GIAC Penetration Tester (GPEN) Cheat Sheet

One-page cram sheet for enterprise penetration testing process, recon, exploitation, validation, and reporting.

Best for	Focus	Use with
Last review before drills or course revision	Methodology + evidence + business impact	Use with ports sheet and commands sheet

1. Penetration test process

Scoping and ROE	Clear scope, targets, allowed methods, test windows, and communication paths are part of the job.
Process-oriented testing	GPEN emphasizes methodology, not just tool output or one-off exploits.
Evidence and notes	Commands, screenshots, proof, and timestamps support both reporting and cleanup.
Business risk lens	The best finding explains impact, not just a technical weakness.

2. Reconnaissance and enumeration

Passive vs active recon	Use passive methods for early context and active methods for precise target details.
Host and service discovery	Ports, banners, certificates, headers, and DNS all shape attack planning.
Auth surface	Login points, MFA gaps, password policy, federation, and exposed admin panels matter.
Environment awareness	On-prem, Azure, and identity infrastructure can all be part of the engagement surface.

3. Exploitation and validation

Validation first	A likely weakness is not a confirmed finding until tested carefully.
Web and auth flaws	Injection, weak auth flow, exposed admin services, and misconfigurations remain high-yield.
Credential attacks	Password spraying, reuse, and weak auth workflows are often safer and more realistic than noisy exploits.
Privilege escalation	Proving local impact can be as important as initial access.

4. Post-exploitation and reporting

Lateral movement	The real impact often lies in what one foothold can reach next.
Data exposure	Focus on business evidence, sensitive access, and trust-path abuse rather than unnecessary damage.
Cleanup	Remove artifacts, restore changes, and document residual risk.

Remediation	Strong reports explain both the issue and the practical fix path.

5. Practical GPEN mindset

Method over hype	Good testing is structured, repeatable, and evidence-backed.
Tool choice matters	Choose the right tool for the target and the rules of engagement.
Cloud-aware pentesting	Modern enterprise pentests include cloud and identity exposure, not just classic internal networks.
Hands-on orientation	This track rewards applied reasoning more than memorized definitions.