How to Tell if Your Meat Is Cooked (Without a Thermometer)

iPhone Security: Apple Refuses FBI's Demands to Create iOS Backdoor

Hack Like a Pro: How to Evade AV Software with Shellter

Crack Any Master Combination Lock in 8 Tries or Less Using This Calculator

Advice to Novice Hackers

Advanced Cryptography - Guide

Hack Like a Pro: How to Crack Passwords, Part 5 (Creating a Custom Wordlist with CeWL)

Posted By occupytheweb 16K 1 year ago Follow

36

KUDOS

Welcome back, my novice hackers!

In my series on cracking passwords, I began by showing off some basic password-cracking principles; developed an efficient password-cracking strategy; demonstrated how to use Hashcat, one of the most powerful password-cracking programs; and showed how to create a custom wordlist using Crunch. In this tutorial, I will show you how to create a custom wordlist based upon the industry or business of the targets using CeWL.

Most password-cracking programs are only as good as the wordlist that you provide them. Brute-force password cracking is very tedious and time consuming, but if you can find an appropriate and well-designed wordlist that is specific to the user whose password you are trying to crack, you can save yourself hours—maybe even days—of password cracking.

Crunch is great at creating wordlists based upon a set of rules such as the number of characters, the character set, etc., but doesn't enable us to choose a wordlist that is particular to a business or industry or interests. We humans are not always very creative and often fall victim to the familiar, especially when generating passwords. If we understand that, it can be helpful to finding potential passwords and generating a relevant password list.

For instance, employees at a construction company are more likely to use words for passwords that are used in their industry, such as lumber, girder, build, soffit, eave, etc. People in the drug industry are more likely have passwords such as prescription, drug, narcotic, barbiturate, etc. You get the idea.

It's simply human nature that words that we use in our everyday experience will first pop into our heads when we are considering passwords. That's why

Popular Now

Hack Like a Pro: How to Evade AV Software with Shellter

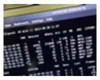
Crack Any Master Combination Lock in 8 Tries or Less Using This Calculator

Related

Hack Like a Pro: How to Crack Passwords, Part 4 (Creating a Custom Wordlist with Crunch)

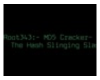
Creating Unique and Safe Passwords, Part 1 Using Wordlists

Hack Like a Pro: How to Crack Online Web Form Passwords with THC-Hydra & Burp Suite



How to Hack Wi-Fi: Cracking WPA2-PSK Passwords with Cowpatty

Hack Like a Pro: How to Crack Passwords, Part 3 (Using Hashcat)



How to Crack MD5 Hashes with All of Kali Linux's Default Wordlists

How to Hack WPA/WPA2-Enterprise Part 2

use words and numbers that first come to mind.

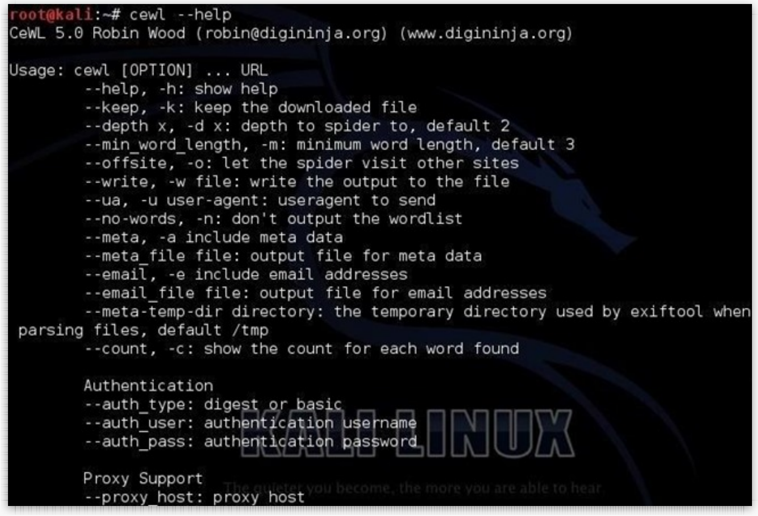
We can use this lack of creativity to develop a specific wordlist for a specific company or industry. That's what CeWL can do for us. It's designed to grab words from the company's website to create a wordlist specific to the company in order to crack passwords of the users at that business.

Let's get started.

Step 1: Fire Up Kali & CeWL Help

First, fire up Kali and open a terminal. Next, let's type the "cewl" command and get its help screen.

