

Homework

Practice tasks to solidify your understanding of hashcat command structure — to be completed before Lesson 04.

Submission: Document your commands, outputs, and answers in a text file or markdown document. Be ready to discuss your findings during the next class.

Task 1 — Command Construction

What to do

For each of the following scenarios, write the complete hashcat command you would use. Do not run them yet — just write the commands.

Scenarios

1. **MD5 dictionary attack** — Crack MD5 hashes in `dump.txt` using `rockyou.txt`. Save results to `cracked.txt` in hash:password format.
2. **NTLM with rules** — Crack NTLM hashes in `ad_hashes.txt` using `rockyou.txt` with the `best64.rule` rule file. Save only the plaintext passwords to `passwords.txt`.
3. **SHA-512 mask attack** — Crack SHA-512 (Unix) hashes in `shadow.txt` using a mask attack with all lowercase characters, trying lengths 5 through 10. Use high workload on GPU only.
4. **Hybrid attack** — Crack MD5 hashes in `web_hashes.txt` using a hybrid dictionary+mask attack. Use `common_words.txt` as the wordlist and append 4 digits to each word. Name the session `web_audit`.
5. **Combinator attack** — Crack NTLM hashes in `corp_hashes.txt` by combining words from `first_names.txt` and `years.txt`. Output hash:password pairs to `combined_results.txt`.

Requirements

- Each command must be syntactically correct (runnable without errors)
- Include all necessary flags for the scenario described
- Use the correct `-m` and `-a` values for each scenario

Self-check: For each command, verify: correct hash mode? Correct attack mode? Arguments in the right order? Output format specified where needed?

Task 2 — Parameter Exploration

What to do

Run `hashcat --help` and answer the following questions. Include the relevant flag or value in your answer.

Questions

1. What is the hash mode number for **bcrypt**?
2. What flag would you use to set the **maximum number of threads** on the CPU?
3. What does the `--force` flag do, and why is it generally discouraged?
4. What is the difference between `--outfile-format 3` and `--outfile-format 5`?
5. What flag shows you all detected **backend devices** (GPUs, CPUs) and their capabilities?
6. How do you tell hashcat to **skip** the first N words in a wordlist, and how do you **limit** it to process only N words?
7. What is the flag for running hashcat in **benchmark mode**?

Self-check: Each answer should reference a specific flag (e.g., `-b`, `--skip`, etc.) found in the `--help` output.

Task 3 — Keyspace Calculation

What to do

Calculate the total keyspace (number of candidate passwords) for each of the following mask configurations. Show your math.

Masks

1. `?d?d?d?d` — 4 digits
2. `?l?l?l?l?l?l` — 6 lowercase letters
3. `?u?l?l?l?l?d?d` — uppercase + 4 lowercase + 2 digits
4. `?a?a?a?a?a?a?a` — 8 printable characters
5. `?d?d?d?d?d?d` with `--increment --increment-min 4 --increment-max 6` — digits, lengths 4 through 6

Reference

- `?d` = 10 characters (0–9)
- `?l` = 26 characters (a–z)
- `?u` = 26 characters (A–Z)
- `?s` = 33 characters (special)
- `?a` = 95 characters (all printable)

Self-check: Verify your answers using `hashcat -m 0 -a 3 --keyspace [mask]`.
The `--keyspace` flag prints the total candidate count without cracking.

Task 4 — Error Diagnosis

What to do

Each of the following commands has an error. Identify the mistake and write the corrected command.

Broken commands

```
# Command A: Dictionary attack on NTLM hashes
hashcat -m 0 -a 0 -o results.txt ntlm_hashes.txt rockyou.txt
```

```
# Command B: Mask attack missing the mask argument
hashcat -m 1000 -a 3 -o results.txt hashes.txt

# Command C: Hybrid attack with wrong argument order
hashcat -m 0 -a 6 -o results.txt hashes.txt ?d?d rockyou.txt

# Command D: Incremental mode without a mask long enough
hashcat -m 0 -a 3 -i --increment-min 4 --increment-max 8 hashes.txt ?a?a?

# Command E: Restoring a session that was never named
hashcat --restore
```

For each command

1. Explain what is wrong
2. Write the corrected version
3. Explain why the fix works

Self-check: Test your corrected commands against test hashes (using the setup from the lab) to verify they work.

Grading Criteria

Task	Points	Key Criterion
Task 1 — Command Construction	25	All 5 commands are syntactically correct with proper flags
Task 2 — Parameter Exploration	25	All 7 questions answered with specific flag references
Task 3 — Keyspace Calculation	25	Correct math shown; answers verified with --keyspace

Task	Points	Key Criterion
Task 4 — Error Diagnosis	25	All 5 errors identified with corrected commands and explanations