

מבוא להאקינג המשך



תוכנה שיוזעת לראות מה עובר ברשת המחשבים

לדוגמא:

WIRESHARK

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.16.72.53	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
2	0.460665	10.16.72.56	10.16.72.255	BROWSERSE	243	Local Master Announcement MININT-MKLFPAF, workstation, Serve
3	0.705331	10.16.72.62	239.255.255.250	SSDP	316	NOTIFY * HTTP/1.1
4	1.617156	10.16.72.51	192.168.174.80	TCP	92	52039 → 8080 [PSH, ACK] Seq=1 Ack=1 win=259 Len=38
5	1.738020	192.168.174.80	10.16.72.51	TCP	60	8080 → 52039 [ACK] Seq=1 Ack=39 win=65535 Len=0
6	1.802184	192.168.174.80	10.16.72.51	TCP	99	8080 → 52039 [PSH, ACK] Seq=1 Ack=39 win=65535 Len=45
7	1.892110	10.16.72.51	192.168.174.80	TCP	55	52285 → 8080 [ACK] Seq=1 Ack=1 win=876 Len=1
8	1.924422	192.168.174.80	10.16.72.51	TCP	60	8080 → 52285 [ACK] Seq=1 Ack=2 win=65535 Len=0
9	2.016788	10.16.72.51	192.168.174.80	TCP	54	52039 → 8080 [ACK] Seq=39 Ack=46 win=259 Len=0
10	2.626253	fe80::113a:681:868d:ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
11	3.510107	fe80::a1f2:bbc:c693:ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
12	3.711042	10.16.72.60	239.255.255.250	SSDP	316	NOTIFY * HTTP/1.1
13	5.635465	fe80::113a:681:868d:ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
14	5.705949	10.16.72.62	239.255.255.250	SSDP	316	NOTIFY * HTTP/1.1
15	6.511100	fe80::a1f2:bbc:c693:ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
16	6.513421	fe80::a1f2:bbc:c693:ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
17	6.515640	fe80::a1f2:bbc:c693:ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
18	6.527777	10.16.72.65	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
19	7.522971	10.16.72.65	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
20	8.524076	10.16.72.65	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
21	8.667383	fe80::113a:681:868d:ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
22	8.709246	10.16.72.60	239.255.255.250	SSDP	316	NOTIFY * HTTP/1.1
23	8.733423	3comEuro_14:a1:01	Broadcast	ARP	60	Gratuitous ARP for 10.16.72.253 (Request)
24	9.510914	fe80::a1f2:bbc:c693:ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
25	9.524145	10.16.72.65	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
26	9.714521	3comEuro_14:a1:01	Broadcast	ARP	60	Gratuitous ARP for 10.16.72.253 (Request)
27	10.582723	10.16.72.64	255.255.255.255	UDP	124	64914 → 1211 Len=82
28	10.706055	10.16.72.62	239.255.255.250	SSDP	316	NOTIFY * HTTP/1.1
29	11.232417	10.16.72.51	192.168.174.80	TCP	55	52181 → 8080 [ACK] Seq=1 Ack=1 win=260 Len=1
30	11.242490	192.168.174.80	10.16.72.51	TCP	60	8080 → 52181 [ACK] Seq=1 Ack=2 win=65535 Len=0
31	12.537167	10.16.72.51	192.168.174.80	TCP	54	52332 → 80 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
32	12.552369	10.16.72.51	192.168.174.80	TCP	54	52338 → 8080 [FIN, ACK] Seq=1 Ack=1 win=258 Len=0
33	12.552587	10.16.72.51	192.168.174.80	TCP	54	52334 → 8080 [FIN, ACK] Seq=1 Ack=1 win=257 Len=0
34	12.552656	10.16.72.51	192.168.174.80	TCP	54	52333 → 80 [FIN, ACK] Seq=1 Ack=1 win=64314 Len=0
35	12.564292	192.168.174.80	10.16.72.51	TCP	60	8080 → 52338 [ACK] Seq=1 Ack=2 win=65535 Len=0
36	12.564411	192.168.174.80	10.16.72.51	TCP	60	8080 → 52338 [FIN, ACK] Seq=1 Ack=2 win=65535 Len=0
37	12.564442	10.16.72.51	192.168.174.80	TCP	54	52338 → 8080 [ACK] Seq=2 Ack=2 win=258 Len=0
38	12.565721	192.168.174.80	10.16.72.51	TCP	60	80 → 52333 [ACK] Seq=1 Ack=2 win=4312 Len=0
39	12.565839	192.168.174.80	10.16.72.51	TCP	60	8080 → 52334 [ACK] Seq=1 Ack=2 win=65535 Len=0
40	12.565864	192.168.174.80	10.16.72.51	TCP	60	80 → 52333 [FIN, ACK] Seq=1 Ack=2 win=4312 Len=0
41	12.565898	10.16.72.51	192.168.174.80	TCP	54	52333 → 80 [ACK] Seq=2 Ack=2 win=64314 Len=0
42	12.565984	192.168.174.80	10.16.72.51	TCP	60	8080 → 52334 [FIN, ACK] Seq=1 Ack=2 win=65535 Len=0
43	12.566017	10.16.72.51	192.168.174.80	TCP	54	52334 → 8080 [ACK] Seq=2 Ack=2 win=257 Len=0
44	12.636247	fe80::113a:681:868d:ff02::c		SSDP	208	M-SEARCH * HTTP/1.1