- **kali > cewl --help**



```
root@kali:~# cewl --help
CeWL 5.0 Robin Wood (robin@digininja.org) (www.digininja.org)

Usage: cewl [OPTION] ... URL
        --help, -h: show help
        --keep, -k: keep the downloaded file
        --depth x, -d x: depth to spider to, default 2
        --min_word_length, -m: minimum word length, default 3
        --offsite, -o: let the spider visit other sites
        --write, -w file: write the output to the file
        --ua, -u user-agent: useragent to send
        --no-words, -n: don't output the wordlist
        --meta, -a include meta data
        --meta_file file: output file for meta data
        --email, -e include email addresses
        --email_file file: output file for email addresses
        --meta-temp-dir directory: the temporary directory used by exiftool when
 parsing files, default /tmp
        --count, -c: show the count for each word found

        Authentication
        --auth_type: digest or basic
        --auth_user: authentication username
        --auth_pass: authentication password

        Proxy Support
        --proxy_host: proxy host
```

Note the depth (-d) and the min_word_length (-m) switches. The -d switch determines how deep (the default is 2) into the website CeWL will crawl grabbing words, and the -m switch determines the minimum length of words it will grab. Since most firms have a minimum password length, there's no need to grab short words. In this case, I will be setting the minimum to 7 letters.

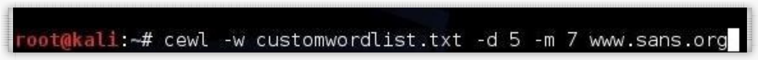
Step 2: Build a Custom List with CeWL

Now, to build a custom wordlist, we set CeWL to scraping words from the website of our friends at SANS Institute. We can do this by typing:

- **kali > cewl -w customwordlist.txt -d 5 -m 7 www.sans.org**

Let's break that down.

- **-w customwordlist.ext**: the -w means write to the file name that follows.
- **-d 5**: the depth (in this case, 5) that CeWL will crawl to website.
- **-m 7**: the minimum word length; in this case it will grab words of 7 characters minimum.
- **www.sans.org**: the website we are crawling.



```
root@kali:~# cewl -w customwordlist.txt -d 5 -m 7 www.sans.org
```

This command will then crawl the sans.org website to a depth of 5 pages, grabbing words at least 7 letters long. After several hours of crawling through the website, CeWL places all of the words it found into the file

(Ft. THC Hydra)

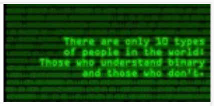
Hack Like a Pro: How to Crack Private & Public SNMP Passwords Using Onesixtyone

Hack Like a Pro: How to Crack Passwords, Part 2 (Cracking Strategy)

Hack Like a Pro: How to Grab & Crack Encrypted Windows Passwords

Newest

The Hacker's Jargon


How to Train Your Python: Part 18, Introduction to Bitwise Operators

Community

GARY CAMP commented on
How to Disable the Lock Screen on Windows 10
This does not work on my windows 10 Home. Seems like I found another thing that is needed only some times but cant find it again. Another method of turning off "login". It did work on another Win 1...

JAZAVICAR commented on
How to Assign a Domain Name to My Local Host ?
You can try with this... http://www.noip.com/

MICHELLE GROISMAN commented on
Spin Your Potatoes for Better Hash Browns at Home
Yesss!!! Just bought a salad spinner and am sooo happy to have another use for it! Breakfast hash browns for dinner? Yes please :-)

JACK SEA commented on
iPhone Security: Apple Refuses FBI's Demands to Create iOS Backdoor
If a backdoor was made, hackers would flood to it and it would probably end up with everyone ditching iPhones and buying secure phones instead.

The "phone" they found is likely worthless anyways.

PETER NEBLETT commented on

Making Electromagnetic Weapons: Directed Microwave Energy

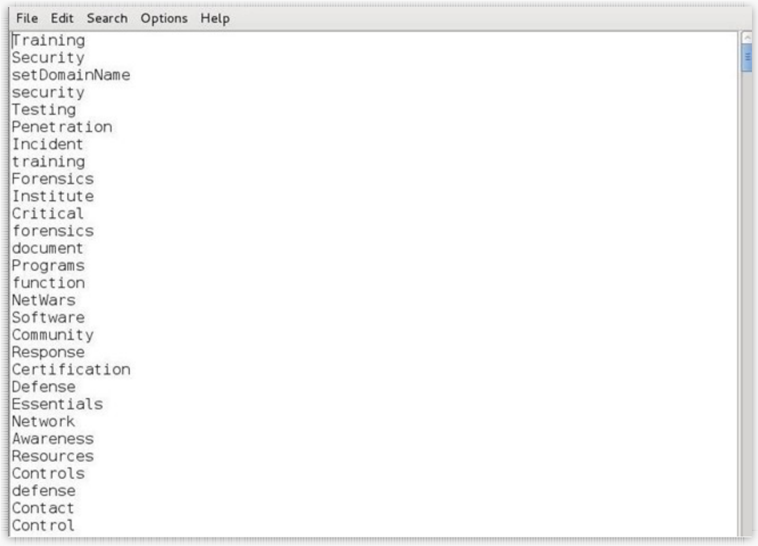
However, you writing -
"I was able to fry an old cell phone from up to 10 feet using three magnetrons and one funnel."
I can...

