Dictionary Attacks

Information Security Inc.

Contents

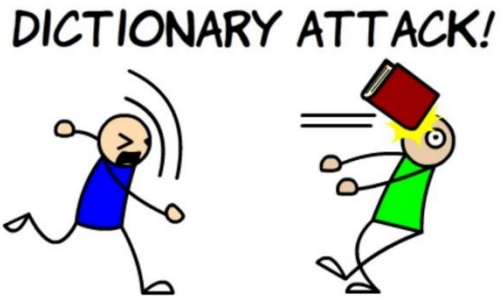
- About Dictionary attacks
- Programs that use dictionary attacks
- Building a wordlist for Dictionary Attacks
- Password lists
- References

Information Security Confidential - Partner Use Only

About Dictionary attacks

- Dictionary Attacks are a method of using a program to try a list of words on the interface or program that is protecting the area that you want to gain access to.

- It means saving all the possible passwords in a text file, then the password recovery program will look for the password from the text file (dictionary) one by one until it finds the password.



Information Security Confidential - Partner Use Only
iSEC information security inc.

Programs that use dictionary attacks

- John the Ripper
- L0phtCrack
- Cain And Abel
- Aircrack
- Hydra
- Medusa
- Brutus

Information Security Confidential - Partner Use Only
iSEC information security inc.

Building a wordlist for Dictionary Attacks

- Wordlist generators
  - ◎ Crunch

```
NAME
       crunch - generate wordlists from a character set

SYNOPSIS
       crunch <min-len> <max-len> [<charset string>] [options]

DESCRIPTION
       Crunch can create a wordlist based on criteria you specify.
```

▲ Example: create a dictionary with the possible combinations from the word password which will have a length between 3 and 9 characters

```
root@LUCKY64:/opt3# crunch 3 9 password -o Dictionary.txt
Crunch will now generate the following amount of data: 462945385 bytes
441 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 47079151

crunch:  96% completed generating output

crunch: 100% completed generating output
```

```
root@LUCKY64:/opt3# less Dictionary.txt
ppp
ppa
pps
ppw
ppo
ppr
ppd
pap
paa
pas
paw
pao
par
pad
psp
psa
pss
```


Information Security Confidential - Partner Use Only

iSEC information security inc.

Building a wordlist for Dictionary Attacks

- Wordlist generators
  - ◎ Cewl

```
NAME
       cewl - custom word list generator

SYNOPSIS
       cewl [OPTION] ... URL

DESCRIPTION
       CeWL (Custom Word List generator) is a ruby app which spiders a given URL, up to a specified depth,
```

▲ Example: create a dictionary using the words from a givenURL

```
root@LUCKY64:/opt3# cewl hackyourselffirst.troyhunt.com -d 2 -w Dictionary.txt
CeWL 5.3 (Heading Upwards) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
root@LUCKY64:/opt3#
root@LUCKY64:/opt3#
root@LUCKY64:/opt3# wc -l Dictionary.txt
318 Dictionary.txt
root@LUCKY64:/opt3# more Dictionary.txt
the
and
First
Hack
Yourself
troyhunt
com
course
risks
Supercar
```


Information Security Confidential - Partner Use Only

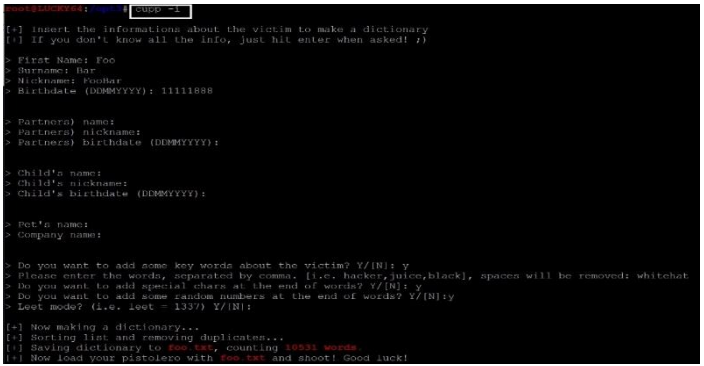
iSEC information security inc.