הפך בהמשך ל-KALI LINUX



כלי האקינג נוספים BACK TRACK

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

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

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

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.

Number of Characters	Complexity (96^x)	QUAD CORE		BOT NET	
		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

מכינים קובץ זאז וקוראים לו בשם : wordlist.txt
הקובץ מכיל: שורות המכילות אותיות או מספרים שעשויים 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>

דוגמאות

Secure <https://github.com/danielmiessler/SecLists/tree/master/Passwords>

danielmiessler / SecLists Watch 807 Star 6,663 Fork 2,540

Code Issues 11 Pull requests 11 Projects 0 Insights

Branch: master SecLists / Passwords / Create new file Find file History

danielmiessler committed on GitHub Merge pull request #98 from DarrenRainey/master Latest commit caa16c8 on May 12

..		
000webhost.txt	Removed duplicate values - awk 'x[\$0]+'	a year ago
10_million_password_list_top_100.txt	Removed duplicate values - awk 'x[\$0]+'	a year ago
10_million_password_list_top_1000.txt	Removed duplicate values - awk 'x[\$0]+'	a year ago
10_million_password_list_top_10000.txt	Removed duplicate values - awk 'x[\$0]+'	a year ago
10_million_password_list_top_100000.txt	Removed duplicate values - awk 'x[\$0]+'	a year ago
10_million_password_list_top_1000000.txt	Removed duplicate values - awk 'x[\$0]+'	a year ago
10_million_password_list_top_500.txt	Removed duplicate values - awk 'x[\$0]+'	a year ago
10k_most_common.txt	Add 10k most common	3 years ago
1337speak.txt	added word alpha iteration	9 months ago
500-worst-passwords.txt	Removed duplicate values - awk 'x[\$0]+'	a year ago
Ashley_Madison.txt	Removed duplicate values - awk 'x[\$0]+'	a year ago
Basic_Spanish_List.txt	Removed duplicate values - awk 'x[\$0]+'	a year ago
KeyboardCombinations.txt	Removed duplicate values - awk 'x[\$0]+'	a year ago
Lizard_Squad.txt	Lizard Squad Passwords	10 months ago
MostPopularLetterPasses.txt	Removed duplicate values - awk 'x[\$0]+'	a year ago
README	Moved withcount files, created merged list	2 years ago
SplashData-2015.txt	Added splashdata 2015 to passwords.	2 years ago
Sucuri_Top_Wordpress_Passwords.txt	Update Sucuri_Top_Wordpress_Passwords.txt	10 months ago

Branch: master SecLists / Passwords /

Go to file

History

clem9669 committed 7da5c78 26 days ago		
..		
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

