



Engagement Methodology and Reporting

CompTIA PenTest+ PT0-003 Domain 1.0 | EC-Council CEH v13 Module 01 | OffSec OSCP report | PTES, OSSTMM, NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment), OWASP WSTG

#PenetrationTesting

#Methodology

#Reporting

#CVSS

✓ Scope and Rules of Engagement First

⚠ No signed authorization, no packets

Test only assets listed in the signed scope, inside the agreed window, from the declared source IPs. Out-of-scope discovery (a forgotten subdomain, a third-party SaaS tenant) is reported, never tested, until the client extends the scope in writing. Unauthorized access is a crime in most jurisdictions (US CFAA, UK Computer Misuse Act, FR art. 323-1 Code penal).

Rules of engagement (RoE) minimum content

✓ baseline / mandatory □ recommended – verify in your context

- ✓ Signed authorization letter from an asset owner with authority to grant it
- ✓ In-scope assets: CIDR ranges, domains, applications, cloud accounts, people
- ✓ Explicit exclusions: production databases, OT (operational technology: industrial control)/medical devices, third parties
- ✓ Testing window, blackout dates, time zone
- ✓ Tester source IPs registered with the SOC (security operations centre), and a decision on whether the WAF/IPS allow-lists them
- ✓ Emergency contacts, escalation path, stop-test criteria
- **MUST** Data handling: what may be exfiltrated as proof, retention, encryption of evidence
- **MUST** Denial-of-service, social engineering and physical testing each need explicit opt-in
- **SHOULD** Cloud provider policy checked (AWS, Azure, GCP allow most tests without notice; DoS excluded)

MSA — Master services agreement - long-term commercial and liability terms.

SOW — Statement of work - this engagement's deliverables, dates, price, acceptance.

NDA — Non-disclosure agreement - protects findings and client data; often mutual.

Authorization letter — The 'get out of jail' letter - names testers, targets, dates, signer's authority.

Third-party authorization — Written consent from hosting or SaaS provider when their assets are touched.

RoE — Rules of engagement: the operational limits of the test (what, when, how, who to call).

CFAA — US Computer Fraud and Abuse Act (1986): federal law criminalising unauthorised access to computers.

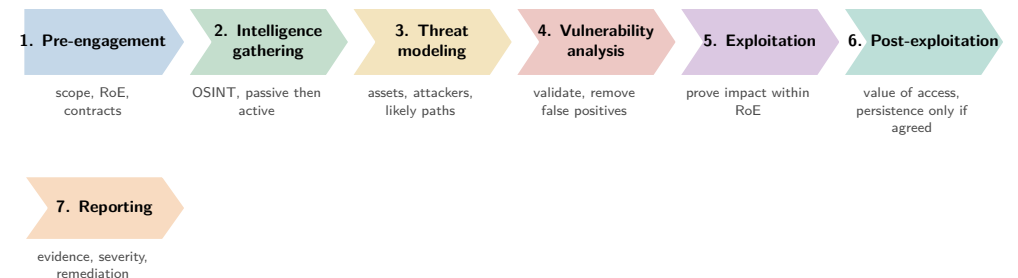
Deconfliction — Telling test activity apart from a real attack, using registered tester IPs and timestamps.

Crown jewels — The client's most valuable assets (customer database, payment system, domain admin) used as test objectives.

☰ Frameworks Compared

PTES = Penetration Testing Execution Standard (community, 2009). **OSSTMM** = Open Source Security Testing Methodology Manual (ISECOM, Institute for Security and Open Methodologies). **RAV** = Risk Assessment Value, OSSTMM's measure of attack surface. **STAR** = Security Test Audit Report, OSSTMM's report template. **CREST** = UK accreditation body for penetration testing companies and testers.

PTES	OSSTMM v3	NIST SP 800-115	OWASP WSTG v4.2
7 phases, pre-engagement to reporting	5 channels: human, physical, wireless, telecom, data networks	4 phases: planning, discovery, attack, reporting	12 test categories, ~100 numbered tests
Community standard, tool-agnostic	ISECOM, metric-driven (RAV score)	US federal technical guide	Web and API applications only
Best for: full-scope pentest structure	Best for: repeatable audit with a score	Best for: government, policy alignment	Best for: web app test plan and coverage
Output: report per phase	Output: STAR report	Output: findings and remediation plan	Output: WSTG-ID coverage matrix



