CompTIA PenTest+ (PT0-002) Quick Summary

Fast 3-5 minute refresh for the workflow, comparisons, and common traps in a legacy PT0-002 context.

Best for	Focus	Use with
Ultra-fast memory refresh	Definitions, priorities, and pentest shortcuts	Use with cheat sheet for deeper review

1. Fast refresh

Pentest flow	Scope, recon, enumerate, validate, exploit, document.
Evidence matters	Screenshots, logs, commands, and timestamps support credibility.
Context beats noise	A long scan report is weaker than a validated chain with business impact.
Reporting is part of the test	A great exploit with a weak report is still weak work.

2. Common traps

Finding vs proof	A vulnerability finding is not the same as demonstrated exploitability.
Recon vs enumeration	Broad discovery differs from detailed target-specific extraction.
Exploit vs post-exploitation	Getting in is not the same as proving impact or pivot paths.
Severity vs priority	The most severe issue is not always the first remediation priority.

3. Operator shortcuts

Start with scope	Know what you are allowed to touch.
Validate carefully	False positives waste time and damage trust.
Think chains	Low-risk findings can combine into major exposure.
Document live	Do not trust memory after a long engagement.

4. Exam traps

Passive first when possible	Sometimes stealth and evidence preservation beat noisy speed.
Privilege matters	Access level shapes what each technique can really prove.
Business context	A small technical flaw can be a large business risk.
Cleanup	Post-engagement hygiene is part of professionalism.