מבוא להאקינג
המשך

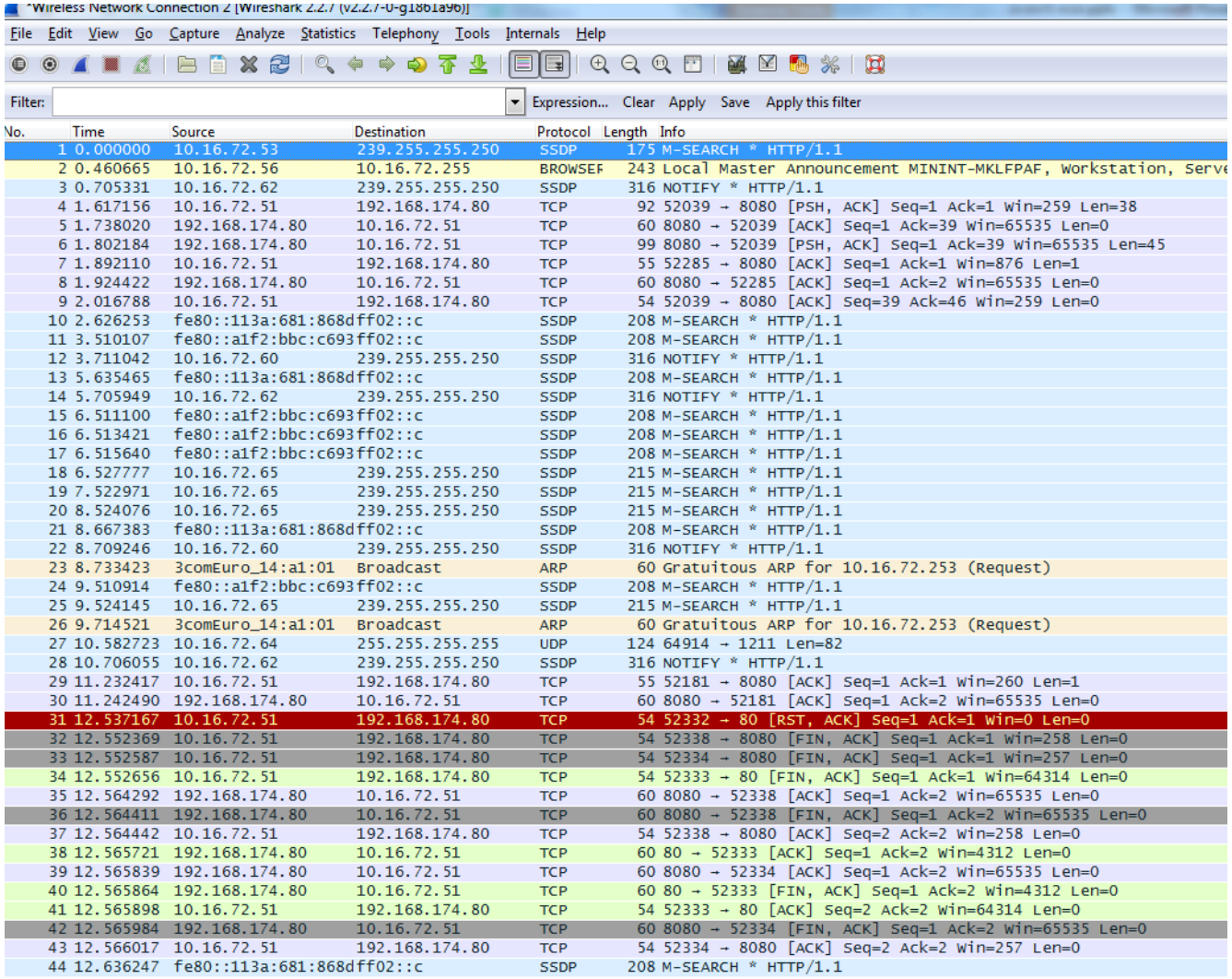
Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

SNIFFER – רחרחן

תוכנה שיודעת לראות מה עובר ברשת המחשבים

לדוגמא:

WIRESHARK

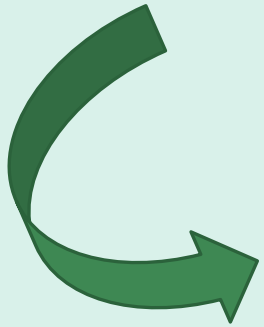


Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

כלי האקינג נוספים

BACK TRACK

הפך בהמשך ל-KALI LINUX



- כלי האזנה לתעבורת רשת
- כלי סריקת חורי אבטחה במערכות שונות
- כלי פיצוח סיסמאות
- כלי פריצת רשתות אלחוטיות
- כלים למתקפות שונות

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

כלי סריקה – PORT SCANNING

Common TCP Ports

According to the Nmap classification, these are the most common TCP ports:

- 21 - FTP (File Transfer Protocol)
- 22 - SSH (Secure Shell)
- 23 - Telnet
- 25 - SMTP (Mail)
- 80 - HTTP (Web)
- 110 - POP3 (Mail)
- 143 - IMAP (Mail)
- 443 - HTTPS (Secure Web)
- 445 - SMB (Microsoft File Sharing)
- 3389 - RDP (Remote Desktop Protocol)

Our TCP Port Scanner with Nmap

The **Full Scan** allows you to perform portscans with **custom parameters**, easily configured from the web interface:

- Specify custom TCP ports to scan (1-65535)
- Enable/disable service detection
- Enable/disable operating system detection
- Enable/disable host discovery
- Do Traceroute

המטרה:

מציאת שירות פתוח (פורט פתוח)

הכלי: NMAP

65,535 TCP Ports
65,535 UDP Ports

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

בעזרת תכנה שנקראת hydra נמצאת בחבילת ה-KALI LINUX - BRUTE FORCE

Password Protection

This table illustrates maximum times for a brute force attack for passwords of 96 character complexity (upper and lower case, numbers, and special characters). If your passwords cannot be this complex, the amount of time would be greatly reduced.

The calculations are based on 96 to the power of the password characters. So a password of length 8 characters has 96^8 complexity or 7.2 quadrillion possible combinations. The table further shows 4 columns of brute force password processing attempts in units per second. The first column is 10 million per second, which is possible to do with a modern quad core processor. The last column is 76 billion per second, which is possible to do with a botnet. The table lists the maximum amount of time. It is possible to reduce this time using different password- cracking technologies such as dictionaries and look-up tables.

		QUAD CORE		BOT NET	
Number of Characters	Complexity (96^x)	10 Million / sec	100 Million / sec	76 Billion / sec	2.5 Quadrillion / sec
4	84.9 Million	8.49 seconds	< 1 second	< 1 second	< 1 second
6	782.8 Billion	21.7 hours	2.2 hours	10.3 seconds	< 1 second
7	75.1 Trillion	87 days	8.7 days	16.5 minutes	< 1 second
8	7.2 Quadrillion	22.9 years	2.3 years	1.1 days	2.9 seconds
9	692.5 Quadrillion	> 100 years	> 100 years	105.5 days	4.6 minutes

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

איך עובד BTUTE FORCE

מכינים קובץ txt וקוראים לו בשם : wordlist.txt

הקובץ מכיל: שורות המכילות אותיות או מספרים שעשוים להיות בסיסמא

למשל אם שמי יוסי (yossi)

