

Lab Guide

Time estimate: 60–90 minutes · Format: Discussion, policy writing, and report ·

Prerequisites: Review the Theory page before starting

Lab Overview

In this lab, you will study ethical principles, discuss real-world dilemmas, and develop a formal ethical use policy for Hashcat within your organization or team. This is a writing and analysis exercise — no password cracking is involved.

Note: This lab is best completed in a group setting to encourage discussion. If working alone, write your responses as if presenting to a team and consider multiple perspectives for each dilemma.

Part 1: Study Ethical Principles (15 minutes)

Task 1.1: Principle Review

Goal: Internalize the five ethical principles and understand how they apply to password recovery.

Instructions

1. Read through the five ethical principles in the Theory page: **Legality, Consent, Confidentiality, Responsibility, Transparency**.
2. For each principle, write one sentence explaining why it matters specifically for Hashcat usage (not just security in general).
3. Rank the five principles in order of importance from your perspective. Be prepared to defend your ranking.

Checkpoint: You should have 5 principle descriptions and a ranked list with justification.

Part 2: Discuss Ethical Dilemmas (20 minutes)

Task 2.1: Scenario Analysis

Goal: Develop ethical judgment by analyzing realistic scenarios.

Instructions

For each scenario below, write a response that addresses: (a) What should you do? (b) Which ethical principle(s) apply? (c) What are the consequences of getting it wrong?

Scenario A: The Overeager Manager

Your manager asks you to run Hashcat against the company's Active Directory password hashes to "see how strong they are." They say verbal approval from the CTO is sufficient. No written authorization exists, and no scope has been defined.

Scenario B: The Curious Colleague

A colleague sees you running Hashcat during an authorized engagement and asks if you can "quickly check" if their ex-partner's password appears in a leaked database they found online.

Scenario C: The Time Pressure

You are conducting an authorized password audit. With one day left in the engagement window, you have only cracked 40% of the hashes. The client asks you to extend testing by a week. The original authorization document specifies the end date as tomorrow.

Scenario D: The Unexpected Discovery

During an authorized password audit of employee accounts, you crack the password of an account that appears to be a backdoor — it does not correspond to any known employee and has elevated privileges.

Task 2.2: Create Your Own Dilemma

Goal: Deepen understanding by creating a novel ethical scenario.

Instructions

1. Write a realistic ethical dilemma related to Hashcat usage that is not covered by the scenarios above.
2. Identify which ethical principles it tests.
3. Write a recommended course of action.

Checkpoint: You should have analysis of all 4 scenarios plus 1 original dilemma.

Part 3: Develop an Ethical Use Policy (30–40 minutes)

Tip: Think of this policy as a real document that your team would actually use. Be specific enough to be actionable, but general enough to cover the range of engagements your team handles.

Task 3.1: Define Policy Goals

Goal: Establish what your policy aims to achieve.

Instructions

1. Write 3–5 specific goals for your ethical use policy. Examples:
 - Ensure all Hashcat usage complies with applicable laws
 - Protect the confidentiality of recovered passwords
 - Establish clear accountability for all testing activities

2. Define the audience: Who will read and follow this policy?
3. Define the scope: What tools, activities, and environments does this policy cover?

Task 3.2: Write the Policy

Goal: Create a complete, actionable ethical use policy for Hashcat.

Required Structure

Your policy must include the following eight sections:

#	Section	Minimum Content
1	Introduction	Purpose statement, scope, definitions of key terms
2	Legality	Applicable laws, compliance requirements, legal review process
3	Consent	Authorization requirements, consent template, approval workflow
4	Confidentiality	Data classification, encryption standards, access controls, destruction procedures
5	Responsibility	Roles and responsibilities, competency requirements, code of conduct
6	Transparency	Reporting requirements, communication channels, disclosure standards
7	Control & Monitoring	Activity logging, audit procedures, violation handling, incident response
8	Conclusion	Acknowledgment requirement, review schedule, version control

Writing Guidelines

- Each section should be 100–200 words

- Use clear, direct language — avoid jargon where possible
- Include specific, measurable requirements (e.g., "AES-256 encryption" not just "strong encryption")
- Reference applicable frameworks (PTES, OWASP, NIST) where relevant

Checkpoint: Your policy should be approximately 1,000–1,500 words across all 8 sections.

Task 3.3: Review and Approve

Goal: Simulate the review and approval process for a real policy.

Instructions

1. **Self-review:** Read your policy from the perspective of a new team member. Is everything clear? Are there gaps?
2. **Peer review (if working in a group):** Exchange policies with another participant. Provide written feedback on:
 - Clarity and completeness of each section
 - Specific, actionable requirements vs. vague statements
 - Missing scenarios or edge cases
 - Compliance with the five ethical principles
3. **Revision:** Incorporate feedback and produce a final version.
4. **Sign-off:** Add a version number, date, and author name to the final document.

Part 4: Write a Report (10–15 minutes)

Task 4.1: Lab Report

Goal: Summarize your work and reflect on what you learned.

Report Structure

1. **Executive Summary** (2–3 sentences) — What did you create and why?

2. **Dilemma Analysis Summary** — Key insights from the ethical dilemma discussions
3. **Policy Overview** — Brief summary of each section of your ethical use policy
4. **Lessons Learned** — What surprised you? What was hardest to write? What would you change in a real-world policy?
5. **Framework Alignment** — Which penetration testing framework (PTES, OWASP, NIST) best aligns with your policy, and why?

Checkpoint: Your report should be 300–500 words.

Deliverables Checklist

Before you finish, verify you have completed:

- Principle review with descriptions and ranking (Part 1)
- Analysis of 4 ethical dilemmas + 1 original dilemma (Part 2)
- Complete ethical use policy with all 8 sections (Part 3)
- Peer review feedback (if applicable) (Part 3)
- Lab report with all 5 sections (Part 4)