

Cybersecurity

Password Cracking Tools



Password Crackers



- Passwords are stored as hashes
- Grab copy of the hashes, crack offline
- Use known, common passwords from a wordlist
- Use rainbow tables
 - Pre-calculated hashes, based on system (SQL, Linux, Windows)
 - Password salting can combat rainbow tables
- Security professionals audit user passwords using same tools as hackers would
 - Find and fix problem before it can be exploited



Example - JtR

- John the Ripper
- Multiple step process
 - Rules, Dictionary, and Brute Force

```
student@kali:~/Desktop$ john passwords
Created directory: /home/student/.john
Warning: detected hash type "sha512crypt", but the string is also recognized as "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2
4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
student      (student)
melissa2     (melissa)
Warning: Only 6 candidates buffered for the current salt, minimum 8 needed for performance.
Further messages of this type will be suppressed.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
123456      (james)
starwars   (colby)
harrypotter (emma)
!@#$$%^   (maddie)
6g 0:00:00:26 23.01% 2/3 (ETA: 09:00:08) 0.2306g/s 1990p/s 2256c/s 2256C/s matthew7..apples7
```



Using JtR to audit passwords

Example - Hash Suite

- Runs on Windows and Android OS
- Different processes allowed

The screenshot displays the Hash Suite 3.7 [64 Bits] [Pro] interface. The main window is titled "Hash Suite 3.7 [64 Bits] [Pro]" and features a menu bar with "Main", "View", "Params", "Hardware", "Reports", "Downloader", and "Rules". Below the menu bar, there are control buttons for "Start", "Stop", and "Resume", along with a "Format" button and a "Key Providers" section. The "Attack Status" section shows "Rate: 16.9G", "Time: 00:00:44", "Keys Tested: [empty]", "Load: 739", "End In: 00:00:00", "Key Space: [empty]", "Done: 100%", "All Time: 00:00:44", and "Last Save: [empty]".

The main display area is a table with columns for "Key Provider Params", "Username", "Hash", and "Cleartext". The table shows the following data:

Key Provider Params	Username	Hash	Cleartext
<input checked="" type="checkbox"/> Charset Params	hcookis	F83C01861FDD23B4354465FE6D7F6402	nurse
Minimum Size 0	emcnees	C1A8D439E09068BF241EBBC04BDB424C	????????????????????
Maximum Size 6	hpasceri	486EA753DEF361967B1A5E9C5D65EC18	????????????????????
<input type="checkbox"/> Use rules	ddauria	34643FD04B90614EF2E9A3E1DB738986	????????????????????
Add new char...	ncuellar	34643FD04B90614EF2E9A3E1DB738986	????????????????????
<input checked="" type="checkbox"/> Lower abcdefghijklmno...	Irothman	85ECE392A6A543E03B0117632CCA706C	????????????????????
<input checked="" type="checkbox"/> Upper ABCDEFGHIJKLM...	mplance	D9D0062E7F69FBC862E1109F034047F	????????????????????
<input checked="" type="checkbox"/> Digit 0123456789	aliao	475BD57348733E0CC223F97FCE352F30	????????????????????
<input checked="" type="checkbox"/> Symbol !@#\$%^&*()-_+...	glibby	F349E6F99BA4795044AF1143A7167909	velvet
<input type="checkbox"/> Wordlist Params	sganji	7902E9B7EEF97019E29CD1979C007BC5	2000
<input type="checkbox"/> Keyboard Params	hmarmon	494877A3209B0EF206A36248E245F2A2	james
<input type="checkbox"/> Phrases Params	jdashno	494877A3209B0EF206A36248E245F2A2	james
	ilanni	1C6C3C6BAEF048DBF0C8C5646AC684B7	????????????????????
	iellingboe	EE62EC5FDB60604066CAEFA22EB35483	lizard

Screenshot of password auditing with Hash Suite



Example - ncrack

- Attempts to crack network authentications
 - Typically, not used with captured hashes

```
student@kali:~/Desktop$ ncrack -v 10.1.57.54 --user student -P dictionary -p rdp CL=1

Starting Ncrack 0.7 ( http://ncrack.org ) at 2021-03-27 09:06 UTC

Failed to resolve given hostname/IP: CL=1. Note that you can't use '/mask' AND '1-4,7,100-'
e IP ranges
Discovered credentials on rdp://10.1.57.54:3389 'student' 'student'
rdp://10.1.57.54:3389 finished.

Discovered credentials for rdp on 10.1.57.54 3389/tcp:
10.1.57.54 3389/tcp rdp: 'student' 'student'

Ncrack done: 1 service scanned in 6.00 seconds.
Probes sent: 29 | timed-out: 19 | prematurely-closed: 0

Ncrack finished.
student@kali:~/Desktop$
```

Screenshot of password auditing a remote desktop system using ncrack



Example - medusa

- Attempts to crack network authentications
 - Typically, not used with captured hashes

```
student@kali:~/Desktop$ medusa -h 10.1.93.4 -u frank -P dictionary -M ftp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 10.1.93.4 (1 of 1, 0 complete) User: frank (1 of 1, 0 complete) Password: 1 (1 of 6 complete)
ACCOUNT CHECK: [ftp] Host: 10.1.93.4 (1 of 1, 0 complete) User: frank (1 of 1, 0 complete) Password: 12 (2 of 6 complete)
ACCOUNT CHECK: [ftp] Host: 10.1.93.4 (1 of 1, 0 complete) User: frank (1 of 1, 0 complete) Password: 123 (3 of 6 complete)
ACCOUNT CHECK: [ftp] Host: 10.1.93.4 (1 of 1, 0 complete) User: frank (1 of 1, 0 complete) Password: 1234 (4 of 6 complete)
ACCOUNT CHECK: [ftp] Host: 10.1.93.4 (1 of 1, 0 complete) User: frank (1 of 1, 0 complete) Password: 12345 (5 of 6 complete)
ACCOUNT FOUND: [ftp] Host: 10.1.93.4 User: frank Password: 12345 [SUCCESS]
student@kali:~/Desktop$
```

Screenshot of password auditing a remote ftp server using medusa