שם הדוא"ל שלי: yosish@sviva.gov.il

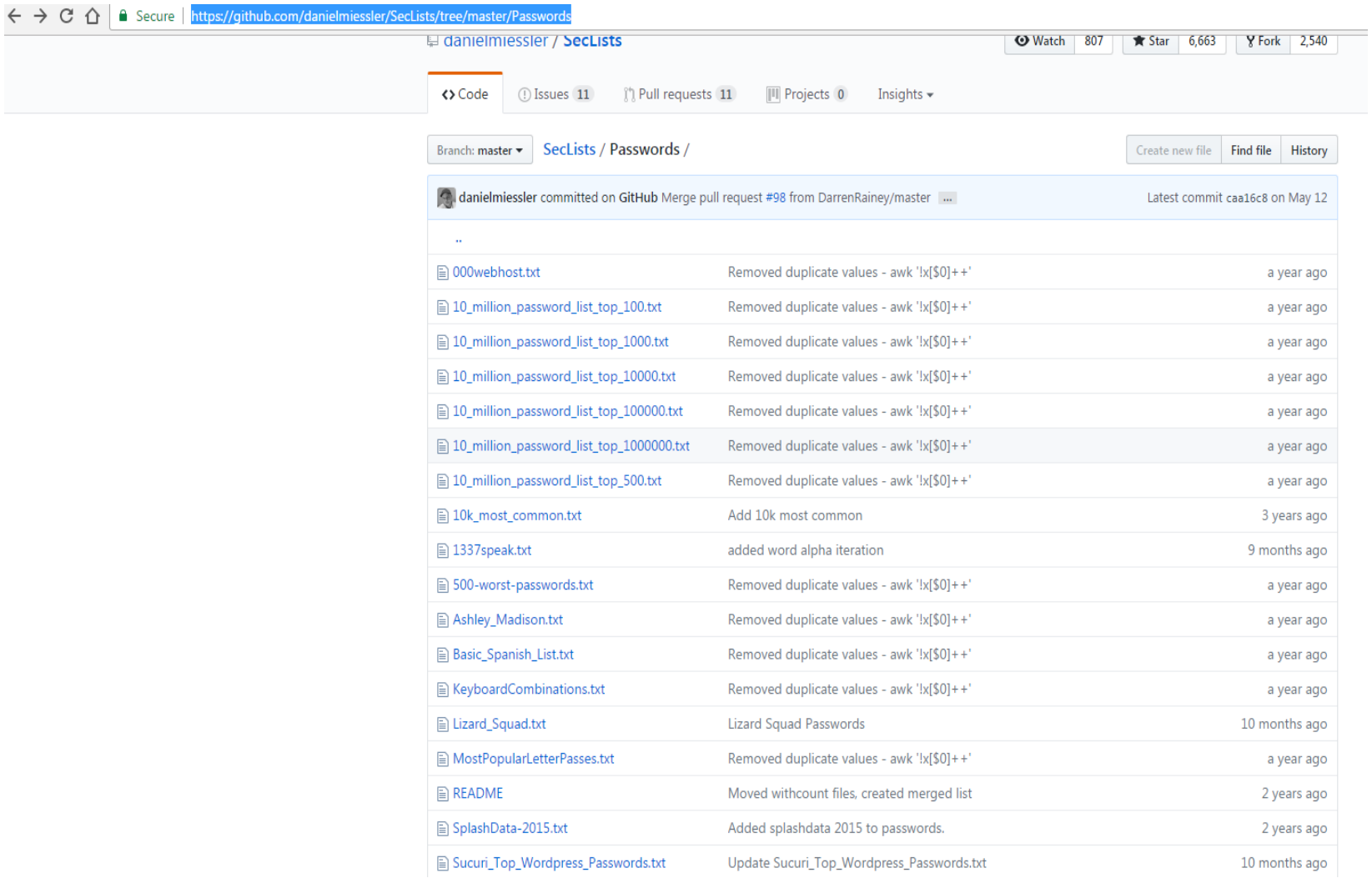
מה עשויה להכיל הסיסמא?

ישנם רשימות מוכנות ברשת שמכילות סיסמאות או קומבינציות שעשויות להביא לסיסמא :

https://github.com/danielmiessler/SecLists/tree/master/Passwords

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

דוגמאות



Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

Branch: master ▾ SecLists / Passwords / Go to file

clem9669 committed 7da5c78 26 days ago ... History

..		
Common-Credentials	PR about the issue: #438	26 days ago
Cracked-Hashes	Quick rename of files	2 years ago
Default-Credentials	strip trailing whitespace	2 months ago
Honeypot-Captures	strip trailing whitespace	2 months ago
Leaked-Databases	strip trailing whitespace	2 months ago
Malware	Close #291 - Fix encoding issues	14 months ago
Permutations	rename 's/_/-/g'	3 years ago
Software	Close #291 - Fix encoding issues	14 months ago
WiFi-WPA	Add "-" to split up words, moved files since PR accepted	2 years ago
Keyboard-Combinations.txt	Add "-" to split up words, moved files since PR accepted	2 years ago
Most-Popular-Letter-Passes.txt	Add "-" to split up words, moved files since PR accepted	2 years ago
PHP-Magic-Hashes.txt	Adding sha256 magic hash	12 months ago
README.md	removes exec. bits	2 years ago
SCRABBLE-hackerhouse.tgz	Add scrabble	11 months ago
UserPassCombo-Jay.txt	"Passwords/" Clean up	3 years ago
bt4-password.txt	strip trailing whitespace	2 months ago
cirt-default-passwords.txt	strip trailing whitespace	2 months ago
clarkson-university-82.txt	strip trailing whitespace	2 months ago

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

Branch: master ▾ SecLists / Passwords / Keyboard-Combinations.txt

g0tmi1k Add "-" to split up words, moved files since PR accepted ...

