CERTCRACK PRACTICE EXAMS

CompTIA PenTest+ (PT0-003)

Free sample — 30 questions from the full CertCrack PenTest+ (PT0-003) practice bank, with detailed explanations.

Full bank: 750 original practice questions + 10 performance-based questions
Domain 1: Engagement Management (13%) · Domain 2: Reconnaissance and Enumeration (21%)
Domain 3: Vulnerability Discovery and Analysis (17%) · Domain 4: Attacks and Exploits (35%)
Domain 5: Post-exploitation and Lateral Movement (14%)

Copyright & Disclaimer

CompTIA PenTest+ (PT0-003) — Free Sample (30 Questions)

Published by CertCrack · certcrack.com

Copyright © 2026 CertCrack. All rights reserved.

All questions in this book are 100% original practice material written by CertCrack. They are not real exam questions and are not affiliated with or endorsed by CompTIA, Inc.

Unofficial practice material — not affiliated with or endorsed by CompTIA, Inc.

The performance-based questions (PBQs) use simplified, fictional exhibits written for this book. Tool-output samples shown anywhere in this book are illustrative examples, not captures of real product screens.

This free sample contains 20 questions drawn from the full bank plus 10 of the new tool-focused questions. The complete bank — 750 questions and 10 performance-based questions — is available at certcrack.com.

Domain 1: Engagement Management (13%)

Q1. [pentest-001] CertCrack.com hires a penetration testing team to assess its production web application. During scoping, the client states that the payment processing subsystem is out of scope, but the testers later discover that the payment API is reachable from the in-scope application. What should the testers do first?

A. Silently test the payment API, since it is reachable from an in-scope system and quietly confirming the exposure would help the client sooner
B. Exclude the payment API from the report entirely
C. Test the payment API and disclose it only if a critical flaw is found
D. Notify the client point of contact and obtain a written scope amendment before testing the payment API

> Correct answer: D Explanation: Correct: testing outside the agreed scope violates the authorization, so the team must notify the client contact and get a written amendment before touching the payment API. Why others are wrong: silently testing it is unauthorized regardless of reachability; excluding it entirely hides a risk the client should know about through proper channels; testing first and disclosing conditionally is still unauthorized testing.

Q2. [pentest-020] Choose two. Which two items must be defined in a scoping document before testing begins?

A. The authorized IP ranges and hostnames
B. The agreed testing windows
C. The testers' personal salaries
D. The exploit code the team plans to use

> Correct answer: A and B Explanation: Correct: authorized targets and agreed testing windows are core scoping elements that bound what may be tested and when. Why others are wrong: tester salaries are a commercial matter, not scope; specific exploit code is a tactical detail decided during testing, not a scoping requirement.

Q3. [pentest-045] During a three-week engagement, how should the testing team keep the client informed?

A. Provide status updates at the frequency and through the channels agreed in the rules of engagement
B. Send raw tool output daily, so the client can follow every test step and finding as it happens without waiting for summaries
C. Report only at the end of the engagement
D. Update only when critical findings appear

> Correct answer: A Explanation: Correct: update frequency and channels are engagement terms, so the team follows what the rules of engagement agreed. Why others are wrong: daily raw output is unsafe and noisy; end-only reporting leaves the client blind for weeks; critical-only updates omit progress and lower findings the client expects to track.

Q4. [pentest-070] Which findings should be remediated first?

A. Those easiest to fix
B. Those found last
C. Those affecting the most systems regardless of severity
D. Critical, exploitable findings on exposed systems

> Correct answer: D Explanation: Correct: remediation order follows risk: critical, exploitable flaws on exposed systems cause the most harm soonest. Why others are wrong: ease of fixing ignores risk; discovery order is arbitrary; affecting many systems does not make a finding the highest priority, since severity and exploitability on exposed systems decide.