PTES phases (Obj 1.3 lists PTES, OSSTMM, MITRE ATT&CK, OWASP, CREST, NIST)

Exam	Format	Where methodology and reporting sit
PenTest+ PT0-003	max 90 questions, 165 min, 750/900, released Dec 2024	Domain 1.0 Engagement Management (13%): Obj 1.1 pre-engagement, 1.2 collaboration, 1.3 frameworks, 1.4 report components, 1.5 remediation
CEH v13 (312-50)	125 questions, 4 h, MCQ; CEH Practical is a separate 6 h lab	Module 01 Introduction to Ethical Hacking: hacking phases, laws, standards; reporting in every module
OSCP / OSCP+	23 h 45 min hands-on exam, then 24 h to submit the report, 70/100 points	Report is graded: missing evidence or steps means lost points; OSCP+ (Nov 2024) expires after 3 years

EXAM TIP

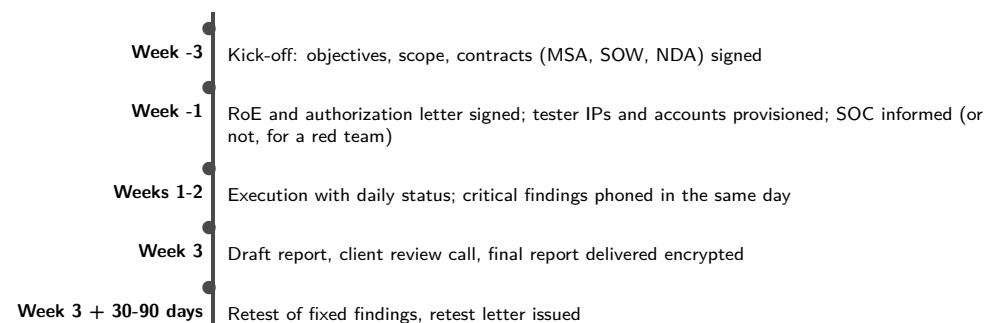
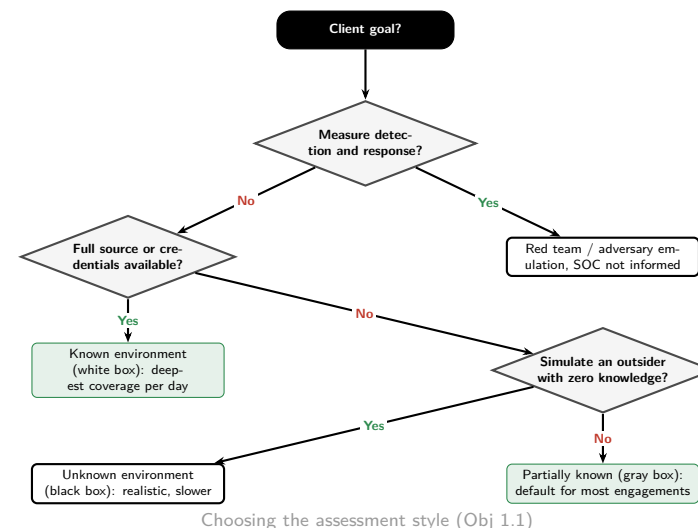
NIST SP 800-115 has FOUR phases and its 'attack' phase contains gaining access, escalating privileges, system browsing and installing additional tools. PTES has SEVEN. OSSTMM produces a RAV (Risk Assessment Value), not a CVSS score. Expect questions that swap phase counts between frameworks.

