

## **Ataki na hasła – wina gwiazd**

### **Wprowadzenie**

Słabe hasło to dobrze znany scenariusz, w którym większość korporacji zostaje naruszona. Wiele osób używa słabych haseł, które można złamać metodą brute force i uzyskać zwykły tekst. W tym rozdziale omówimy różne sposoby złamania skrótu hasła uzyskanego podczas aktywności pentestu wykonywanej w aplikacji internetowej/sieci, między innymi. Identyfikowanie różnych typów skrótów w środowisku naturalnym! Skróty są generowane przez jednokierunkowe algorytmy matematyczne, co oznacza, że nie można ich odwrócić. Jedynym sposobem na ich złamanie jest próba brute force. W tym przepisie dowiesz się, jak identyfikować niektóre z różnych typów skrótów.

### **Jak to zrobić...**

Oto typy skrótów.

MD5

To najpopularniejszy typ skrótu. MD to skrót od algorytmu Message Digest. Te skróty można zidentyfikować, korzystając z następującej obserwacji:

Są szesnastkowe.

Mają 32 znaki długości i 128 bitów, na przykład 21232f297a57a5a743894a0e4a801fc3

### **MySQL w wersji krótszej niż v4.1**

Możemy natknąć się na takie hasze podczas wyodrębniania danych z wstrzyknięcia SQL. Te hasze można zidentyfikować, korzystając z następującej obserwacji:

Są również szesnastkowe

Mają 16 znaków długości i 64 bity, na przykład 606727496645bcba

### **MD5 (WordPress)**

Jest to używane w witrynach internetowych tworzonych za pośrednictwem WordPressa. Te skróty można zidentyfikować, korzystając z następującej obserwacji:

Zaczynają się od \$P\$

Zawierają znaki alfanumeryczne

Mają 34 znaki długości i 64 bity, na przykład,

\$P\$9QGUsR07ob2qNMbmSCRh3Moi6ehJZR

### **MySQL 5**

Jest to używane w nowszych wersjach MySQL do przechowywania poświadczeń. Te skróty można zidentyfikować, korzystając z następującej obserwacji:

Są wszystkie WIELKIMI LITERAMI

Zawsze zaczynają się gwiazdką

Mają 41 znaków długości, na przykład,

\*4ACFE3202A5FF5CF467898FC58AAB1D615029441



```
root@kali: ~  
  
Not Found.  
-----  
HASH: D033E22AE348AEB5660FC2140AEC35850C4DA997  
  
Possible Hashs:  
[+] SHA-1  
[+] MySQL5 - SHA-1(SHA-1($pass))  
  
Least Possible Hashs:  
[+] Tiger-160  
[+] Haval-160  
[+] RipeMD-160  
[+] SHA-1(HMAC)
```

### Łamanie za pomocą patatora

Czasami jest możliwe, że mamy nazwy użytkowników, ale chcemy spróbować siłowego ataku na hasło. Patator to niesamowite narzędzie, które pozwala nam siłowo atakować wiele typów loginów, a nawet hasła ZIP. W tym przepisie zobaczymy, jak użyć patatora, aby wykonać atak siłowy.

#### Jak to zrobić...

Oto kroki, aby użyć patatora:

1. Aby zobaczyć wszystkie opcje, używamy następującego polecenia:

```
patator -h
```

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

```
root@kali:~# patator -h  
Patator v0.5 (http://code.google.com/p/patator/)  
Usage: patator.py module --help  
  
Available modules:  
+ ftp_login : Brute-force FTP  
+ ssh_login : Brute-force SSH  
+ telnet_login : Brute-force Telnet  
+ smtp_login : Brute-force SMTP  
+ smtp_vrfy : Enumerate valid users using SMTP VRFY  
+ smtp_rcpt : Enumerate valid users using SMTP RCPT  
+ finger_lookup : Enumerate valid users using Finger  
+ http_fuzz : Brute-force HTTP  
+ pop_login : Brute-force POP3  
+ pop_passwd : Brute-force popassd (http://netwin.com)  
+ imap_login : Brute-force IMAP4  
+ ldap_login : Brute-force LDAP  
+ smb_login : Brute-force SMB  
+ smb_lookupsid : Brute-force SMB SID-lookup
```

