

Homework

Complete these tasks after the lab. Focus on critical thinking and real-world application of ethical principles. Written tasks should be clear and well-structured.

Task 1: Legal Research Report

Goal: Understand the legal landscape governing password recovery tools in your jurisdiction.

Instructions

1. Research the laws in your country (or a country of your choice) that regulate the use of password cracking tools. Consider:
 - Computer fraud and abuse laws (e.g., CFAA in the US, Computer Misuse Act in the UK)
 - Data protection regulations (e.g., GDPR in the EU)
 - Penetration testing exemptions or safe harbours
2. Write a 300–500 word summary covering:
 - Which specific laws apply to password recovery tools?
 - Under what conditions is their use legal?
 - What are the penalties for unauthorized use?
 - Are there any safe harbour provisions for security researchers?

✓ **Self-check: Your report cites at least 2 specific laws or regulations by name and explains how they apply to Hashcat usage.**

Task 2: Ethical Dilemma Analysis

Goal: Practice ethical reasoning in realistic cybersecurity scenarios.

Instructions

For each of the following scenarios, write 100–150 words explaining: (a) what ethical principles are at stake, (b) what you would do, and (c) why.

1. **Scenario A:** Your manager asks you to crack password hashes from a competitor's leaked database "to check if any of our employees reused passwords." You have no written authorization from the employees or the competitor.
2. **Scenario B:** During an authorized penetration test, you recover the CEO's password and discover it is used across multiple personal accounts (you can tell from the password pattern). The scope of the engagement only covers corporate systems.
3. **Scenario C:** A colleague shares a list of "practice hashes" for a training exercise. You suspect some of them may be real production hashes from a client system, not synthetic test data.

✓ **Self-check: Each response explicitly names the ethical principles involved (legality, consent, confidentiality, responsibility, or transparency) and provides a clear course of action.**

Task 3: Organizational Security Policy

Goal: Create a professional-quality policy document for ethical use of password auditing tools.

Instructions

Write a 1–2 page "Acceptable Use Policy for Password Auditing Tools" suitable for a fictional organization. Your policy must include:

1. **Purpose & Scope:** What the policy covers and why it exists
2. **Authorization Requirements:** Who can approve password auditing, what documentation is required
3. **Consent & Notification:** How affected parties are informed
4. **Data Handling:** How recovered passwords and hash files must be stored, encrypted, and destroyed
5. **Approved Tools & Methods:** Which tools are permitted, what attack types are allowed

- 6. **Reporting:** What must be documented and reported after an audit
- 7. **Violations & Consequences:** What happens if the policy is breached
- 8. **Review Schedule:** How often the policy is reviewed and updated

✓ **Self-check:** Your policy covers all 8 sections listed above and could realistically be adopted by a small to mid-size company.

Grading Criteria

Criterion	Weight	Description
Legal accuracy	25%	Correct identification and explanation of relevant laws
Ethical reasoning	25%	Clear application of ethical principles to scenarios
Policy completeness	30%	All required sections present with actionable content
Writing quality	20%	Clear, professional, well-organized writing