Domain 2: Reconnaissance and Enumeration (21%)

Q5. [pentest-100] While reviewing DNS records for CertCrack.com, a tester reads a TXT record containing v=spf1 and several include statements. What does this record most usefully reveal?

A. The version of the company's web server software and its patch level and loaded modules
B. A complete list of the company's subdomains
C. The company's internal network address ranges
D. Which third-party services are authorized to send mail for the domain

> Correct answer: D Explanation: Correct: SPF data published in TXT records lists authorized mail senders, revealing email providers and related third parties. Why others are wrong: web server versions appear in HTTP banners, not DNS TXT records; TXT records do not enumerate subdomains; internal address ranges are not published in public TXT records.

Q6. [pentest-150] Version detection on an authorized target shows SSH answering on TCP 8080. What should the tester conclude?

A. Report port 8080 as a web server because 8080 is conventionally used for web traffic
B. Ignore the version result and use the port number instead
C. Skip the host, since non-standard ports are out of scope
D. Report SSH on port 8080, since the service matters more than the port number

> Correct answer: D Explanation: Correct: version detection reports the actual service, and services can bind any port, so the port number alone never identifies the service. Why others are wrong: assuming HTTP from the port number repeats the error; reporting 8080 as a web server would be factually wrong; skipping identification leaves the finding inaccurate.

Q7. [pentest-200] A tester runs curl -I against an authorized target's website. What does this command return?

A. Downloading the full page body and its linked resources
B. Scanning ports on the web server
C. Reading the server header without the page body
D. Exploiting the web server

> Correct answer: C Explanation: Correct: curl with -I requests headers only, so the tester reads the Server header without downloading the page body. Why others are wrong: a plain curl call downloads the full body; curl does not scan ports; and it does not exploit the server.

Q8. [pentest-701] A penetration tester engaged by CertCrack.com has only the root domain to start from and needs the most complete inventory of subdomains possible before any scanning begins. Which tool should the tester run to enumerate subdomains by merging many OSINT sources with DNS enumeration techniques?

A. theHarvester, to collect employee email addresses from search engines
B. Amass, in enumeration mode against the root domain
C. Shodan, queried for the domain's known IP ranges
D. A single DNS zone transfer attempt against the primary name server

Correct answer: B Explanation: Correct: Amass is built for attack-surface mapping — it merges dozens of OSINT data sources with DNS techniques (brute forcing, permutations, certificate and web scraping) to produce the subdomain inventory other tools then scan. Why others are wrong: theHarvester gathers email addresses and some hostnames from search engines — an email-focused collection, not a systematic subdomain enumeration; Shodan indexes services on addresses it has already scanned; it cannot enumerate the subdomains of a domain; a zone transfer works only when a server is misconfigured to allow AXFR, and even then yields one server's records rather than a merged multi-source inventory.

Domain 3: Vulnerability Discovery and Analysis (17%)

Q9. [pentest-250] CertCrack.com's tester must scan a network segment that contains fragile legacy devices the client says cannot tolerate unexpected traffic. Which scan approach best balances assessment value against the risk of disruption?

A. A full credentialed scan at maximum intensity against every device
B. An aggressive scan of every port on every device in the segment
C. A denial-of-service test to confirm the devices can survive heavy traffic without disruption
D. An unauthenticated scan with safe checks only, plus passive observation of traffic

> Correct answer: D Explanation: Correct: safe checks plus passive observation assess the segment without sending disruptive probes to fragile devices. Why others are wrong: maximum-intensity credentialed scans risk crashing fragile devices; denial-of-service testing is a disruption, not an assessment method, and is out of place here; aggressive full-port scanning is exactly the traffic the client warned against.

Q10. [pentest-300] A Nessus report for a CertCrack.com host includes several informational results alongside the vulnerabilities. How should the tester treat the informational results?

