MNA TECH ACADEMY
LEARN • PRACTICE • SUCCEED

PENETRATION TESTING · 2026 EDITION

PTES Penetration Testing Execution Standard Handbook

A phase-by-phase operational handbook for scoping, evidence, controlled testing, and decision-ready reporting.

7	30+	1
Core phases	Delivery checks	Repeatable workflow

mnatech.in @mna_tech_academy +91 9216110094

MNA TECH ACADEMY
LEARN • PRACTICE • SUCCEED

How to use this guide

Use this handbook to structure an authorized assessment from the first scope conversation to remediation validation. Adapt depth and techniques to risk, time, and written rules of engagement.

> **Professional-use notice:** Security testing must stay within systems you own or have explicit written authorization to assess. Standards summaries are educational aids, not certification, legal, or audit advice.

Inside this resource

01 **Pre-engagement Interactions**
Define why the test exists, what is allowed, and how safety decisions will be made.

02 **Intelligence & Threat Modeling**
Build context before sending intrusive traffic.

03 **Vulnerability Analysis**
Combine tooling with manual reasoning and validate before escalation.

04 **Exploitation & Post-exploitation**
Prove impact with restraint and continuous safety checks.

05 **Reporting & Retest**
Produce evidence that executives and engineers can act on.

06 **Field Checklists & References**
A compact quality gate for every engagement.

Pre-engagement Interactions

Define why the test exists, what is allowed, and how safety decisions will be made.

Objectives
Translate business concerns into measurable test goals.

Scope
List assets, environments, exclusions, third parties, and permitted identities.

Rules of engagement
Define methods, hours, rate limits, social engineering, persistence, and data handling.

Contacts
Name operational, security, legal, and emergency decision makers.

Stop conditions
Document impact thresholds and the exact escalation channel.

Deliverables
Agree formats, severity method, evidence needs, retest, and retention.

Intelligence & Threat Modeling

Build context before sending intrusive traffic.

Asset intelligence

Map domains, applications, cloud services, technology, and ownership from approved sources.

Business context

Identify critical workflows, regulated data, trust boundaries, and high-impact roles.

Threat actors

Prioritize realistic motivations, access levels, and techniques.

Attack surface

Connect exposed services, identities, integrations, and supply-chain dependencies.

Output: an evidence-backed attack-surface map and prioritized test hypotheses—not an uncontrolled collection exercise.

Vulnerability Analysis

Combine tooling with manual reasoning and validate before escalation.

Step	Action	Evidence
Discover	Identify candidate weakness within scope	Tool output, request/response, configuration
Triage	Remove false positives and duplicates	Manual validation notes
Contextualize	Map affected asset, identity, and business process	Data flow and preconditions
Prioritize	Estimate likelihood, impact, and exploit path	Severity rationale
Plan validation	Choose lowest-impact proof	Test steps and rollback

Exploitation & Post-exploitation

Prove impact with restraint and continuous safety checks.

Minimum proof
Stop when agreed impact is demonstrated; avoid unnecessary data access.

Session control
Record target, source, identity, timestamps, and commands.

Privilege and pivoting
Require explicit scope before escalation or lateral movement.

Sensitive data
Use synthetic evidence where possible; encrypt approved captures.

Persistence
Only when explicitly authorized, time-bound, documented, and removed.

Cleanup
Remove accounts, files, agents, rules, tokens, and test data.

Reporting & Retest

Produce evidence that executives and engineers can act on.

Section	Contents
Executive summary	Objectives, overall risk, themes, and business decisions
Scope and limitations	Assets, dates, methods, exclusions, and constraints
Finding	Title, severity, asset, evidence, impact, root cause, fix
Attack narrative	Validated chain and defensive control opportunities
Appendices	Method, tools, accounts, timestamps, evidence index
Retest	Fixed, partially fixed, not fixed, or cannot verify

Field Checklists & References

A compact quality gate for every engagement.

- Signed authorization and final asset list received
- Emergency contacts tested before active work
- Time synchronization and evidence storage verified
- Daily scope and safety review completed
- All high-impact observations escalated as agreed
- Cleanup evidence captured
- Report peer-reviewed for accuracy and sensitive data
- Retest criteria agreed

References

- PTES — http://www.pentest-standard.org/
- OWASP Web Security Testing Guide — https://owasp.org/www-project-web-security-testing-guide/
- NIST SP 800-115 — https://csrc.nist.gov/publications/detail/sp/800-115/final



Keep learning. Keep building.

Use this guide as a working plan: practise, document evidence, review outcomes, and improve the next iteration.

mnatech.in @mna_tech_academy +91 9216110094

© 2026 MNA Tech Academy. Original educational resource. Product names and trademarks belong to their respective owners. Verify standards and product details against official sources before production use.