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 zaq1.1o9
10 zaq1;p0
11 zaq1ZQ!
12 zaq1XW@
13 zaq1DE#
14 zaq1FR$
15 zaq1BGT%
16 zaq1NH^
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-=\
```

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

סרטון האקר בפעולת פריצת סיסמא...



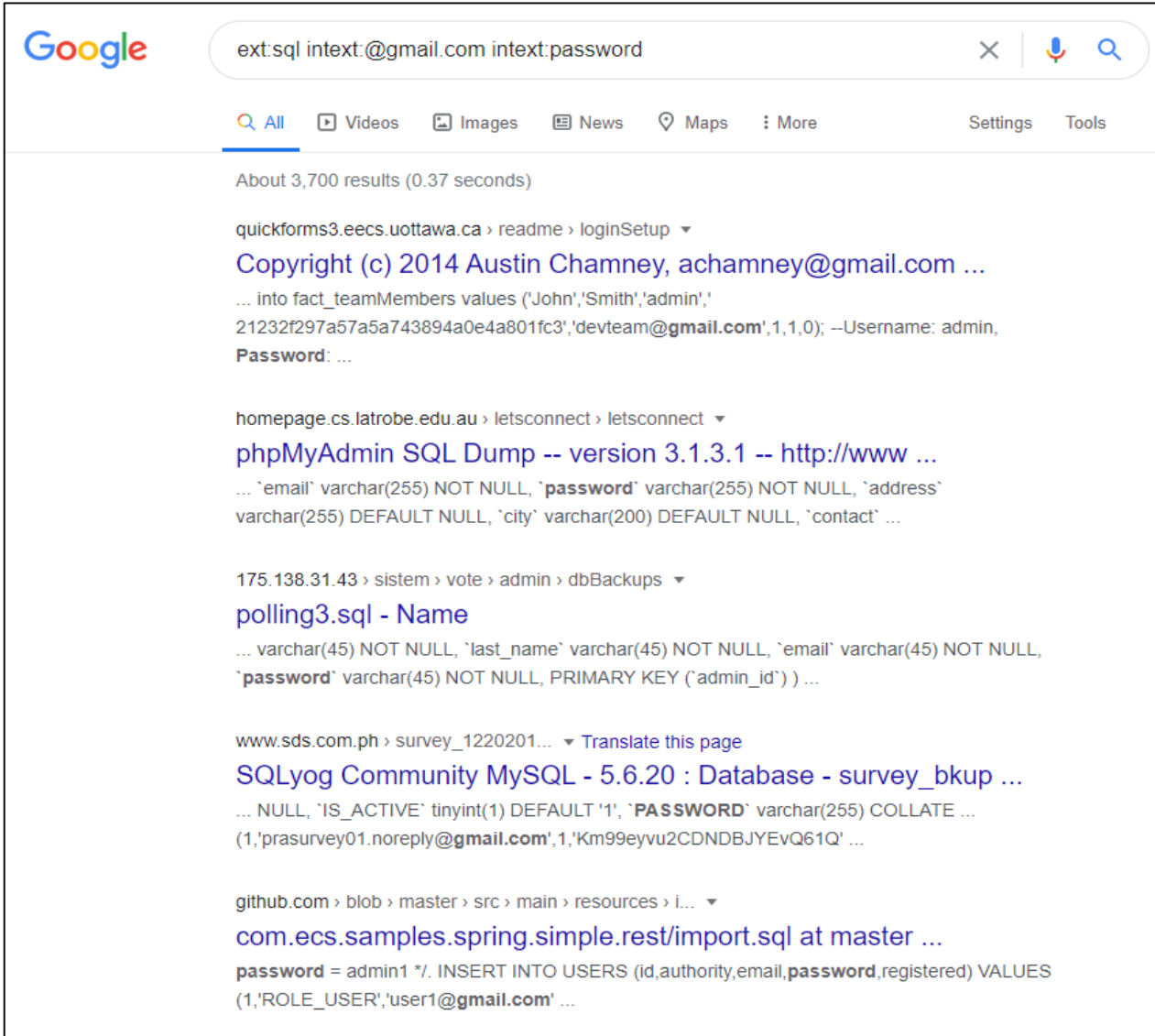
Google Hack

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.	<ul style="list-style-type: none"> site:example.com
filetype:	Limit the search to text found in a specific file type	<ul style="list-style-type: none"> mysqldump filetype:sql
link:	Search for pages that link to the requested URL	<ul style="list-style-type: none"> link:www.example.com
cache:	Search and display a version of a web page as it was shown when Google crawled it.	<ul style="list-style-type: none"> cache:example.com
intitle:	Search for a string text within the title of a page.	<ul style="list-style-type: none"> intitle:"index of"
inurl:	Search for a string within a URL	<ul style="list-style-type: none"> inurl:passwords.txt

Logical Operator	Description	Examples
AND or +	Used to include keywords. All the keywords need to be found.	<ul style="list-style-type: none"> web AND application AND security web +application +security
NOT or -	Used to exclude keywords. All the keywords need to be found.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> web application OR security web application security
Tilde (~)	Used to include synonyms and similar words.	<ul style="list-style-type: none"> web application ~security
Double quote ("")	Used to include exact matches.	<ul style="list-style-type: none"> "web application security"
Period (.)	Used to include single-character wildcards.	<ul style="list-style-type: none"> .eb application security
Asterisk (*)	Used to include single-word wildcards.	<ul style="list-style-type: none"> web * security
Parenthesis (())	Used to group queries	<ul style="list-style-type: none"> ("web security" websecurity)

דוגמא לחיפוש



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

About 3,700 results (0.37 seconds)

quickforms3.eecs.uottawa.ca > readme > loginSetup ▾
Copyright (c) 2014 Austin Chamney, achamney@gmail.com ...
... into fact_teamMembers values ('John','Smith','admin',
21232f297a57a5a743894a0e4a801fc3','devteam@gmail.com',1,1,0); --Username: admin,
Password: ...

homepage.cs.latrobe.edu.au > letsconnect > letsconnect ▾
phpMyAdmin SQL Dump -- version 3.1.3.1 -- http://www ...
... `email` varchar(255) NOT NULL, `password` varchar(255) NOT NULL, `address`
varchar(255) DEFAULT NULL, `city` varchar(200) DEFAULT NULL, `contact` ...

175.138.31.43 > sistem > vote > admin > dbBackups ▾
polling3.sql - Name
... varchar(45) NOT NULL, `last_name` varchar(45) NOT NULL, `email` varchar(45) NOT NULL,
`password` varchar(45) NOT NULL, PRIMARY KEY (`admin_id`)) ...

www.sds.com.ph > survey_1220201... ▾ Translate this page
SQLyog Community MySQL - 5.6.20 : Database - survey_bkup ...
... NULL, `IS_ACTIVE` tinyint(1) DEFAULT '1', `PASSWORD` varchar(255) COLLATE ...
(1,'prasurvey01.noreply@gmail.com',1,'Km99eyvu2CDNDBJYEvQ61Q' ...

github.com > blob > master > src > main > resources > i... ▾
com.ecs.samples.spring.simple.rest/import.sql at master ...
password = admin1 *?. INSERT INTO USERS (id,authority,email,password,registered) VALUES
(1,'ROLE_USER','user1@gmail.com' ...

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

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

הוצאת רשימת סיסמאות