A. They are low-severity vulnerabilities, just below the reporting threshold for clients
B. They are false positives that should be removed from the report
C. They describe observed facts, such as the detected OS, and are not vulnerabilities
D. They prove the host was exploited at some point in the past

> Correct answer: C Explanation: Correct: informational results describe what the scanner observed, such as the operating system, and are not vulnerabilities. Why others are wrong: informational results are not low-severity flaws; they are not false positives, since they make no vulnerability claim; they are not proof of exploitation.

Q11. [pentest-350] Two low-severity flaws at CertCrack.com chain together: one discloses a session token, the other uses it to reach an administrative function. How should the tester prioritize them for exploitation planning?

A. Treat each flaw in isolation at its own low priority level
B. Prioritize the chain as a unit, since it reaches administrative access
C. Deprioritize the chain because each flaw is low severity alone
D. Patch only the first flaw and ignore the second one entirely

> Correct answer: B Explanation: Correct: two low-severity flaws that chain into administrative access present a higher risk together than either does alone, so the chain is prioritized as a unit. Why others are wrong: treating each flaw in isolation misses the chain; the chain's risk is higher, not lower, than its parts; patching only one link without noting the chain leaves the path partially open.

Q12. [pentest-709] CertCrack.com's CI pipeline must block builds that leak credentials. A developer once committed an AWS key and later 'removed' it in a follow-up commit. Which tool should scan the repository's full git history — including that earlier commit — for secrets, and can verify whether found keys are still live?

A. TruffleHog, scanning git history for secrets
B. Grype, matching vulnerabilities from an SBOM
C. Docker Bench, auditing the build host's Docker configuration

D. Nikto, scanning the running web server

> Correct answer: A Explanation: Correct: TruffleHog digs through git history commit by commit, finds secrets with hundreds of detectors, and can validate many of them against the live service — so the key 'removed' in a later commit is still caught in history, where it remains exposed. Why others are wrong: Grype matches known package vulnerabilities in images and SBOMs; it does not hunt credentials in commit history; Docker Bench checks a Docker host's configuration against benchmark guidance, not repositories; Nikto scans a running web server for dangerous files and misconfigurations; it never reads git history.

Domain 4: Attacks and Exploits (35%)

Q13. [pentest-400] During an authorized test of CertCrack.com, you broadcast an open network named for the building's cafe and present a login page asking for the company's email credentials. Several visitors enter credentials, which you capture for the report. Which attack is this?

A. Rogue wired access point
B. Evil twin attack alone
C. Captive portal phishing with a fake login page
D. Karma attack

> Correct answer: C Explanation: Correct: a fake captive portal that collects credentials from users who believe they are joining a legitimate guest network is captive portal phishing. Why others are wrong: An evil twin impersonates the SSID but does not necessarily present a credential-harvesting portal. A karma attack answers probes rather than presenting a portal. A rogue wired access point bridges to the LAN rather than harvesting web credentials.

Q14. [pentest-450] During an authorized test of CertCrack.com, you log in to several network switches using the vendor's factory username and password, which nobody changed after installation. Which weakness did you exploit?

A. Password spraying
B. Brute force
C. Unchanged default credentials
D. Credential stuffing

> Correct answer: C Explanation: Correct: default credentials on network devices are a configuration failure, and vendors publish them, so no cracking is needed at all. Why others are wrong: A brute force attack guesses many passwords rather than using one known default. Credential stuffing replays breached pairs rather than vendor defaults. Password spraying tries common passwords broadly rather than a device-specific default.

Q15. [pentest-480] During an authorized test of CertCrack.com, which two of the following are SQL injection techniques? (Choose two.)

A. Union-based injection
B. Reflected cross-site scripting
C. Boolean blind injection
D. Directory traversal

> Correct answer: A and C Explanation: Correct: union-based and boolean blind injections are both SQL injection techniques, while the other options belong to different attack classes. Why others are wrong: Reflected XSS is a scripting attack, not a database attack. A directory traversal reads files rather than querying a database.

Q16. [pentest-500] During an authorized test of CertCrack.com, which two of the following are session management vulnerabilities? (Choose two.)