1 contributor

9604 lines (9604 sloc) | 82.5 KB

```
1   zaq1zaq1
2   zaq1xsw2
3   zaq1cde3
4   zaq1vfr4
5   zaq1bgt5
6   zaq1nhy6
7   zaq1mju7
8   zaq1,ki8
9   zaq1.lo9
10  zaq1/;p0
11  zaq1ZQ!
12  zaq1XW@
13  zaq1DE#
14  zaq1FR$
15  zaq1BGT%
16  zaq1NHY^
17  zaq1JU&
18  zaq1<KI*
19  zaq1LO(
20  zaq1?:P)
21  zaq1qwer
22  zaq11234
23  zaq1asdf
24  zaq1zxcv
25  zaq1!@#$
26  zaq12345
27  zaq13456
28  zaq14576
29  zaq15678
30  zaq16789
31  zaq17890
32  zaq1890-
33  zaq190=-
34  zaq10-=\
```


Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

סיסמאות נפוצות

המשרד להגנת הסביבה

סייבר בתעשייה
המשרד להגנת הסביבה

Rank	2011[4]	2012[5]	2013[6]	2014[7]	2015[8]	2016[3]	2017[9]	2018[10]	2019[11]
1	password	password	123456	123456	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password	password	123456789
3	12345678	12345678	12345678	12345	12345678	12345	12345678	123456789	qwerty
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty	12345678	password
5	abc123	qwerty	abc123	qwerty	12345	football	12345	12345	1234567
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789	111111	12345678
7	1234567	letmein	111111	1234	football	1234567890	letmein	1234567	12345
8	letmein	dragon	1234567	baseball	1234	1234567	1234567	sunshine	iloveyou
9	trustno1	111111	iloveyou	dragon	1234567	princess	football	qwerty	111111
10	dragon	baseball	adobe123[a]	football	baseball	1234	iloveyou	iloveyou	123123
11	baseball	iloveyou	123123	1234567	welcome	login	admin	princess	abc123
12	111111	trustno1	admin	monkey	1234567890	welcome	welcome	admin	qwerty123
13	iloveyou	1234567	1234567890	letmein	abc123	solo	monkey	welcome	1q2w3e4r
14	master	sunshine	letmein	abc123	111111	abc123	login	666666	admin
15	sunshine	master	photoshop[a]	111111	1qaz2wsx	admin	abc123	abc123	qwertyuiop
16	ashley	123123	1234	mustang	dragon	121212	starwars	football	654321
17	bailey	welcome	monkey	access	master	flower	123123	123123	555555
18	passw0rd	shadow	shadow	shadow	monkey	passw0rd	dragon	monkey	lovely
19	shadow	ashley	sunshine	master	letmein	dragon	passw0rd	654321	7777777
20	123123	football	12345	michael	login	sunshine	master	!@#$%^&*	welcome
21	654321	jesus	password1	superman	princess	master	hello	charlie	888888
22	superman	michael	princess	696969	qwertyuiop	hottie	freedom	aa123456	princess
23	qazwsx	ninja	azerty	123123	solo	loveme	whatever	donald	dragon
24	michael	mustang	trustno1	batman	passw0rd	zaq1zaq1	qazwsx	password1	password1
25	Football	password1	000000	trustno1	starwars	password1	trustno1	qwerty123	123qwe

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

התאחדות התעשיינים בישראל

סרטון האקר בפעולת פריצת סיסמא...

