versions of pwdump to keep up with variousupdates to Windows. But they all rely on extracting hashes from the Registry, SAMfile, or the lsass.exe process's memory space. The lsass.exe process handles the LocalSecurity Subsystem Service; it's essentially responsible for authentication, which iswhy its memory contains the system's password hashes.

All the pwdump variants may be found at www.openwall.com/passwords/microsoft-windows-nt-2000-xp-2003-vista-7. The Openwall site is also the home ofJohn the Ripper, covered previously.

How to use pwdump

The pwdump tools are simple to use. They require Administrator privileges, so you'llneed to start the cmd.exe shell with Run As Administrator. The following

exampledemonstrates pwdump6 on a 64-bit Windows system. The -x option is necessary to letpwdump6 know the target system is 64-bit. Otherwise, the process will hang withoutreturning results. The -n option instructs pwdump6 to forego the search for passwordhistories. The output may be passed to John the Ripper in order to start cracking hashes.

```
C:\pwdump6\PwDumpRelease>          PwDump.exe          -n          -x
localhostAdministrator:500:NO                PASSWORD*************:NO
PASSWORD***********:::
Abs:1007:NO PASSWORD**************:2CxxxxxxxxxxxxxxxxxC01C591BC9:::
Guest:501:NO PASSWORD***********:NO PASSWORD*********************:::
Completed.
```

Note that neither the Administrator account nor the Guest account has a passwordset. This will be more common on home desktop systems because modern Windowssystems encourage users to conduct their activities under their own account privilegesand use the runas.exe or Run As Administrator commands to execute programs thatrequire privileged access.

3.3.4 THC-HYDRA

THC-Hydra (aka simply Hydra) easily surpasses the majority of brute-force toolsavailable on the Internet for two reasons: it is fast, and it targets authenticationmechanisms for several dozen protocols. Its source code and documentation are availablefrom https://www.thc.org/thc-hydra/. The Hacker's Choice web site (https://www.thc.org) contains many security tools, although some of them have not been maintainedfor several years.

THC (The Hackers Choice) created Hydra for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely.

Installing THC-Hydra

If you are running Kali Linux you will already have a version of Hydra installed, for all other Debian based Linux operating systems download from the repository by using.

```
sudo apt-get install hydra
```

or you can download the latest version from THC’s public GitHub development repository https://github.com/vanhauser-thc/thc-hydra

Start by using git to clone the GitHub repository.

```
git clone https://github.com/vanhauser-thc/thc-hydra
```

next change into the thc-hydra directory.

```
cd thc-hydra
```

now just type.

```
./configure
```

then…

```
make
```

and then.

