Password Cracking tools

Sadhasivasubramanian H

IITM PRAVARTAK CATALYSING INNOVATION

Overview of Popular Password Cracking Tools

- **Hashcat:** A high-performance, GPU-accelerated tool known for speed and versatility. Supports various attack modes like brute-force, dictionary, and hybrid attacks. Widely used for large-scale password cracking.
- **John the Ripper :** A flexible, open-source tool designed for both Unix and Windows password cracking. Effective for smaller, targeted cracking jobs and supports various attack modes, including wordlist and incremental.
- **Aircrack-ng:** Specialized in cracking Wi-Fi passwords (WEP, WPA, WPA2). It uses techniques like brute-force and dictionary attacks to test wireless network security.
- **Medusa:** A parallel, brute-force password cracking tool that focuses on network services. Supports multiple protocols like SSH, FTP, HTTP, and SMB. Medusa is fast and scalable, making it ideal for cracking passwords on remote systems.

IITM PRAVARTAK
CATALYSING INNOVATION

Hashcat

What is Hashcat?

- **Hashcat:**
  - A high-performance, open-source password recovery tool.
- **Purpose:**
  - Used to recover passwords by cracking password hashes.
- **Key Feature:**
  - GPU-accelerated, making it one of the fastest tools available.
- **Supports:**
  - A wide variety of hashing algorithms (MD5, SHA-256, WPA, etc.).

Hashcat Attack Modes

Brute-force Attack (-a 3):

- Tries every possible character combination.
- Time-consuming but effective.

Dictionary Attack (-a 0):

- Uses predefined wordlists to attempt password matches.
- Fast but limited by the wordlist quality.

Combination Attack (-a 1):

- Combines two wordlists, useful for longer, compound passwords.

Mask Attack (-a 3):

- Targets specific patterns based on partial knowledge of the password (e.g., known characters, length).

Hybrid Attack (-a 6, -a 7):

- Combines dictionary and mask-based attacks.

Popular Hash Types Supported

- MD5 (-m 0)
- SHA-1 (-m 100)
- SHA-256 (-m 1400)
- NTLM (-m 1000)
- bcrypt (-m 3200)
- WPA/WPA2 (-m 2500)

IITM PRAVARTAK CATALYSING INNOVATION

Dictionary Attack Mode (-a 0): (Demo)

```
┌──(sadha㉿sadha)-[~/workshop]
└─$ hashcat -a 0 -m 0 --session work target_hashes_md5.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEF,
=============================================================================================
* Device #1: cpu--0x000, 1437/2939 MB (512 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 10 digests; 10 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

5d41402abc4b2a76b9719d911017c592:hello
42f749ade7f9e195bf475f37a44cafcb:Password123
75b71aa6842e450f12aca00fdf54c51d:P455w0rd
2c9341ca4cf3d87b9e4eb905d6a3ec45:Test1234
958152288f2d2303ae045cffc43a02cd:MYSECRET
66747fe723d6a91fbfc953ac4494a465:A1B1C1D1E1
Approaching final keyspace - workload adjusted.
```

```
Session..........: work
Status...........: Exhausted
Hash.Mode........: 0 (MD5)
Hash.Target......: target_hashes_md5.txt
Time.Started.....: Sun Sep 15 17:26:36 2024 (2 secs)
Time.Estimated...: Sun Sep 15 17:26:38 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  6441.0 kH/s (0.05ms) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered........: 6/10 (60.00%) Digests (total), 6/10 (60.00%) Digests (new)
Progress.........: 14344385/14344385 (100.00%)
Rejected.........: 0/14344385 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[206b72697374656e616e6e65] → $HEX[042a0337c2a156616d6f7
Hardware.Mon.#1..: Util: 40%

Started: Sun Sep 15 17:26:36 2024
Stopped: Sun Sep 15 17:26:40 2024

┌──(sadha㉿sadha)-[~/workshop]
└─$
```