```

filetype:txt username pas: X Full text of "Opisrael Of ( X www.fu
thonthao6.sextgem.com/files/superhit.txt
?><?php
='USER ID:rahul9267671167bimt@gmail.com';
='PASSWORD:rahulhina111';
?><?php
='USER ID:rahul9267671167bimt@gmail.com';
='PASSWORD:rahulhina111';
?><?php
='USER ID:yar yeh phisher kon kon use krha hai';
='PASSWORD:????';
?><?php
='USER ID:dvirus_ajju@yahoo.in';
='PASSWORD: ';
?><?php
='USER ID:Prakashpsm@live.in';
='PASSWORD:akshaykatrina';
?><?php
='USER ID:Prakashpsm@live.in';
='PASSWORD:akshaykatrina';
?><?php
='USER ID:prakashpsm@live.in';
='PASSWORD:akshaykatrina';
?><?php
='USER ID:ashukp584@yahoo.com';
='PASSWORD:divyaps';
?><?php
='USER ID:ashukp584@yahoo.com';
='PASSWORD:divyaps';
?><?php
='USER ID:shrishsha@gmail.com';
='PASSWORD:9900878675';
?><?php
='USER ID:shrishsha@gmail.com';
='PASSWORD:9900878675';
?><?php
='USER ID:8hinda18@yahoo.com';
='PASSWORD: ';
?><?php
='USER ID:Dhiraj.suryavanshi';
='PASSWORD:585523';
?><?php
='USER ID:akibbagwan007@yahoo.com';
='PASSWORD:akibakib';
?><?php
='USER ID:akibbagwan007@yahoo.com';
='PASSWORD:786786';
?><?php

```



```

beithamaayan@walla.com 679239
hodakai@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
shimixxx@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 tull12000
joel70@walla.com 123456
talizh@gmail.com tal1234
orit_nakar2003@yahoo.com tuxyrkhv
liormaaam@walla.com 0528546365
shacharf1@bezeqint.net ys321948
dreshef@gmail.com a355v411

```

you are wathing user and password

כלי האקינג נוספים



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



MetaSploit – סט כלי תקיפה בעיקר כדי להפוך exploits למודולרים



Mac Spoofing , ARP Poisoning – Ettercap