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

Google Hack

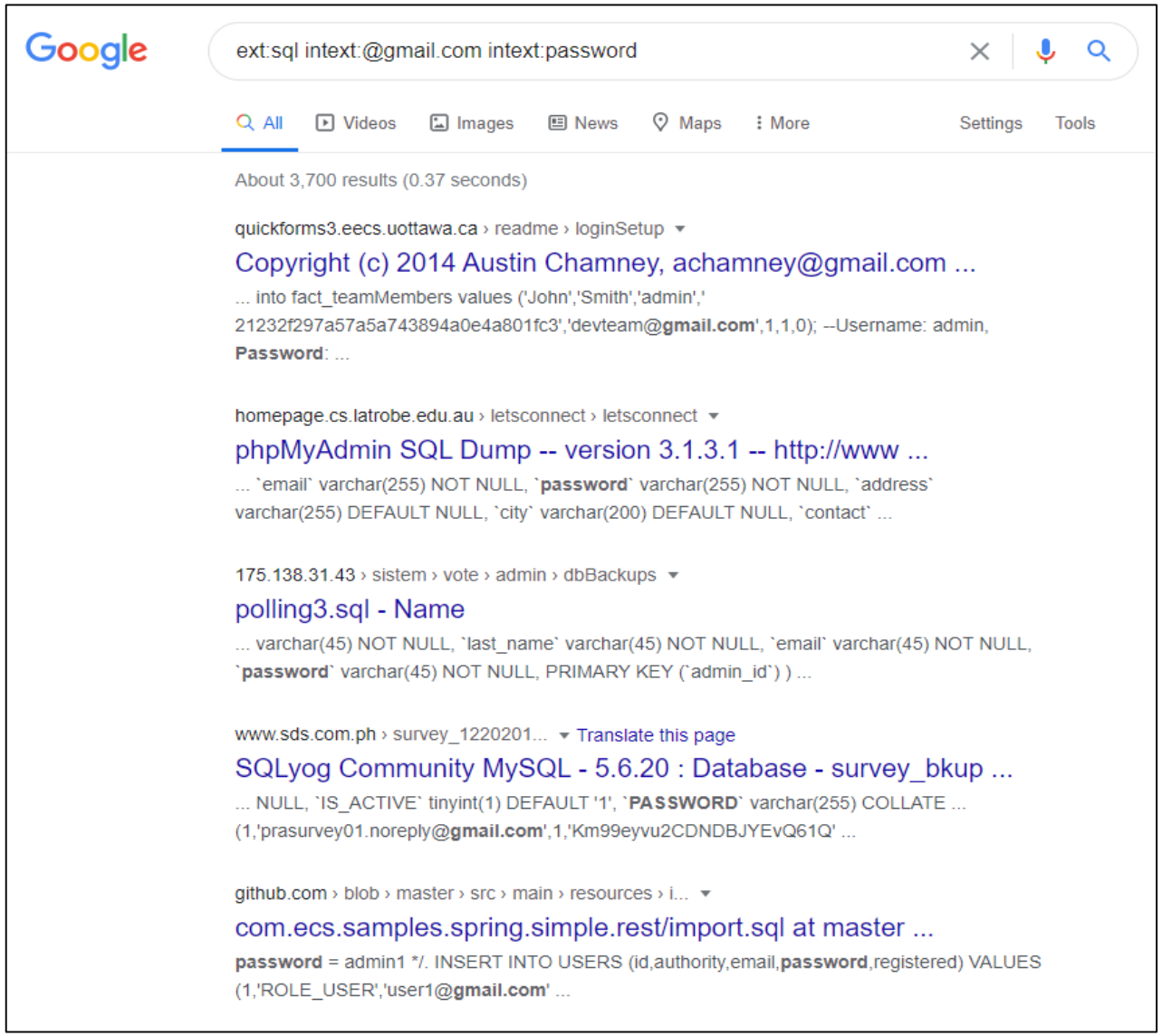
ניצול יכולות החיפוש בגוגל לצורך קבלת מידע על סיסמאות, משתמשים, חולשות וכדומה

Advanced Operator	Description	Examples
site:	Limit the search query to a specific domain or web site.	• site:example.com
filetype:	Limit the search to text found in a specific file type	• mysqldump filetype:sql
link:	Search for pages that link to the requested URL	• link:www.example.com
cache:	Search and display a version of a web page as it was shown when Google crawled it.	• cache:example.com
intitle:	Search for a string text within the title of a page.	• intitle:"index of"
inurl:	Search for a string within a URL	• inurl:passwords.txt

Logical Operator	Description	Examples
AND or +	Used to include keywords. All the keywords need to be found.	• web **AND** application **AND** security • web **+**application **+**security
NOT or –	Used to exclude keywords. All the keywords need to be found.	• web application **NOT** security • web application **–**security
OR or |	Used to include keywords where either one keyword or another is matched. All the keywords need to be found.	• web application **OR** security • web application **|**security
Tilde (~)	Used to include synonyms and similar words.	• web application ~security
Double quote (")	Used to include exact matches.	• "web application security"
Period (.)	Used to include single-character wildcards.	• .eb application security
Asterisk (*)	Used to include single-word wildcards.	• web * security
Parenthesis (())	Used to group queries	• ("web security" | websecurity)