2. Spróbujmy wykonać atak siłowy na logowanie FTP:

```
patator ftp_login
```

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

```
root@kali:~# patator ftp_login
Patator v0.5 (http://code.google.com/p/patator/)
Usage: ftp_login <module-options ...> [global-options ...]

Examples:
  ftp_login host=10.0.0.1 user=FILE0 password=FILE1 0=logins.txt 1=passwords.txt
  -x ignore:msg='Login incorrect.' -x ignore,reset,retry:code=500
  report
Module options:
  host      : target host
  port      : target port [21]
  user      : usernames to test
  password  : passwords to test
  tls       : use TLS [0|1]
  timeout   : seconds to wait for a response [10]
  persistent : use persistent connections [1|0]
```

3. Teraz możemy ustawić hosta, plik użytkownika i plik hasła oraz uruchomić moduł:

```
patator ftp_login host=192.168.36.16 user=ftp password=ftp
```

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

```
root@kali:~# patator ftp_login host=192.168.36.16 user=ftp password=ftp
00:49:42 patator INFO - Starting Patator v0.5 (http://code.google.com/p/patator/)
00:49:42 patator INFO -
00:49:42 patator INFO - code size | candidate
00:49:42 patator INFO - -----|-----
00:49:42 patator INFO - 230 44 |
00:49:42 patator INFO - Hits/Done/Skip/Fail/Size: 1/1/0/0/1, Avg: 9 r/s,
root@kali:~#
```

4. Widzimy, że dostęp został przyznany, a moduł został zatrzymany.

### Łamanie haszy online

Często, gdy natrafiamy na hasze podczas testów penetracyjnych, dobrym pomysłem jest sprawdzenie hasza online: czy został już złamany, czy nie. W tym przepisie dowiesz się o kilku fajnych stronach internetowych, które oferują usługę łamania haszy.

#### Jak to zrobić...

Przyjrzyjmy się identyfikacji różnych typów haszy.

### Hashkiller

Poniższe kroki demonstrują użycie Hashkillera:

1. Hashkiller to świetna usługa, w której możemy przysyłać nasze hasze, a jeśli zostały już złamane w przeszłości, pokaże nam tekst jawny:

Secure | https://hashkiller.co.uk

THE PERCENTAGE **ONLY REAL PASSWORDS OF USERS!** IS MORE THAN 50%!

Home Forums **Decrypter / Cracker** Database Info Hash Min Max WPA Crack Lists and Competition

HashKiller's purpose is to serve as a meeting place for computer hobbyists, security researchers and penetration testers demonstrating the weakness of using hash based storage / authentication.

**Last 50 successful MD5 decriptions / founds**

#	Hash	Type
1	ac7fcc79d7d4e0837d76759b5455e48cf04665f4	MySQL4.1/MySQL5
2	8d51ea84c08d644a00d9421a63c5cb860bddfe73	MySQL4.1/MySQL5
3	510a42dea314f9b130b868bdac7dcdc673efec58	MySQL4.1/MySQL5
4	e3b06c4a3493985195d4999490471b6cc74428f0	MySQL4.1/MySQL5
5	b047d1c64f0eb83fbc97319b155560fa6d3fd13a	MySQL4.1/MySQL5
6	2aa1b7bc14e72e7914e461afcb16419c9a760c58	MySQL4.1/MySQL5

2. Proces jest prosty; wystarczy wybrać opcję na stronie internetowej, gdzie jest napisane Decrypter/Cracker, a następnie kliknąć na typ hasha, który chcemy złamać:

**Decrypter / Cracker** Database

MD5 Decrypter

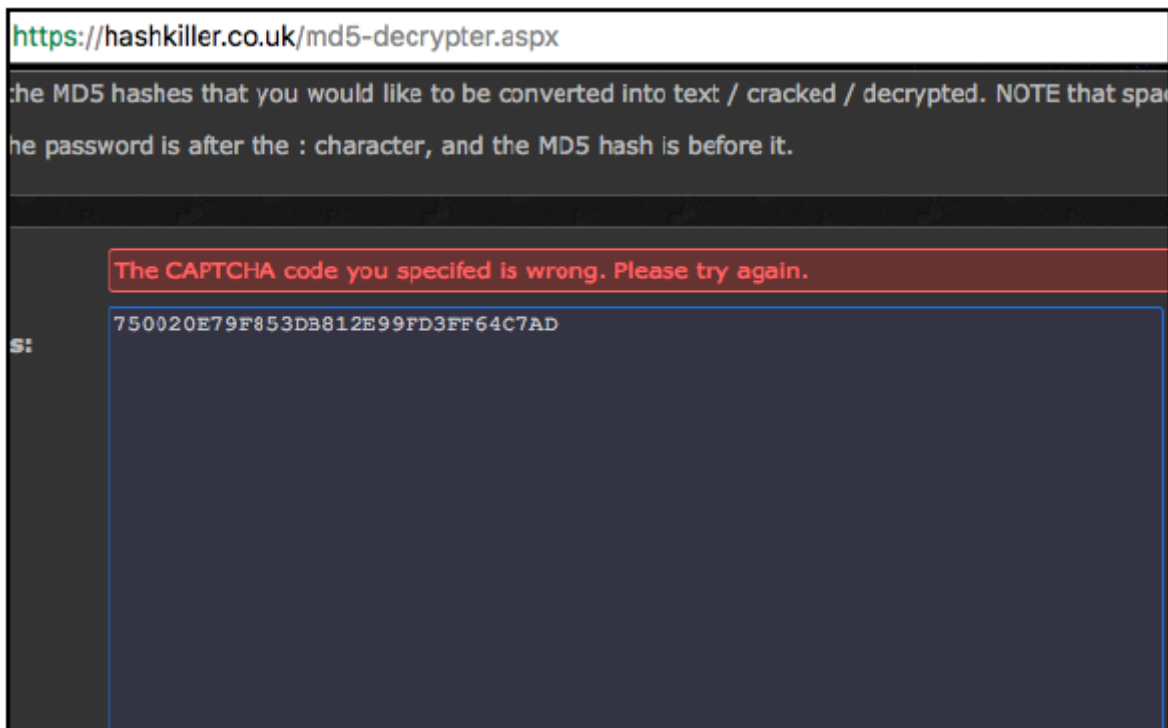
NTLM Decrypter

SHA1 Decrypter

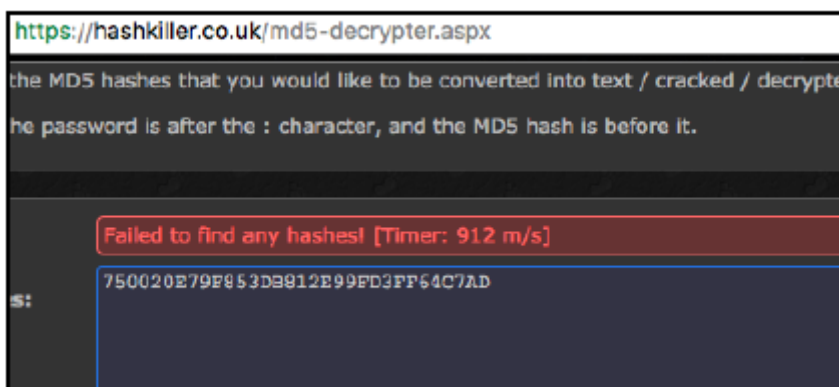
Submit Finds

Competition

3. Na stronie, która się otworzy, wklejamy nasz hash, wypełniamy CAPTCHA, a następnie klikamy Prześlij:



4. Jeśli hash istnieje, zostanie nam wyświetlony tekst jawny; w przeciwnym razie zobaczymy komunikat: Nie znaleziono żadnych hashów!:



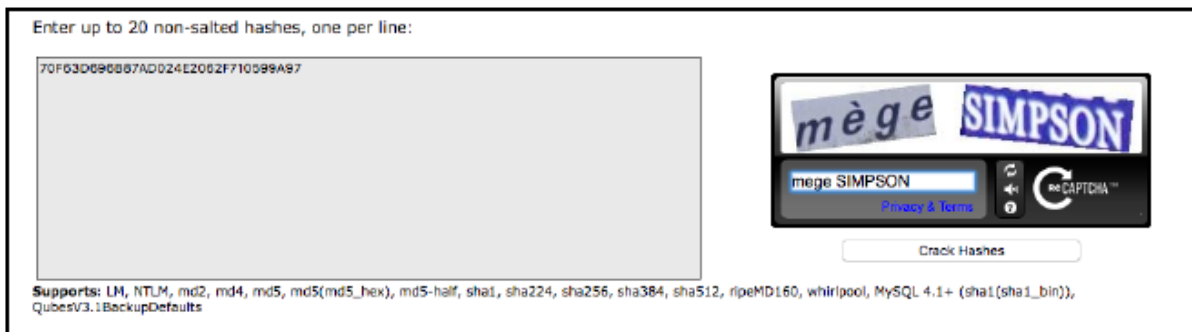
### Crackstation

Crackstation to bezpłatna usługa obsługująca łamanie MD2, MD5, NTLM i SHA1. Używa własnej listy słów i tabel wyszukiwania, aby skutecznie przeprowadzić wyszukiwanie zwykłego tekstu hasha w swojej bazie danych:

1. Odwiedzamy stronę internetową <https://crackstation.net/> :



2. Wklejamy hash, który chcemy złamać i wypełniamy CAPTCHA:



3. Jeśli skrót zostanie znaleziony, zobaczymy tekst jawny; w przeciwnym razie zobaczymy komunikat informujący, że skrót nie został znaleziony:

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1(sha1\_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
70F63D696B87AD024E2062F710599A97	Unknown	Not found.

Color Codes: **Green**: Exact match, **Yellow**: Partial match, **Red**: Not found.

4. Crackstation udostępnia również link do pobrania listy haseł i tabel wyszukiwania, jeśli chcemy ich użyć do łamania haseł offline za pomocą m.in. hashcat, <https://crackstation.net/buy-crackstation-wordlist-passwordcracking-dictionary.htm>:

<https://crackstation.net/buy-crackstation-wordlist-password-cracking-dictionary.htm>

**Step 2: Download!**

**Note:** To download the torrents, you will need a torrent client like Transmission (for Linux and Mac), or uTorrent for Windows.

**Torrent (Fast)**  
GZIP-compressed (level 9). 4.2 GiB compressed. 15 GiB uncompressed.

**HTTP Mirror (Slow)**

**Checksums (crackstation.txt.gz)**

MD5: 4748a72706ff934a17662446862ca4f8  
 SHA1: efa3f5ecbfba03df523418a70871ec59757b6d3f  
 SHA256: a6dc17d27d0a34f57c989741acdd485b8aee45a6e9796daf8c9435370dc61612

**Smaller Wordlist (Human Passwords Only)**

I got some requests for a wordlist with just the "real human" passwords leaked from various website databases. This list contains 64 million passwords. There are about 64 million passwords in this list!

**Torrent (Fast)**  
GZIP-compressed. 247 MiB compressed. 684 MiB uncompressed.

**HTTP Mirror (Slow)**

### OnlineHashCrack

To usługa freemium i jedna z moich ulubionych. Obsługuje OSX, MD4, MD5, NTLM, WPA(2) i brute force dokumentów chronionych Word, Excel, PPT. Zapewnia do ośmiu znaków bez hasła, po czym pobiera niewielką opłatę za ujawnienie hasła, które zostało pomyślnie złamane:

1. Odwiedzamy stronę internetową <http://onlinehashcrack.com/>:

<https://www.onlinehashcrack.com>

onlineHashCrack  
Professional Password Recovery

**HOME** | **HASHES** | **WIFI** | **Office**

MD5, NTLM, MYSQL, SHA1.. | Recover WPA(2) Handshakes | Word, Excel & Powerpoint Files

**ONLINE HASH CRACK IS A PASSWORD RECOVERY SERVICE**  
**ASSISTING PENTESTERS & SECURITY EXPERTS**

2. Tutaj możemy przesłać nasze hashe lub plik .apt do złamania oraz adres e-mail, na który chcemy otrzymywać powiadomienia:



### Password/Hashes crack

ENTER YOUR HASHES (UP TO 10):

ONE HASH PER LINE

Hash acceptance list.