A. SQL injection
B. Session fixation
C. Predictable session identifiers
D. SSRF

> Correct answer: B and C Explanation: Correct: session fixation plants an identifier before login, and predictable session identifiers can be guessed, so both are session management flaws, while the other options belong to different attack classes. Why others are wrong: SQL injection targets database queries rather than sessions. SSRF forces server requests rather than abusing sessions.

Q17. [pentest-550] During an authorized test of CertCrack.com, you take a captured request and automatically iterate its user identifier through hundreds of values to test for IDOR. Which Burp component is this?

A. Burp Intruder to automate identifier iteration
B. Burp Proxy
C. Burp Sequencer
D. Burp Repeater

> Correct answer: A Explanation: Correct: Intruder automates parameter variations, such as iterating identifiers or fuzzing inputs, across many requests from a template. Why others are wrong: Repeater handles one request at a time manually rather than automating. Proxy intercepts traffic rather than automating variations. Sequencer analyzes token entropy rather than sending varied requests.

Q18. [pentest-600] During an authorized test of CertCrack.com, you access a restricted file that proves the impact of a vulnerability. Within scope, what is the appropriate next step?

A. Disabling the host's firewall
B. Capturing proof of access for the report
C. Deleting the restricted file after reading it
D. Changing the file's permissions

> Correct answer: B Explanation: Correct: capturing proof of access, such as a screenshot of a restricted file or a captured hash, documents the finding for the report without altering the target beyond scope. Why others are wrong: Deleting the file would destroy evidence and exceed scope. Changing the file's permissions would alter the target unnecessarily. Disabling the host's firewall would expand exposure beyond the engagement's needs.

Q19. [pentest-715] A tester with a low-privilege domain account at CertCrack.com wants to Kerberoast: request service tickets for accounts that have SPNs, save the tickets, and crack the service account passwords offline. Which tool performs this attack from the tester's Windows attack machine?

A. Mimikatz, extracting credentials from LSASS memory
B. Certify, enumerating AD CS certificate templates
C. Rubeus, requesting and harvesting Kerberos service tickets
D. Seatbelt, sweeping the local host's security posture

Correct answer: C Explanation: Correct: Rubeus is the Kerberos toolkit — its kerberoast function requests TGS tickets for SPN accounts from the KDC, exports them in a crackable format, and hands them to an offline cracker, exactly the attack described. Why others are wrong: Mimikatz extracts credentials that already exist in a compromised host's memory; it does not request or harvest service tickets; Certify finds and abuses AD CS misconfigurations — a certificate attack path, not SPN ticket harvesting; Seatbelt enumerates a host's configuration and security settings; it performs no Kerberos attacks.

Q20. [pentest-721] A CertCrack.com developer's AWS access keys are recovered from a public repository during the test. The tester now needs a purpose-built framework to work inside the account: enumerate what the keys can do, escalate privileges, and establish persistence. Which tool fits?

A. Pacu, the AWS exploitation framework
B. Prowler, checking the account against CIS benchmarks
C. ScoutSuite, generating a cloud posture report
D. Trivy, scanning the account's container images

Correct answer: A Explanation: Correct: Pacu is the AWS exploitation framework — modular tooling for exactly this phase: permission enumeration, privilege escalation, persistence, and data access, driven by the compromised keys. Why others are wrong: Prowler evaluates configuration against benchmarks and reports pass/fail; it deliberately does not exploit anything; ScoutSuite produces a read-only posture assessment across cloud services; it has no exploitation modules; Trivy scans container artifacts for vulnerabilities and never operates inside a cloud account.

Q21. [pentest-726] During a wireless test at CertCrack.com, the tester captures the WPA2 four-way handshake from the corporate access point. The next step is offline cracking of the pre-shared key against a wordlist. Which tool performs the crack?

