

Homework

Complete these tasks before Lesson 02. They reinforce the concepts from this lesson and prepare you for the next one.

Task 1: Research Hash Types

Goal: Familiarize yourself with the variety of hash types Hashcat supports.

Instructions

Using the `hashcat --help` output or the [Hashcat Example Hashes](#) page, research and document 5 different hash types.

For each hash type, record:

1. The hash type name (e.g., "MD5")
2. The `-m` mode number (e.g., `0`)
3. A brief description of where this hash type is commonly used
4. An example hash from the Hashcat example hashes page

Deliverable

A table in this format:

Hash Type	Mode (-m)	Common Use	Example Hash
MD5	0	Legacy web apps, checksums	8743b52063cd8409...
...	...	...	...

Self-check

- ✓ You have 5 distinct hash types in your table.
- ✓ Each entry includes all four requested fields.

- ✓ At least one hash type is something other than MD5, SHA-1, or SHA-256 (explore less common types).

Task 2: Dictionary vs. Mask Attacks

Goal: Understand the conceptual difference between the two most common attack types.

Instructions

Write a short explanation (150–250 words) comparing dictionary attacks and mask attacks. Your explanation should address:

1. **How each attack works** — what input does each require, and how does it generate password candidates?
2. **Strengths** — when is each attack type most effective?
3. **Weaknesses** — when does each attack type fail or become impractical?
4. **A practical example** — describe a scenario where you would choose one over the other, and explain why.

Self-check

- ✓ Your explanation is 150–250 words.
- ✓ You describe both attacks, not just one.
- ✓ You include a concrete scenario with a clear justification for your choice.
- ✓ A classmate who missed this lesson could understand your explanation.

Task 3: Create and Crack Your Own Hash

Goal: Practice the full workflow of creating a hash, building a wordlist, and running Hashcat.

Instructions

1. Choose a simple password (e.g., "sunshine", "iloveyou", "football").
2. Generate the MD5 hash of your chosen password. You can use any of these methods:

```
# macOS / Linux
echo -n "yourpassword" | md5sum

# macOS alternative
echo -n "yourpassword" | md5

# Python
python3 -c "import hashlib; print(hashlib.md5(b'yourpassword').hexdigest())"
```

3. Save the hash to a new file (e.g., `myhash.txt`).
4. Create a custom wordlist file (at least 20 words) that includes your chosen password somewhere in the list.
5. Run Hashcat to crack your hash using your custom wordlist.
6. Verify the result.

Hint

Make sure to use `echo -n` (no newline) when generating the hash. Without the `-n` flag, `echo` adds a trailing newline character, which changes the hash entirely.

Deliverable

A short write-up that includes:

- The password you chose
- The MD5 hash you generated
- The Hashcat command you ran
- The contents of your output file confirming the crack

Self-check

- ✓ You generated the hash yourself (not copied from this guide).
- ✓ Your custom wordlist has at least 20 entries.
- ✓ Hashcat successfully cracked the hash.
- ✓ The output file shows the correct `hash:password` pair.

Submission

There is no formal submission for this course. These tasks are for your own development. However:

- Keep your homework answers — you will refer back to them in later lessons.
- If you are working through this course with a group or mentor, share your Task 2 explanation for discussion.
- Ensure Task 3 is complete before Lesson 02, as the next lesson builds on these skills.

*Next lesson: **Lesson 02 — Installation & Setup** — detailed platform-specific installation, driver configuration, and performance benchmarking.*