EMAIL:

valid email for notification

SUBMIT

### Wifi WPA(2) crack

UPLOAD YOUR CAPTURE FILE:

[Choose file](#) No file chosen

- 📁 \*.cap or \*.pcap or \*.hccap
- 📁 Max size : 10 Mb
- 📁 Automatically select the first ESSID

EMAIL:

Valid email for notification

SUBMIT

3. Na unikalnym linku, który otrzymujemy w wiadomości e-mail, możemy zobaczyć status wszystkich hashów, które zostały złamane lub nie zostały znalezione na stronie internetowej:

Online HashCrack		Professional Password Recovery		HOME	HASHES	WIFI	OFFICE	HOW TO?	A
50	2016-01-13	00D3CE11561C36889060663B629F8D34	-	Not found.	-	-	-	✕	✎
51	2015-11-23	\$P\$Bc5Np.ZY4CPkgUNM6woyHAz18imEy1	Wordpress/Joomla	Found !	8	<a href="#">Buy now</a>	-	✕	✎
52	2015-11-23	\$P\$Bn/FwVncpeJ9R3MMA9OFwfUDRLvTBa.	-	Not found.	-	-	-	✕	✎
53	2015-11-19	12ADFBC1A3123845B1826BC6306D4F7D	MD5	Found !	8	<a href="#">Buy now</a>	-	✕	✎
54	2015-11-19	2A7343A0F575C37262EDAD20156B11CE	MD5	Found !	9	Asho0k!23	-	✕	✎ ↓ i

### Zabawa z Johny The Ripper

Strony internetowe i usługi online mogą nie być zawsze dostępne i możliwe jest również, że te strony internetowe mogą nie mieć zwykłego tekstu hasha, który znaleźliśmy. W takich przypadkach możemy użyć różnych narzędzi offline, które są dostępne do łamania haszy. Załóżmy, że mamy teraz hash i zidentyfikowaliśmy jego typ. W tym przepisie zobaczymy, jak łamać hasze za pomocą Johna the rippera. John jest szybki i obsługuje różne tryby łamania. Ma również możliwość automatycznego wykrywania typu hasha.

### Jak to zrobić...

aby dowiedzieć się więcej o Johnie the ripperze, wykonaj następujące kroki:

1. Możemy zobaczyć pełne funkcje za pomocą polecenia help (-h):

```
john -h
```

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

```
root@kali:~# john -h
John the Ripper password cracker, version 1.8.0.6-jumbo-1-bleeding_omp [linux-gr
Copyright (c) 1996-2015 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION]      "single crack" mode
--wordlist[=FILE] --stdin wordlist mode, read words from FILE or stdin
                        --pipe   like --stdin, but bulk reads, and allows rules
--loopback[=FILE]      like --wordlist, but fetch words from a .pot file
--dupe-suppression      suppress all dupes in wordlist (and force preload)
--encoding=NAME         input encoding (eg. UTF-8, ISO-8859-1). See also
                        doc/ENCODING and --list=hidden-options.
--rules[=SECTION]      enable word mangling rules for wordlist modes
--incremental[=MODE]   "incremental" mode [using section MODE]
--mask=MASK             mask mode using MASK
--markov[=OPTIONS]     "Markov" mode (see doc/MARKOV)
--external=MODE         external mode or word filter
--stdout[=LENGTH]      just output candidate passwords [cut at LENGTH]
--restore[=NAME]       restore an interrupted session [called NAME]
--session=NAME         give a new session the NAME
--status[=NAME]        print status of a session [called NAME]
```