A. Aircrack-ng, cracking the captured handshake
B. Kismet, logging the networks it detects
C. InSSIDer, surveying channel utilization
D. BeEF, hooking browsers on the network

Correct answer: A Explanation: Correct: Aircrack-ng is the wireless suite whose cracking engine attacks the captured WPA/WPA2 handshake (or a PMKID) with dictionary or brute-force candidates until the pre-shared key is recovered. Why others are wrong: Kismet detects and logs wireless networks and clients; it has no key-cracking function; InSSIDer visualizes channels and signal strength for surveys; it cannot crack anything; BeEF exploits hooked web browsers — a different layer and a different engagement phase entirely.

Q22. [pentest-730] For an authorized phishing exercise at CertCrack.com, the tester wants to clone the company's real SSO login page in minutes and harvest the credentials employees type into the clone. Which toolkit provides this site-cloner and credential-harvester workflow?

A. Gophish, scheduling campaign waves and tracking clicks
B. BeEF, exploiting browsers that were already hooked
C. Evilginx, proxying the live login to steal sessions
D. The Social-Engineer Toolkit (SET), cloning the page and harvesting input

Correct answer: D Explanation: Correct: SET's website attack vector clones a target page and stands up its credential harvester in one workflow — the fast, classic way to run the cloned-login exercise described. Why others are wrong: Gophish is the campaign platform — sending, tracking, and reporting across many targets — not the one-shot site-clone harvester; BeEF takes control of browsers after they are hooked; it does not clone login pages; Evilginx transparently proxies the genuine site to steal live sessions — a different mechanism from SET's static clone, and heavier to set up.

Q23. [pentest-734] To test how CertCrack.com's firewall handles malformed traffic, a tester needs to build packets field by field in Python — fragmented probes, hand-set flags, and a custom protocol exchange — and read the replies programmatically. Which tool is the packet-crafting library for this?

A. Nmap, running its standard scan types
B. Wireshark, dissecting a capture the tester already has
C. Netcat, piping a raw byte stream over TCP
D. Scapy, constructing and sending custom packets

Correct answer: D Explanation: Correct: Scapy forges, sends, and sniffs packets layer by layer under script control — the standard tool when the test needs packets that no fixed scanner template produces. Why others are wrong: Nmap's scans are pre-built probes; fine-grained, field-by-field packet construction is not its job; Wireshark analyzes traffic that already exists in a capture; it creates nothing; Netcat moves raw byte streams between endpoints but cannot assemble layered protocol headers field by field.

Q24. [pentest-738] CertCrack.com wants adversary emulation that runs like a real intrusion: a server deploys agents, chains ATT&CK abilities — discovery, then credential access, then movement — and adapts the operation to what the environment answers. Which platform does this?

A. Atomic Red Team, executing isolated technique tests
B. Infection Monkey, spreading to test segmentation
C. Caldera, running chained adversary-emulation operations
D. Metasploit, driven manually by the operator

Correct answer: C Explanation: Correct: Caldera, MITRE's adversary-emulation platform, runs operations in which its planner chains abilities across agents — exactly the autonomous, multi-step emulation the scenario describes — and maps results to ATT&CK. Why others are wrong: Atomic Red Team is a library of small, single-technique tests run one at a time; it does not chain an operation; the Monkey's purpose is propagation and segmentation testing, not a directed multi-step emulation with a planner; Metasploit is an operator-driven exploitation framework; the emulation automation and ability chaining are Caldera's.

Q25. [pentest-742] CertCrack.com's new REST API ships with a request collection. The tester wants a workbench to send crafted requests, swap authorization headers and tokens, chain calls, and inspect responses interactively before automating anything. Which tool is this workbench?