Engagement Lifecycle



Mnemonic: SCOPE

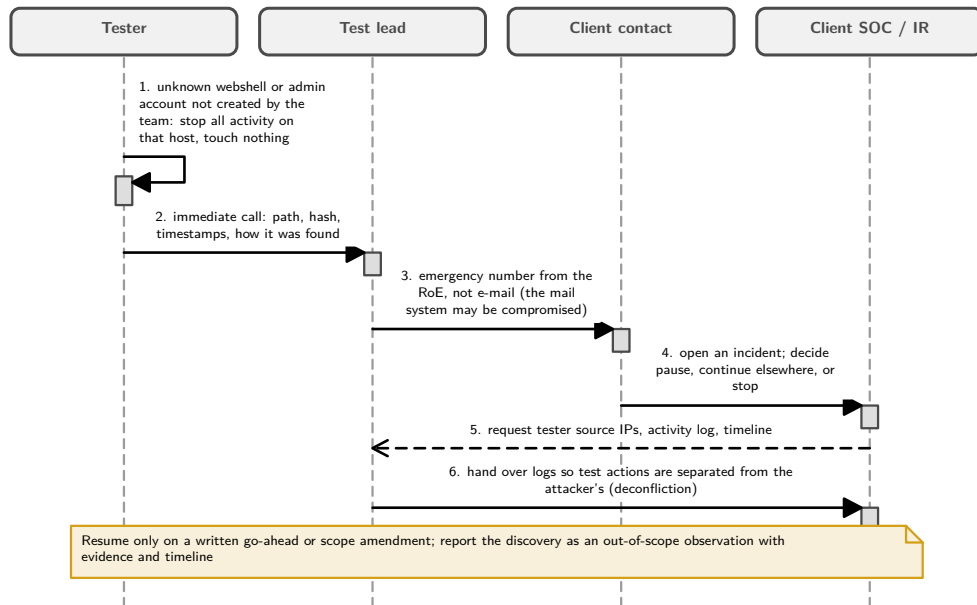
- S** **Systems** exact asset list, environments (prod, staging)
- C** **Constraints** window, rate limits, excluded techniques
- O** **Objectives** compliance evidence, crown-jewel access, coverage
- P** **People** contacts, escalation, who knows the test is running
- E** **Evidence** what proof is acceptable, how it is stored and destroyed



📱 Communication During the Test (Obj 1.2)

Trigger for an immediate call to the client contact

- **Critical finding on an internet-facing asset** do not wait for the report; client may need to patch today
- **Evidence of a prior compromise (webshell, unknown admin account)** stop, preserve, hand over to incident response
- **Sensitive data found (PII, health, payment)** stop at proof of access; never download bulk data
- **Service instability caused by testing** pause, notify, agree on safer approach
- **Scope creep request from client staff** accept only via written scope amendment
- **Daily status and weekly summary** situational awareness for client and tester



Signs of a prior compromise found mid-test (PT0-003 Obj 1.2): stop, escalate out of band, deconflict, resume only in writing

Task	Client sponsor	Client contact	Client SOC	Test lead	Tester	Legal
Sign the authorization and rules of engagement	A	C	I	R	I	C
Define scope, exclusions and test windows	A	R	C	R	C	I
Deconflict alerts raised by test traffic	I	A	R	C	R	
Stop testing on a critical finding or prior compromise	I	C	C	A	R	
Deliver the report and debrief	I	C	I	A	R	
Remediate findings or formally accept the risk	A	R	C	I		I
Destroy evidence and recovered credentials at close	I	C		A	R	I

R Responsible A Accountable C Consulted I Informed

Who does what across an engagement (typical split; one Accountable per task)

Deconfliction
SOC needs tester IPs and timestamps to separate test traffic from a real attack.

Goal reprioritization
Client shifts focus mid-test (new release, incident); record the change in writing.

Situational awareness
Client sees progress; tester learns about changes and outages.

EXAM TIP
PT0-003 Obj 1.2 wording: 'deconfliction', 'de-escalation', 'goal reprioritization', 'situational awareness', 'stakeholder alignment'. A question about a tester who found signs of an APT expects: stop testing, notify the client contact immediately, preserve evidence.

⚠️ Severity Rating

CVSS 4.0 group	Metrics	Who sets it
Base: exploitability	AV attack vector (network, adjacent, local, physical), AC attack complexity, AT attack requirements, PR privileges required, UI user interaction	vendor or tester
Base: vulnerable system impact	VC, VI, VA: confidentiality, integrity, availability impact on the flawed system	vendor or tester
Base: subsequent system impact	SC, SI, SA: the same three impacts on other systems reached from it	vendor or tester
Threat	E exploit maturity (attacked, proof-of-concept, unreported)	tester, from CTI (cyber threat intelligence)
Environmental	modified base + CR, IR, AR: how much the client needs confidentiality, integrity, availability of the asset	client
Supplemental	Safety, Automatable, Recovery, Value Density, Response Effort, Urgency	informational

Score	Rating	Report SLA (typical)
9.0-10.0	critical	fix or mitigate within days; call the client now
7.0-8.9	high	next patch cycle, weeks
4.0-6.9	medium	planned, quarter
0.1-3.9	low	backlog or accept
0.0	n/a	informational, no action

TIP

State the nomenclature used: CVSS-B (base metrics only) vs CVSS-BT (plus threat) vs CVSS-BTE (plus environmental). A 9.8 library flaw on an isolated host can be a business Medium; a 5.3 leak of all customer emails can be a business High. Say which scale you used and why.