2. Aby złamać hasło, używamy następującego polecenia:

```
john --format=raw-md5
```

```
--wordlist=/usr/share/wordlists/rockyou.txt /root/demo_hash.txt
```

3. Zobaczymy, że hasło zostało pomyślnie złamane!

```
root@kali:~# john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt /root
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 32/32])
Press 'q' or Ctrl-C to abort, almost any other key for status
admin      (7)
lg 0:00:00:00 DONE (2017-02-20 01:29) 8.333g/s 165158p/s 165158c/s 165158C/s admin
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

## Johnny Bravo!

Johnny to klient GUI dla Johna. Ponieważ dodaje interfejs użytkownika, staje się znacznie łatwiejszy w użyciu.

Jak to zrobić...

Aby dowiedzieć się więcej o Johnnym, wykonaj podane kroki:

1. Nauczysz się używać Johna w poprzednim przepisie. Uruchomimy Johnny'ego za pomocą następującego polecenia:

```
johnny
```

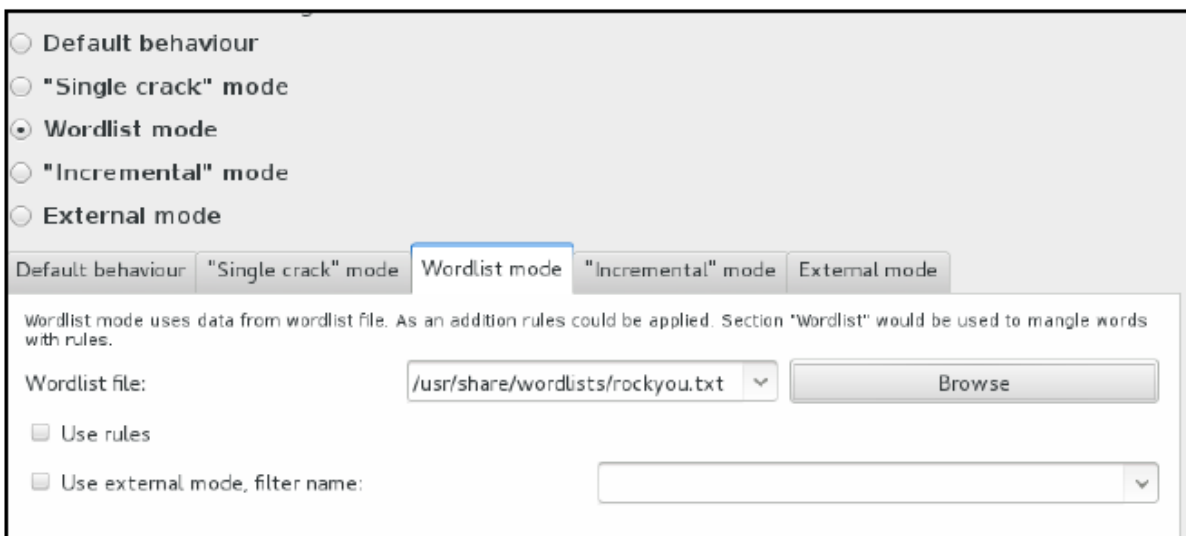
Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:



2. Wczytujemy nasz plik haseł, klikając na opcję Open Passwd File. Nasz plik jest wczytywany:

	User	Password	Hash	GECOS
1 ?			21232f297...	
2 ?				

3. Teraz przechodzimy do Opcji i wybieramy rodzaj ataku, który chcemy przeprowadzić:



4. Wybieramy format skrótu:



5. Po wykonaniu tej czynności klikamy na Start Attack, a powinniśmy zobaczyć nasze hasło po jego złamaniu.

## Używanie cewl

Cewl to oparty na Ruby crawler, który przeszukuje adres URL i wyszukuje słowa, które mogą być użyte do ataków na hasła. W tym przepisie przyjrzymy się, jak wykorzystać go na naszą korzyść.

### Jak to zrobić...

Oto kroki dotyczące korzystania z cewl:

1. Aby wyświetlić wszystkie opcje cewl, używamy tego polecenia:

```
cewl -h
```

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

```
root@kali:~# cewl -h
CeWL 5.1 Robin Wood (robin@digl.ninja) (http://digl.ninja)