Building a wordlist for Dictionary Attacks

- Wordlist generators
  - ◎ Cupp (apt-get install cup)

```
NAME
       cupp - generate dictionaries for attacks from personal data

SYNOPSIS
       cupp [options]

DESCRIPTION
       CUPP(Common  User  Passwords Profiler) is tool to generate wordlist from common user profiler.
```

  - ▲ Example:

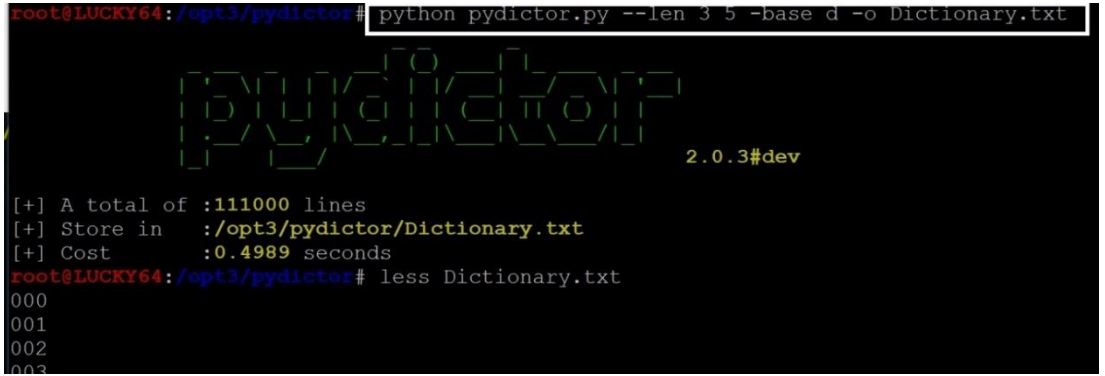


Information Security Confidential - Partner Use Only
iSEC information security inc.

Building a wordlist for Dictionary Attacks

- Wordlist generators
  - ◎ Pydictor (git clone https://github.com/LandGrey/pydictor.git)

▲ Example:



Information Security Confidential - Partner Use Only

iSEC information security inc.

Building a wordlist for Dictionary Attacks

- Wordlist generators
  - ◎ Pydictor (git clone https://github.com/LandGrey/pydictor.git)

▲ Example:

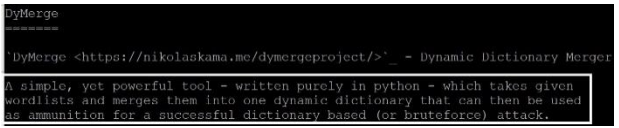
```
root@LUCKY64:/opt3/pydictor# python pydictor.py --len 5 5 -base d --encode b64 -o Dictionary.txt

                                                    2.0.3#dev

[+] A total of :100000 lines
[+] Store in   :/opt3/pydictor/Dictionary.txt
[+] Cost       :0.4817 seconds
root@LUCKY64:/opt3/pydictor# less Dictionary.txt
root@LUCKY64:/opt3/pydictor# less Dictionary.txt
MDAwMDA=
MDAwMDE=
MDAwMDI=
```


