Users and Access Control

Study Guide

This is a skill-building guide. Its purpose is to train you to produce, test, and revise precise access-control claims until they are reviewable by someone else. You are expected to write concrete statements, test them against reality, and correct only what fails.

What You Must Remember

The Access Model

User + Group Membership + Permission Scope → Allowed Actions

If you can reliably translate permissions into sentences about identities and actions, you can reason about access control without guessing.

What Each Word Means

Component	Meaning
User	A named identity that the system uses to decide authority. Processes run as a user.
Group	A named set of users. Group membership is how access spreads.
Permission	Recorded rules for read, write, and execute applied to owner, group, and others.
Ownership	Which user and group does a file or directory belong to?

If you forget everything else, permissions are the system's recorded trust decisions.

The Two Translation Questions

Translate every finding into these before doing anything else:

1. Who can reach this? (Which users and groups are effectively included?)
2. What can they do from there? (Read, write, traverse, execute?)

If you cannot write the sentence:

> "These identities can do X to this thing,"

you do not yet understand the risk.

The Meaning of r, w, x (Correctly)

Files:

- `r`: read file contents
- `w`: modify file contents (including truncation)
- `x`: execute the file

Directories:

- `r`: list names in the directory
- `w`: create, delete, or rename entries
- `x`: traverse the directory

Rule: Directory execute means can pass through. It does not mean can run.

The Three Review Tests

An access-control claim is ready for review only if it passes all three:

Test	What It Requires
Identity Test	Name concrete users or groups, not roles or job titles
Action Test	Name a specific action (read, write, traverse, execute)
Verification Test	Supported by an actual attempt at that identity

Rewrite rule: If a claim fails one test, rewrite only the failing part.

CIA, Used Correctly

CIA is outcome vocabulary, not an explanation.

Category	Meaning
Confidentiality	The wrong identity can read information
Integrity	The wrong identity can modify information or behaviour
Availability	A required action fails when needed

Rule: Apply CIA only after you can state who can do what to what.

Core Process to Practice

Use this sequence until it becomes automatic:

1. Name the thing: Identify the file or directory, owner, and group.
2. Translate permissions: Write who can read, write, traverse, or execute.
3. Predict access: State what each identity can do.
4. Verify: Attempt the action as that identity.
5. Record evidence: Write what actually happened in plain language.
6. Fix only what's wrong: Adjust ownership or permissions.
7. Retest: Confirm the change affected only the intended access.
8. Classify harm: Apply CIA if access exceeds intent.
9. Improve friction: Narrow reachability without breaking normal work.

Common Traps

- Treating permissions as syntax instead of people and actions
- Assuming octal values mean something instead of compression
- Confusing directory read with directory execute
- Using shared identities while pretending accountability exists
- Skipping verification and trusting mental models
- Listing CIA labels without a concrete access statement

Readiness Questions

Answer without notes. Hesitation shows what to practice next.

Model Recall

1. Write the access model from memory.
2. Define user, group, and permission in one sentence each.

Identification Skill

3. Given `ls -l` output, state who can read, write, and execute the file.
4. Given a directory with no read but execute permission, explain what access exists.

Verification Discipline

5. When a test fails, what is the only part you are allowed to change?
6. How do you record test results as evidence rather than interpretation?

CIA Correctness

7. If a group can read private records, which CIA category is the primary one, and why?
8. If a group can write a config file that drives the output, which CIA category is the primary one, and why?
9. If a service fails because its directory is writable by many users, which CIA category is the primary one?

Confidence Check

10. Which is hardest for you to make concrete: identities, actions, or verification evidence?
11. When revising an access claim, what do you check first to confirm improvement?

Practice Questions

Answer in writing. Short, precise statements are better than long explanations.

Definitions and Recall

1. Write the access model from memory.
2. Define user using the word “identity.”
3. Define group using the word “membership.”
4. Define permission using the word “actions.”
5. Explain why octal values are not explanations.

Extraction from Scenarios

6. What is a sign that your access statement names roles instead of identities?
7. What is a sign that your action description is too vague to test?
8. What is a sign that your statement assumes behaviour without verification?
9. What is a sign that you changed more permissions than necessary?

Writing Reviewable Claims

10. Write a sentence template for naming who can read a file.
11. Write a sentence template for naming who can traverse a directory.
12. Write a sentence template for recording verification evidence.
13. What minimum information must an access claim contain to be reviewable?

Test Practice

14. Give an example of a claim that fails the Identity Test.
15. Give an example of a claim that fails the Action Test.

16. Give an example of a claim that fails the Verification Test.
17. If only the Verification Test fails, what can you rewrite?
18. Why does rewriting only the failing component matter?

CIA Classification

19. A group can read a password file but not modify it. Which CIA category is primary, and why?
20. A group can modify a script executed by root. Which CIA category is primary, and why?
21. A shared directory becomes unusable due to conflicting writes. Which CIA category is primary?
22. Why is it misleading to list multiple CIA categories without choosing one?

Friction Thinking

23. Describe one change that reduces unintended access without breaking normal workflows.
24. Describe one change that sounds like security work but does not change access.
25. Why does removing shared credentials usually improve both security and accountability?

Confidence Check

26. Which part of access control do you personally over-assume instead of verifying?
27. What is the first test you run after changing permissions, and why?

If you can consistently write, test, and revise access-control claims that pass all three review tests, you understand Linux access control well enough to secure it.