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 pa
  --count, -c: show the count for each word found
```

2. Aby przeszukać witrynę, używamy tego polecenia:

```
cewl -d 2 http://192.168.36.16/forum/
```

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

```
root@kali:~# cewl -d 2 "http://192.168.36.16/forum/"
CewL 5.1 Robin Wood (robin@digi.ninja) (http://digi.ninja)

ssh
Mar
testbox
131
User
from
RSS
pam
auth
port
unix
preauth
invalid
thread
Bye
Forum
```

3. Zobaczymy listę interesujących słów kluczowych, które można wykorzystać do utworzenia własnego słownika listy haseł:

```
root@kali:~# crunch 2 2 abcdef
Crunch will now generate the following amount of data: 108 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 36
aa
ab
ac
ad
ae
af
ba
```

### Generowanie listy słów za pomocą crunch

Crunch to generator listy słów. Używa permutacji i kombinacji, aby wygenerować wszystkie możliwe kombinacje dostarczonego zestawu znaków.

#### Jak to zrobić...

Aby dowiedzieć się więcej o Crunch, wykonaj poniższe kroki:

1. Crunch jest preinstalowany z Kali i możemy go uruchomić za pomocą tego polecenia:

```
crunch -h
```

```
root@kali:~# crunch -h
crunch version 3.6

Crunch can create a wordlist based on criteria you specify. The output

Usage: crunch <min> <max> [options]
where min and max are numbers

Please refer to the man page for instructions and examples on how to use
```

2. Jak widać, łatwo jest wygenerować listę haseł składającą się z minimum dwóch znaków i maksimum dwóch znaków, zawierającą tylko abcdef, i możemy użyć następującego polecenia:

```
crunch 2 2 abcdef
```

Możemy zobaczyć, że lista słów została wygenerowana:

```
root@kali:~# crunch 2 2 abcdef
Crunch will now generate the following amount of data: 108 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 36
aa
ab
ac
ad
ae
af
ba
```

3. Aby zapisać go w pliku, możemy użyć przełącznika -o. Crunch ma również wbudowaną listę zawierającą wstępnie zdefiniowany zestaw znaków. Można ją znaleźć w /usr/share/crunch/charset.lst.

4. Aby użyć zestawu znaków, używamy przełącznika -f:

```
crunch 2 2 -f /usr/share/crunch/charset.lst lalpha
```

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

```

1 # charset configuration file for winrtgen v1.2 by Massimiliano Montoro (mao@oxid.it)
2 # compatible with rainbowcrack 1.1 and later by Zhu Shuanglei <shuanglei@hotmail.com>
3
4
5 hex-lower          = [0123456789abcdef]
6 hex-upper         = [0123456789ABCDEF]
7
8 numeric           = [0123456789]
9 numeric-space    = [0123456789 ]
10
11 symbols14         = [!@#%&*()-_+=]
12 symbols14-space  = [!@#%&*()-_+= ]
13
14 symbols-all      = [!@#%&*()-_+=~`[]{}|\:;''<>,.?/]
15 symbols-all-space = [!@#%&*()-_+=~`[]{}|\:;''<>,.?/ ]
16
17 ualpha           = [ABCDEFGHIJKLMNOPQRSTUVWXYZ]
18 ualpha-space     = [ABCDEFGHIJKLMNOPQRSTUVWXYZ ]
19 ualpha-numeric   = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]
20 ualpha-numeric-space = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 ]
21 ualpha-numeric-symbol14 = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#%&*()-_+=]
22 ualpha-numeric-symbol14-space = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#%&*()-_+= ]
23 ualpha-numeric-all = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#%&*()-_+=~`[]{}|\:;''<>,.?/]
24 ualpha-numeric-all-space = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#%&*()-_+=~`[]{}|\:;''<>,.?/ ]
25

```

5. Spowoduje to wygenerowanie listy o minimalnej i maksymalnej długości 2, zawierającej małe litery alfabetu. Crunch ma również przełącznik -t, który można wykorzystać do utworzenia listy słów określonego wzorca:

@: Spowoduje to wstawienie małych liter

,: Spowoduje to wstawienie wielkich liter

?: Spowoduje to wstawienie cyfr

^: Spowoduje to wstawienie symboli

6. Przełącznik -b można wykorzystać do określenia rozmiaru pliku, który chcesz utworzyć:

```

root@kali:~# crunch 10 10 -t @@packt,,% -b 1mib -o START
Crunch will now generate the following amount of data: 50267360 bytes
47 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 4569760

crunch: 2% completed generating output
crunch: 4% completed generating output

```

7. Spróbujmy utworzyć listę ze specyficznym wzorcem i o rozmiarze 1 MB:

crunch 10 10 -t @@packt,,% -b 1mib -o START

8. Po wykonaniu tej czynności zobaczymy listę plików tekstowych utworzonych ze wzorcem w tym samym folderze:

```
ubpacktTM5-uppacktWC9.txt
uppacktWD0-vdpacktYT4.txt
vdpacktYT5-vspacktBJ9.txt
vspacktBK0-wgpacktEA4.txt
wgpacktEA5-wupacktGQ9.txt
wupacktGR0-xipacktJH4.txt
xipacktJH5-xwpacktLX9.txt
xwpacktLY0-ykpackt004.txt
ykpackt005-yypacktRE9.txt
yypacktRF0-zmpacktTV4.txt
zmpacktTV5-zzpacktZZ9.txt
```

9. Flaga -z może być użyta do utworzenia listy słów i zapisania jej w skompresowanym pliku. Kompresja jest wykonywana na bieżąco:

```
crunch 10 10 -t @@packt,,% -b 1mib -o START -z gzip
```

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

```
pepacktVU0-pspacktYK4.txt.gz
pspacktYK5-qhpacktBA9.txt.gz
qhpacktBB0-qvpacktDR4.txt.gz
qvpacktDR5-rjpacktGH9.txt.gz
rjpacktGI0-rxpacktIY4.txt.gz
rxpacktIY5-slpacktLO9.txt.gz
slpacktLP0-szpacktOF4.txt.gz
szpacktOF5-tnpacktQV9.txt.gz
tnpacktQW0-ubpacktTM4.txt.gz
ubpacktTM5-uppacktWC9.txt.gz
uppacktWD0-vdpacktYT4.txt.gz
vdpacktYT5-vspacktBJ9.txt.gz
vspacktBK0-wgpacktEA4.txt.gz
wgpacktEA5-wupacktGQ9.txt.gz
wupacktGR0-xipacktJH4.txt.gz
xipacktJH5-xwpacktLX9.txt.gz
xwpacktLY0-ykpackt004.txt.gz
ykpackt005-yypacktRE9.txt.gz
yypacktRF0-zmpacktTV4.txt.gz
zmpacktTV5-zzpacktZZ9.txt.gz
```



pepacktVU0-pspacktYK4.txt.gz  
pspacktYK5-qhpacktBA9.txt.gz  
qhpacktBB0-qvpacktDR4.txt.gz  
qvpacktDR5-rjpacktGH9.txt.gz  
rjpacktGI0-rxpacktIY4.txt.gz  
rxpacktIY5-slpacktL09.txt.gz  
slpacktLP0-szpackt0F4.txt.gz  
szpackt0F5-tnpacktQV9.txt.gz  
tnpacktQW0-ubpacktTM4.txt.gz  
ubpacktTM5-uppacktWC9.txt.gz  
uppacktWD0-vdpacktYT4.txt.gz  
vdpacktYT5-vspacktBJ9.txt.gz  
vspacktBK0-wgpacktEA4.txt.gz  
wgpacktEA5-wupacktGQ9.txt.gz  
wupacktGR0-xipacktJH4.txt.gz  
xipacktJH5-xwpacktLX9.txt.gz  
xwpacktLY0-ykpackt004.txt.gz  
ykpackt005-yypacktRE9.txt.gz  
yypacktRF0-zmpacktTV4.txt.gz  
zmpacktTV5-zzpacktZZ9.txt.gz