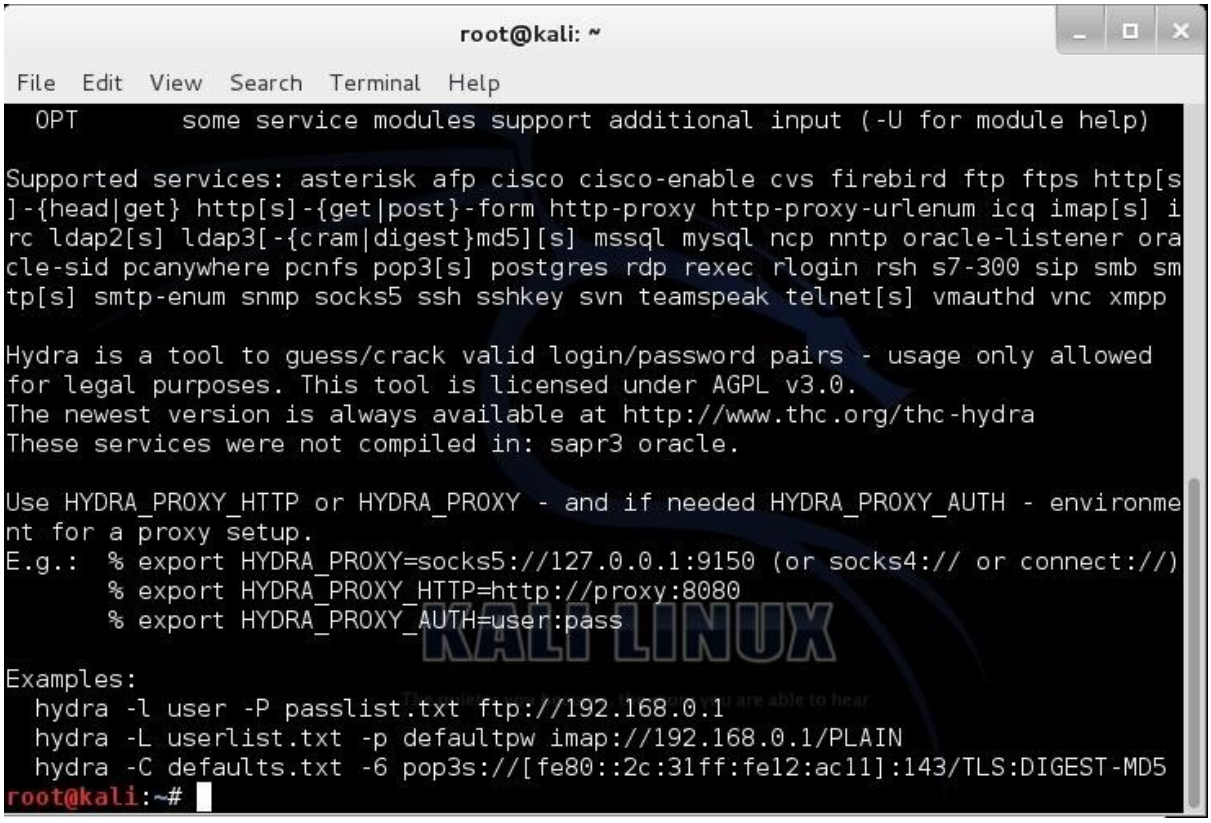
```
sudo make install
```

Hydra-GTK

Hydra GTK is a GUI front end for hydra, as this is a GUI for hydra you do have to have THC-hydra already installed. If you are running Kali Linux this will already be pre-installed for everyone.

Understand the Hydra Basics

When we open Hydra, we are greeted with this help screen. Note the sample syntax at the bottom of the screen. Hydra's syntax is relatively simple and similar to other password cracking tools.



Let's take a look at it further.

```
hydra -l username -p passwordlist.txt target
```

The username can be a single user name, such as "admin" or username list, passwordlist is usually any text file that contains potential passwords, and target can be an IP address and port, or it can be a specific web form field.

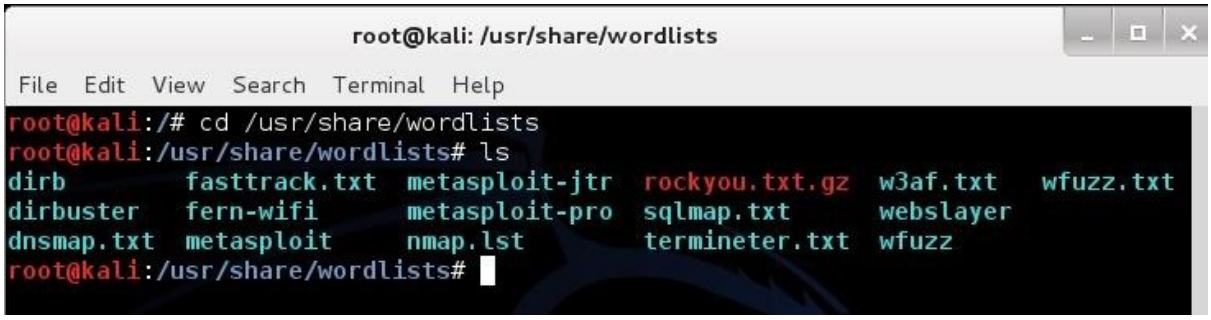
Although you can use ANY password text file in Hydra, Kali has several built in. Let's change directories to /usr/share/wordlists:

```
kali > cd /usr/share/wordlists
```

Then list the contents of that directory:

```
kali >ls
```

You can see below, Kali has many word lists built in. You can use any of these or any word list you download from the web as long as it was created in Linux and is in the .txt format.



Use Hydra to Crack Passwords

In the example below, I am using Hydra to try to crack the "admin" password using the "rockyou.txt" wordlist at 192.168.89.190 on port 80.

Check Your Progress 1:

1. Define Brute-Force attack
2. What is JtR?
3. What is the use L0PhtCrack?

3.4LET US SUM UP

This block covers the password cracking and brute-force tools like John the Ripper, L0PhtCrack, Pwdump and THC-Hydra.

3.5CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Check Your Progress 1:

1. A brute force attack is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through exhaustive effort (using brute force) rather than employing intellectual strategies.

2. John the Ripper (JtR) is a free password cracking software tool. Initially developed for the Unix operating system, it now runs on fifteen different platforms.
3. It is used to test password strength and sometimes to recover lost Microsoft Windows passwords, by using dictionary, brute-force, hybrid attacks.

3.6 FURTHER READING

For more focus on cyber security domain use CEH (Certified Ethical Hacking) books. Also you can refer “Anti-Hacker Toolkit By Mike Shema”.
For THC Hydra: https://github.com/vanhauser-thc/thc-hydra

3.7ASSIGNMENTS

- How to use John the Ripper tool?

3.8ACTIVITIES

- Perform password recovery using brute-force tools.