Information Security Confidential - Partner Use Only

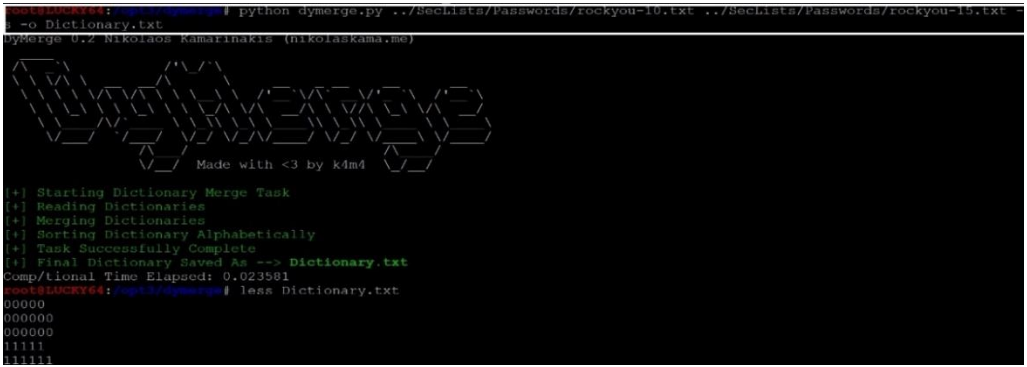
iSEC information security inc.

Building a wordlist for Dictionary Attacks

- Wordlist generators
  - ◎ Dymerge (git clone https://github.com/k4m4/dymerge.git)



▲ Example:



Information Security Confidential - Partner Use Only

iSEC information security inc.

Building a wordlist for Dictionary Attacks

- Wordlist generators
  - ◎ Munchkin (pip install munchkin)

▲ Example:

1) A user named Foo generates a card from passwordcard.org with an initial seed of f08aa69067c73300. He creates two passwords for his Instagram and Gmail accounts, "**rfUMK2V "** and *"***Ntdh6K6"**.

2) When Foo takes out his password card to log into Gmail, he gets sloppy and leaves it on his desk while he steps out

3) User Bar then downloads Munchkin. He uses it to generate a wordlist.

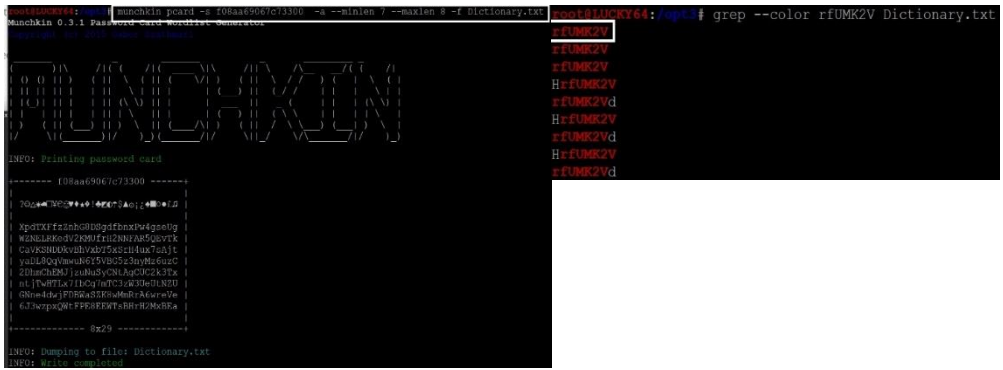
Information Security Confidential - Partner Use Only

iSEC information security inc.

Building a wordlist for Dictionary Attacks

- Wordlist generators
  - ◎ Munchkin (pip install munchkin)
  - ▲ Example:

1) A user named Foo generates a card from passwordcard.org with an initial seed of f08aa69067c73300. He creates two passwords for his Instagram and Gmail accounts, “**rfUMK2V "** and *“***xzkNVaw "**
2) When Foo takes out his password card to log into Gmail, he gets sloppy and leaves it on his desk while he steps out
3) User Bar then downloads Munchkin. Bar collects **3852** possible passwords into the Dictionary.txt file and brute-force Foo’s Gmail account with Hydra.



Information Security Confidential - Partner Use Only

References

• Wikipedia
https://en.wikipedia.org/wiki/Dictionary_attack

• SecTools
http://sectools.org/tag/pass-audit/

• PasswordCard
https://www.passwordcard.org/en

• Pwned Passwords
https://haveibeenpwned.com/Passwords