IITM PRAVARTAK CATALYSING INNOVATION

Combination Attack Mode (-a 1): Demo

```
┌──(sadha㉿sadha)-[~/workshop]
└─$ hashcat -a 1 -m 0 --session work target_hashes_md5.txt /usr/share/wordlists/rockyou.txt worklist2.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEF, POCL_DEBUG)
==========================================================================================================
* Device #1: cpu--0x000, 1437/2939 MB (512 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

Dictionary cache built:
* Filename..: worklist2.txt
* Passwords.: 4
* Bytes.....: 20
* Keyspace..: 4
* Runtime...: 0 secs

Hashes: 10 digests; 10 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash
```

```
fb9aab0c4314447b2263fd841acf9cdf:MYSECRET1234
e05dad5279e5eaeab3563b11edd8663a:Guess1234
Approaching final keyspace - workload adjusted.


Session..........: work
Status...........: Exhausted
Hash.Mode........: 0 (MD5)
Hash.Target......: target_hashes_md5.txt
Time.Started.....: Sun Sep 15 17:29:32 2024 (3 secs)
Time.Estimated...: Sun Sep 15 17:29:35 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt), Left Side
Guess.Mod........: File (worklist2.txt), Right Side
Speed.#1.........: 14803.4 kH/s (0.15ms) @ Accel:256 Loops:4 Thr:1 Vec:4
Recovered........: 8/10 (80.00%) Digests (total), 2/10 (20.00%) Digests (new)
Progress.........: 57377540/57377540 (100.00%)
Rejected.........: 0/57377540 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-4 Iteration:0-4
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[206b72697374656e616e6e6531323334] → $HEX[042a0337c2a156
Hardware.Mon.#1..: Util: 49%

Started: Sun Sep 15 17:29:31 2024
Stopped: Sun Sep 15 17:29:37 2024
```

Mask attack Mode (-a 3): Demo

```
┌──(sadha㉿sadha)-[~/workshop]
└─$ hashcat -a 3 -m 0 --session work target_hashes_md5.txt Guess?u?l
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPI
=============================================================================
* Device #1: cpu--0x000, 1437/2939 MB (512 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 10 digests; 10 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 r

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Brute-Force
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce perfor
If you want to switch to optimized kernels, append -O to your commandli
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your devi
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

031cbcccd3ba6bd4d1556330995b8d08:GuessMe
```

John the Ripper

What is John the Ripper?

- John the Ripper is a popular open-source password cracking tool.
  - Initially developed for Unix-based systems.
  - Designed to detect weak passwords and crack password hashes.
  - Supports many operating systems, including Unix, Windows, and macOS.
- Hash Support: Cracks multiple hash types, including:
  - Unix-based hashes (DES, MD5)
  - Windows LM/NTLM
  - SHA hashes, bcrypt, and more.
- Customizable: Supports plugins and extensions to add more functionality.

Attack Modes in John the Ripper

Single Crack Mode:

- Uses username and other information to guess passwords.
- Default mode and often the fastest.

Wordlist Mode:

- Uses a wordlist (dictionary) to crack passwords.
- Can be combined with rules to modify wordlist entries (e.g., adding numbers or symbols).

Incremental Mode:

- Performs a brute-force attack by trying all character combinations.
- Time-consuming but effective for short passwords.

External Mode:

- Allows users to create custom attack modes using external scripts.
- Highly flexible and customizable for unique cracking strategies.

Single crack mode: (demo)

```
┌──(sadha㉿sadha)-[~/workshop]
└─$ john --format=raw-md5 target_hashes_md5.txt
Using default input encoding: UTF-8
Loaded 10 password hashes with no different salts (Raw-MD5 [MD5 128/128 ASIMD 4×2])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
hello            (?)
Proceeding with incremental:ASCII
1g 0:00:00:31  3/3 0.03225g/s 37450Kp/s 37450Kc/s 337054KC/s 26431622..26434rfu
1g 0:00:00:36  3/3 0.02777g/s 37598Kp/s 37598Kc/s 338389KC/s czrxiv..czupcc
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session aborted
```

Wordlist Mode: (demo)

```
┌──(sadha㉿sadha)-[~/workshop]
└─$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt target_hashes_md5.txt
Using default input encoding: UTF-8
Loaded 10 password hashes with no different salts (Raw-MD5 [MD5 128/128 ASIMD 4×2])
Remaining 9 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
Password123      (?)
P455w0rd         (?)
Test1234         (?)
MYSECRET         (?)
A1B1C1D1E1       (?)
5g 0:00:00:00 DONE (2024-09-15 18:00) 8.474g/s 24310Kp/s 24310Kc/s 123332KC/s """anokax"..*7¡Vamos!
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Zip password cracking: (demo)

```
┌──(sadha㉿sadha)-[~/workshop]
└─$ zip2john Secret.zip > zip.hashes

┌──(sadha㉿sadha)-[~/workshop]
└─$ john zip.hashes
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 ASIMD 4x])
Cost 1 (HMAC size) is 17 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Topgun           (Secret.zip/worklist2.txt)
1g 0:00:00:00 DONE 2/3 (2024-09-15 18:10) 1.030g/s 48418p/s 48418c/s 48418C
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

IITM PRAVARTAK CATALYSING INNOVATION

Linux password: (demo)

```
┌──(sadha㉿sadha)-[~/.john]
└─$ sudo unshadow /etc/passwd /etc/shadow > linux_password.txt

┌──(sadha㉿sadha)-[~/.john]
└─$ john --format=crypt linux_password.txt
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt])
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
sadha            (sadha)
1g 0:00:00:00 DONE 1/3 (2024-09-15 18:17) 5.555g/s 533.3p/s 533.3c/s 533.3C/s sadha..hasa
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```


Thanks