**WHAT İS HYDRA?**

Weak passwords are still big problem in security. it is becoming easier to cracking algorithms with brute-forcing which is a major kind of attack. Hydra is a parallelized login cracker which supports many of protocols to attack remotely. With Hydra, it is getting faster and flexible and there is a chance to add new modules easily. Hydra uses wordlists to attack systems. Wordlists, contains most used passwords and we can customize our own wordlists to attack specific persons. In this case, this situation shows the importance of using a strong password.

**tablo içeren bir resim

Açıklama otomatik olarak oluşturuldu**

**the list of all protocols supported by hydra.**

Hydra is a pre-installed tool in Kali Linux. You can check the usage of Hydra with using this command. This page gives us the knowledge about parameters which we can use with Hydra tool:

#hydra -h

metin içeren bir resim

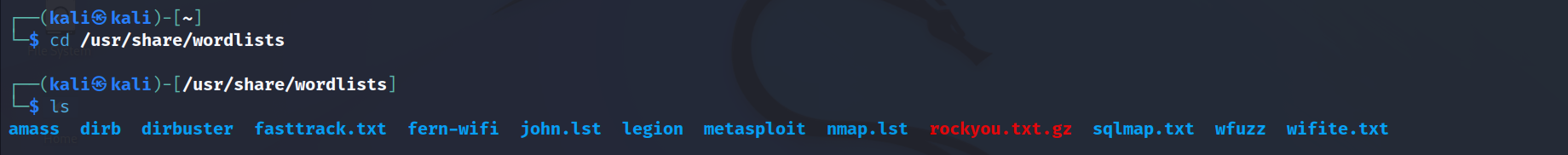
Açıklama otomatik olarak oluşturuldu

**To brute-force ssh username and password**

**#hydra <Target\_IP> ssh -l <username> -P <password\_file> -s 22 -vV**

We have username and password list to attack the target by using Hydra. You can access the wordlist files with this directory (for instance rockyou.txt file iz zipped. You have to unzip to use.)

**cd /usr/share/wordlists**

****

**To brute-force FTP username and password:**

**#hydra -L <username\_file> -P <password\_file> ftp://<Target\_IP>**

**-l : input login(not the list of usernames)**

**-L: username list**

**-p: if you will try single password**

**-P: list of passwords to do brute-forcing**

**-v : gives us details**

**-s : we can add the spesific ports that we want to attack with that parameter**

**-S: If it is possible, Hydra will try to connect with SSL with that parameter**

**-M: We will specified the location of the list of ports of the servers with this parameter**

There is no difference between ssh and ftp connections usage . Parameters are same.

**To brute-force telnet username and password:**

**#hydra -l <username> -p <password>** [**telnet://<Target\_IP**](telnet://%3cTarget_IP)**>**

**xHydra**

Hydra also has interface page name that xHydra. You can open the xHydra page in terminal with “xhydra” command. In this interface you can pick the protocols and ports and other options from there. All the options are same with Hydra.

**WORDLISTER TOOL**

Firstly, we should install the Wordlister.

git clone <https://github.com/4n4nk3/Wordlister.git> command will help us.

metin içeren bir resim

Açıklama otomatik olarak oluşturuldu

**python3 wordlister.py –help**

This command will give us options about how we can use the tool.

metin içeren bir resim

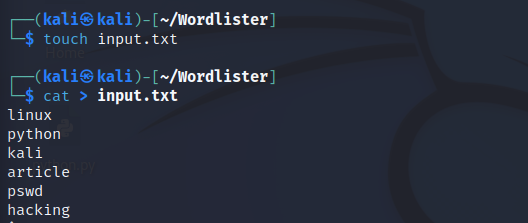
Açıklama otomatik olarak oluşturuldu

We must have input word list to give Python to make wordlister with all combinations.

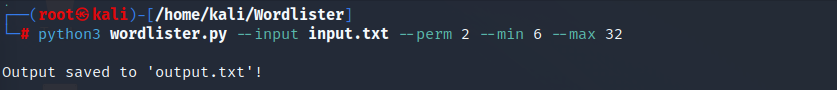
Then, we will give the details. For instance, we can choose the character size. Like you have to choose minimum 6 character for passwords.

**python3 wordlister.py –input list.txt –perm 2 –min 6 –max 32**

this command perm command tells us max 2 words can be conbined on the same possible password.



We put the words in a txt file. Then run the command.



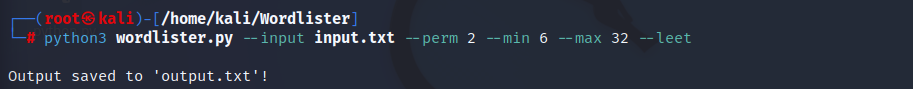
We have the txt file that contains combinations.

metin içeren bir resim

Açıklama otomatik olarak oluşturuldu

**Using Leet mod**

**python3 wordlister.py --input input.txt --perm 2 --min 6 --max 32 --leet**

****

****

**Using cap option to capitalize the first letter:**

**python3 wordlister.py –input list.txt –perm 2 –min 6 –max 32 –cap**

**metin içeren bir resim

Açıklama otomatik olarak oluşturuldu**

**Transform every letter in a word into uppercase:**

**python3 wordlister.py –input list.txt –perm 2 –min 6 –max 32 –up**

**metin içeren bir resim

Açıklama otomatik olarak oluşturuldu**

[**https://www.geeksforgeeks.org/**](https://www.geeksforgeeks.org/how-to-install-and-use-hydra-in-linux/)

[**https://allabouttesting.org/**](https://allabouttesting.org/examples-of-kali-linux-hydra-tool/)

[**https://www.kali.org/tools/hydra/**](https://www.kali.org/tools/hydra/)

[**https://anilcelik.medium.com/**](https://anilcelik.medium.com/)