Report Structure (Obj 1.4)

- Executive summary 1-2 pages, no jargon
 - Scope, dates, method, assumptions
 - Overall risk statement and top 3 findings
 - Charts: findings by severity, by category
- Methodology and coverage
 - Framework followed (PTES, WSTG IDs tested)
 - What was NOT tested and why (out of scope, time, blocked)
- Findings
 - One entry per finding, ordered by severity
 - Title, ID, severity, CVSS vector, affected assets
 - Description, evidence, impact, remediation, references
- Appendices
 - Full host and port inventory, tool list, raw evidence index
 - Attack narrative or path diagram (red team)
 - Retest and remediation tracker

Evidence	Screenshot with hostname, timestamp and tester prompt visible; request/response pairs; hash of any file used as proof
Impact	What an attacker gains in business terms (customer data, fraud, downtime), not only 'RCE'
Root cause	Missing patch, insecure default, absent validation, process gap - drives the fix
Remediation	Specific, testable, prioritized; short-term mitigation plus long-term fix
References	CVE, CWE, ATT&CK technique, WSTG ID, vendor advisory, benchmark control
Distribution	Encrypted delivery, classification marking, named recipients, retention period

EXAMPLE

Finding title done right: 'Unauthenticated SQL injection in /api/v2/orders?id= allows read of the orders database (CWE-89, CVSS 4.0 B:9.3)'. Wrong: 'SQL injection found'. The title alone must tell a manager where, what and how bad.

Remediation Recommendations (Obj 1.5)

Technical controls	Administrative and operational
Patch or upgrade, with version	Policy or standard update
Configuration hardening (CIS benchmark item)	Secure SDLC gate, code review
Input validation, parameterized queries	User awareness, role-based training
MFA, least privilege, network segmentation	Vendor management, SLA clause
Logging and alert rule for the technique	Asset inventory and ownership

- Ticket per finding owner, due date derived from severity, link to report ID
- Risk decision fix, mitigate, transfer or accept - signed by the risk owner, with expiry
- Retest same tester method, same evidence format; close, partially fixed or reopened
- Trend compare with previous engagements: time-to-fix, recurring root causes

Remediation tracking loop

WARNING

A retest verifies the specific finding, not the whole application. Say so in the retest letter. A 'fixed' status with a WAF rule only is 'mitigated', not 'remediated': the root cause remains.

Detect and Prevent the Tester

NOTE

At close-out, classify each tester action as alerted, logged only, or invisible; map each to an ATT&CK technique and a detection backlog item.

Tester activity	Detected?	Detection source to build
External port and service scan	partial	perimeter IDS threshold, honeypot ports
Credential spraying against SSO	yes	IdP failed-login correlation per source
Web parameter tampering	no	WAF in blocking mode, app-level anomaly logs
Internal host discovery	no	NetFlow baseline, canary hosts and tokens
Privileged group change	yes	Windows events 4728/4732/4756 (member added to a security-enabled global/local/universal group) to SIEM

SOC console during the test window

S	SIEM Password spray on SSO from 203.0.113.25 Source IP is on the registered tester list, inside the window: tag 'pentest', keep the alert	now
E	EDR Suspicious PowerShell on FIN-WS-042 Host in scope but no tester activity logged at 10:41: treat as real, call the test lead	4 min
I	IDP Admin sign-in from 198.51.100.7 Not a tester IP: open an incident, do not wait for the report	12 min

Deconfliction in practice: an alert is closed as test traffic only when source IP, time window and the tester's activity log all match; anything else is a real incident (IPs from documentation ranges).

Q1 Which document names the testers, the targets, the dates and the signer's authority?

A The authorization letter (part of the RoE), signed by an asset owner with authority.

Q2 Four phases of NIST SP 800-115?

A Planning, Discovery, Attack, Reporting.

Q3 CVSS 4.0 nomenclature when Threat and Environmental metrics are applied?

A CVSS-BTE.

Q4 Tester finds an active webshell that is not theirs. Next step?

A Stop, preserve evidence, notify the client contact immediately; incident response takes over.

Q5 Difference between mitigated and remediated?

A Mitigated reduces exposure (WAF rule, segmentation); remediated removes the root cause (patch, code fix).