RAQUEL LYNN published

Spin Your Potatoes for Better Hash Browns at Home

- kali > leafpad customwordlist.txt

This will open the file like that below.



```
Training
Security
setDomainName
security
Testing
Penetration
Incident
training
Forensics
Institute
Critical
forensics
document
Programs
function
NetWars
Software
Community
Response
Certification
Defense
Essentials
Network
Awareness
Resources
Controls
defense
Contact
Control
```

Note that these words are a reflection of the industry that SANS Institute is in—information security.

Step 3: Combine This List with a List Generated by Crunch

Now, combine this wordlist with another wordlist, or one generated by Crunch. Place these words first as they are specific to this user or company and are more likely to be correct.

Of course, we can use CeWL to create custom wordlists for password cracking targets other than employees at a particular company. For instance, if we know the individual who is our target is a soccer fan, we use CeWL to crawl a soccer site to grab soccer related words. That is, we can use CeWL to create specific password lists based upon just about any subject area by simply crawling a website to grab potential keywords.

Stay tuned: we will continue to explore new and better ways to crack passwords in this series, so keep coming back, my novice hackers!

Cover image via Shutterstock

See Also

- Hack Like a Pro: How to Crack Passwords, Part 4 (Creating a Custom Wordlist with Crunch)
- Creating Unique and Safe Passwords, Part 1 Using Wordlists
- Hack Like a Pro: How to Crack Online Web Form Passwords with THC-Hydra & Burp Suite

Show More...

Remember to Give Kudos, Tweet, Like, & Share

Join the Discussion

Subscribe OFF

GHOST_ 2

It always amuses me how simple and easy to guess passwords are. Not only that but the fact that almost everyone uses the same password for everything. What's so hard about creating passwords consisting of ghost_

1 year ago Reply

CIUFFY 1

Effort in remembering or writing them down and time to look them up in your password file.
O tempora, O mores!
People start preventing only when it's too late I guess.

1 year ago Reply

SE7ENPEACE 1

Sometimes you register on a small site.. after a long time.. say 2 years you forget about it.. then you suddenly nees your id for one thing or another... im sure you wont remember the password if you have diff passwords for different accounts..

So it can be a pain in the..

5 months ago Reply

CIUFFY 1

I am sure being hacked is more pain.

Trust me.

5 months ago Reply

ARITRA DRAGNEEL CHAKRABORTY 3

I use my favorite song lines as passwords.. it spans over 25 characters and also i change the usual stuff like o to 0, i to 1, e to 3 etc. I remain consistent and adapt one changing technique, and remembering it is easy!

Note: I use japanese songlines in Romanji, because i love J-pop. More security for free!.. :D

8 months ago Reply

SE7ENPEACE 1

Thats a nice idea..!!

5 months ago Reply

CIUFFY 1

That's clever, I gotta say!
You start writing the password, stop singing and then join ;-)

5 months ago Reply

SE7ENPEACE 1

Hey the qords cewl gets are case sensitive right??
So what to do to try all possible cases or atleast full upper or lower case??

5 months ago Reply

Share Your Thoughts

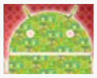
YOU

Click to share your thoughts

ATTACH

Popular How-To Topics in Computers & Programming

Hack router password
Hack facebook account
Hack another computer from y...
Open other computer through ...
Hack security cameras
How to Hack wifi password
Hack other computer with ubu...
How to Hack gmail password
Get your friends facebook pass...
How to Bypass rar password
How to Hack skype password
Bypass facebook blocked
Hack router password
Create video album in my face...
How to Hack wifi passwords
Hack in to another computer t...
Hack an at&t account password
Hack school computer passwor...
Hack into a protected wireless ...
How to Progress bar flash
Hack into someone's gmail
How to Hack hotmail on mac
How to Crack wifi codes
Boost ps3 wifi signal



7 Android-Only Apps That Will Make iPhone Users Green with Envy

Spin Your Potatoes for Better Hash Browns at Home

How to Tell if Your Meat Is Cooked (Without a Thermometer)

Is TOR No Longer Safe?

4 Ways to Crack a Facebook Password and How to Protect Yourself from Them

The World's First $4 Android Phone Is Here... Maybe

iPhone Security: Apple Refuses FBI's Demands to Create iOS Backdoor

How Thieves Unlock Passcodes on Stolen iPhones (And How to Protect Yourself Against It)

Arts

Arts & Crafts
Beauty & Style
Dance
Fine Art
Music & Instruments

Science & Tech

Autos, Motorcycles & Planes
Computers & Programming
Disaster Preparation
Education
Electronics
Film & Theater
Software
Weapons

Lifestyle

Alcohol
Business & Money
Dating & Relationships
Diet & Health
Family
Fitness
Food
Home & Garden
Hosting & Entertaining
Language
Motivation & Self Help
Outdoor Recreation
Pets & Animals
Pranks & Cons
Spirituality
Sports
Travel

Gaming

Gambling
Games
Hobbies & Toys
Magic & Parlor Tricks
Video Games