Dictionary Attack:

An attacker tries each of the words in a dictionary as passwords to gain access to the system via some user's account. If the password chosen by the user was a word within the dictionary, this attack will be successful (in the absence of other mitigations). This is a specific instance of the password brute forcing attack pattern.

Source: https://capec.mitre.org/data/definitions/16.html

Detecting Dictionary Attack:

1. Cracking Wi-Fi Passwords via Aircrack-ng

Aircrack-ng is used to attack WPA/WAP2 wireless protocols.
Once you have the captured packet, you can use the "-w" parameter of the aircrack-ng tool to perform a dictionary attack

Eg:

```
sudo aircrack-ng -w rockyou.txt -b 84:D8:1B:06:EF:06 packet.cap
```

84:D8:1B:06:EF:06 is the MAC address of the access point used in the example

Hence, to detect pattern match on

```
aircrack-ng -w
```

https://miloserdov.org/?p=2178

2. John the Ripper

We can use the "`–wordlist`" flag to perform a dictionary attack

Eg:

```
john --wordlist=/usr/share/wordlists/rockyou.txt crackmypasswordhash.txt
```

Hence, to detect pattern match on

john --wordlist

https://mcsi-library.readthedocs.io/articles/2022/07/hands-on-with-john-the-ripper-performing-a-basic-dictionary-attack/hands-on-with-john-the-ripper-performing-a-basic-dictionary-attack.html

3. Hashcat

We can use the parameter "-a 0" for a dictionary attack.

Eg:

```
hashcat -m 100 -a 0 sha1.txt rockyou.txt
```

NOTE: The m value is not always 100, there are many hash types which can be defined here.

The -m flag is used to specify the hash type and the -a flag is to specify the attack mode.

Dictionary attack (-a 0)

https://www.freecodecamp.org/news/hacking-with-hashcat-a-practical-guide/

4. Ncrack

In ncrack, we use “-U” to define a wordlist for username, and “-P” to define a wordlist for passwords.

Note: “-user”, “-pass” parameter are used, if the actual username/password is known

Eg:

```
ncrack -user msfadmin -P pass.txt 192.168.0.105:21
ncrack -U user.txt -pass msfadmin 192.168.0.105:21
ncrack -U user.txt -P pass.txt 192.168.0.105:21
```

https://www.hackingarticles.in/comprehensive-guide-on-ncrack-a-brute-forcing-tool/

5. Hydra

In Hydra, we use “-L” to define a wordlist for username and “-P” to define a wordlist for passwords.

Eg:

```
hydra -l user -P passlist.txt ftp://192.168.0.1

hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN

hydra -C defaults.txt -6 pop3s://[2001:db8::1]:143/TLS:DIGEST-MD5

hydra -l admin -p password ftp://[192.168.0.0/24]/

hydra -L logins.txt -P pws.txt -M targets.txt ssh
```

https://resources.infosecinstitute.com/topic/online-dictionary-attack-with-hydra/

6. Detection by wordlists

We can also detect this attack by looking for the common wordlists being used:

Most common wordlist being: rockyou.txt in the path: /usr/share/wordlists/

This path has the default wordlists on kali: /usr/share/wordlists/

Some of the other famous wordlist paths being:

/etc/theHarvester/wordlists

/usr/share/amass/wordlists

/usr/share/dirb/wordlists

/usr/share/dirbuster/wordlists

/usr/share/fern-wifi-cracker/extras/wordlists

/usr/share/legion/wordlists

/usr/share/metasploit-framework/data/wordlists

*** These are a good place to start, as these are some of the most commonly used password cracking tools, but there can be many other tools out there.