CompTIA PenTest+ (PT0-002) Cheat Sheet

One-page cram sheet for scoping, recon, vulnerability analysis, exploitation, and reporting. Legacy PT0-002 set.

Best for	Focus	Use with
Last review for legacy notes or comparisons	Pentest workflow + validation + reporting logic	Use with ports sheet and commands sheet

1. Engagement and scoping

Rules of engagement	Define scope, targets, windows, communication paths, and what is explicitly off-limits.
Authorization	A pentest without clear written authorization is not a valid engagement plan.
Risk-aware scoping	Production sensitivity, data exposure, and test impact affect method choice.
Reporting expectations	Executive summary, technical findings, proof, and remediation must be planned early.

2. Reconnaissance and enumeration

Passive vs active recon	Passive reduces visibility to defenders; active usually yields richer technical detail.
DNS / service enumeration	Names, records, banners, and exposed services often shape the first attack path.
OSINT	People, domains, leaks, metadata, and public infrastructure can all feed initial hypotheses.
Validation mindset	Enumerate with a purpose: identify attack surface, trust paths, and likely weak controls.

3. Vulnerability analysis

Scan vs exploit	A finding is not proof until validated with context and safe testing.
False positives	Good testers verify before escalating or reporting.
Prioritization	Exploitability, business impact, exposure, and chain potential matter more than raw score alone.
Web and cloud awareness	PT0-002 still expects broad awareness across apps, auth, and misconfigurations.

4. Attacks and post-exploitation

Credential attacks	Password spraying, brute force, reuse, and weak auth workflows remain high-yield.
Web attacks	Injection, XSS, auth flaws, insecure direct object reference, and logic issues matter.

Privilege escalation	Local weaknesses often matter as much as initial access.
Lateral movement	The real finding is often how far one foothold can spread.

5. Reporting and remediation

Proof of impact	Show enough evidence to support the finding without causing unnecessary damage.
Actionable remediation	The best pentest report explains what to fix and why it matters.
Audience split	Executives need impact; engineers need reproducible detail.
Cleanup	Remove artifacts, restore changes, and document residual risk clearly.