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

דוגמא לחיפוש



ext:sql intext:@gmail.com intext:password

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

Google hacking

Advanced operator table:

Operator	Purpose	Mixes with other operators?	Can be used alone?	Does search work in			
				Web	Images	Groups	News
intitle	Search page title	yes	yes	yes	yes	yes	yes
allintitle	Search page title	no	yes	yes	yes	yes	yes
inurl	Search URL	yes	yes	yes	yes	not really	like intitle
allinurl	Search URL	no	yes	yes	yes	yes	like intitle
filetype	Search specific files	yes	no	yes	yes	no	not really
allintext	Search text of page only	not really	yes	yes	yes	yes	yes
site	Search specific site	yes	yes	yes	yes	no	not really
link	Search for links to pages	no	yes	yes	no	no	not really
inanchor	Search link anchor text	yes	yes	yes	yes	not really	yes
numrange	Locate number	yes	yes	yes	no	no	not really
daterange	Search in date range	yes	no	yes	not really	not really	not really
author	Group author search	yes	yes	no	no	yes	not really
group	Group name search	not really	yes	no	no	yes	not really
insubject	Group subject search	yes	yes	like intitle	like intitle	yes	like intitle
msgid	Group msgid search	no	yes	not really	not really	yes	not really

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

הוצאת רשימת סיסמאות

thonthao6.sextgem.com/files/superhit.txt

```
?><?php
='USER ID:rahul9267671167bimt@gmail.com';
='PASSWARD:rahulhina111';
?><?php
='USER ID:rahul9267671167bimt@gmail.com';
='PASSWARD:rahulhina111';
?><?php
='USER ID:yar yeh phisher kon kon use krha hai';
='PASSWARD:????';
?><?php
='USER ID:dvirus_ajju@yahoo.in';
='PASSWARD:';
?><?php
='USER ID:Prakashpsm@live.in';
='PASSWARD:akshaykatrina';
?><?php
='USER ID:Prakashpsm@live.in';
='PASSWARD:akshaykatrina';
?><?php
='USER ID:prakashpsm@live.in';
='PASSWARD:akshaykatrina';
?><?php
='USER ID:ashukp584@yahoo.com';
='PASSWARD:divyaps';
?><?php
='USER ID:ashukp584@yahoo.com';
='PASSWARD:divyaps';
?><?php
='USER ID:shrishesha@gmail.com';
='PASSWARD:9900878675';
?><?php
='USER ID:shrishesha@gmail.com';
='PASSWARD:9900878675';
?><?php
='USER ID:Bhinda18@yahoo.com';
='PASSWARD:';
?><?php
='USER ID:Dhiraj.suryavanshi';
='PASSWARD:585523';
?><?php
='USER ID:akibbagwan007@yahoo.com';
='PASSWARD:akibakib';
?><?php
='USER ID:akibbagwan007@yahoo.com';
='PASSWARD:786786';
?><?php
```


```
beithamaayan@walla.com  679239
hodaka1@gmail.com       1q2w3e4r
aviv_rent1@bezeqint.net 7233826
inbalims@zahav.net.il   301084
etl88@walla.co.il       340867
contact@ekdesign.co.il  123456
adi.tzachar@gmail.com   adi123456
yeudit@green1realestate.com     123456
eve@vayax.co.il e1234567
stevenalina@walla.com   eldorado
shimixxxx@walla.com     1122
shayn@nioi.gov.il       dba621
alon@ekdesign.co.il     123456
karnona@yahoo.com       23307maya
elie_asaraf@walla.co.il 1q2w3e
kifkef@kifkef.co.il     458123
coolit@inn.co.il        tamar15
yardenbp@gmail.com      tulli2000
joel70@walla.com        123456
talizh@gmail.com        tal1234
orit_nakar2003@yahoo.com        tuxyrkhv
liormaaam@walla.com     0528546365
shacharf1@bezeqint.net  ys321948
drreshef@gmail.com      a355v411
```

you are wathcing user and password

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

כלי האקינג נוספים

Minikatz – לקחת הרשאות , לבצע תנועה צידית (Lateral Movement)

MetaSploit – סט כלי תקיפה בעיקר כדי להפוך exploits למודולרים

Mac Spoofing , ARP Poisioning – Ettercap


שאלות ותשובות