A. Postman, building and sending API requests interactively
B. sqlmap, automating injection through one parameter
C. Nikto, scanning the API host for server issues
D. Wfuzz, blasting value lists at a single endpoint

Correct answer: A Explanation: Correct: Postman is the API testing workbench — collections of requests the tester can edit, authenticate, chain, and re-send, with full response inspection, which is how API engagements explore a surface before scripting attacks. Why others are wrong: sqlmap automates SQL injection detection and exploitation against parameters; it is not a general request-building workbench; Nikto scans a web server for known dangerous files and settings, an infrastructure check rather than API exploration; Wfuzz fuzzes values at scale; interactive request crafting, header management, and response study are Postman's role.

Domain 5: Post-exploitation and Lateral Movement (14%)

Q26. [pentest-620] A tester enumerating a Windows host for privilege escalation finds several conditions. Which two allow escalation to SYSTEM? (Choose two.)

A. A service running as SYSTEM whose binary path is unquoted and whose parent folder is writable
B. A service running as SYSTEM that the tester is permitted to reconfigure
C. A service running as SYSTEM with a quoted path, a protected binary, and locked-down permissions
D. A standard user account with no special privileges or group memberships

> Correct answer: A and B Explanation: Correct: an unquoted path with a writable parent folder lets the tester plant an executable Windows runs as SYSTEM, and a reconfigurable SYSTEM service lets the tester point its binary path at a payload. Why others are wrong: a quoted path with a protected binary and locked-down permissions offers no abuse path, and a plain standard user account carries no privilege to abuse.

Q27. [pentest-650] A tester's rules of engagement authorize privilege escalation only on hosts explicitly listed in scope. During enumeration the tester finds an unpatched privilege-escalation flaw on a host that is not on the list. What should the tester do?

A. Escalate on every host discovered, regardless of scope, to maximize test coverage
B. Verify scope and report the finding, escalating only if authorized
C. Skip escalation entirely without telling the client
D. Escalate only on the tester's own workstation

> Correct answer: B Explanation: Correct: scope is binding, so the tester must verify the host is authorized and report the finding, escalating only if authorization is confirmed. Why others are wrong: escalating outside scope violates the engagement; silently skipping hides a finding the client should know about; escalating on the tester's own workstation tests nothing.

Q28. [pentest-665] A tester holds stolen credentials but no plaintext passwords. Which two techniques allow lateral movement without knowing any plaintext password? (Choose two.)

A. Pass-the-hash, using a stolen NTLM hash
B. Pass-the-ticket, using a stolen Kerberos ticket
C. RDP logon with the user's password
D. SSH logon with the user's password

> Correct answer: A and B Explanation: Correct: pass-the-hash authenticates with a hash and pass-the-ticket authenticates with a ticket, neither requiring the plaintext password. Why others are wrong: RDP and SSH logons with a password both require the plaintext password the tester does not have.

Q29. [pentest-690] A tester deletes a scheduled task the tester created, at the end of an authorized engagement, after confirming it is no longer needed. Is this covering tracks or cleanup?

A. Covering tracks, because it removes evidence of the tester's activity from the host
B. Persistence, because it maintains access
C. Cleanup, because it restores the pre-test state at the engagement's end
D. Lateral movement, because it affects another system

Correct answer: C Explanation: Correct: removing tester-created artifacts at the end of the engagement is cleanup, done openly and reported to the client. Why others are wrong: covering tracks hides activity during the engagement rather than restoring systems afterward; persistence maintains access rather than removing it; no new system is reached, so it is not lateral movement.

Q30. [pentest-745] For the Windows-focused phase of a CertCrack.com engagement, the team wants a collaborative command-and-control platform: browser-based, multi-operator, built on .NET, with implants it calls Grunts that the whole team can task and watch in real time. Which framework is this?

A. Covenant, the collaborative .NET C2 with Grunts
B. Metasploit, driven from its single-operator console
C. Netcat, opening raw listener connections
D. sshuttle, tunneling traffic through an SSH server

Correct answer: A Explanation: Correct: Covenant is the collaborative, .NET-based C2 framework — its Grunt implants are tasked from a web interface where several operators share sessions, data, and tasking, which is the model the team describes. Why others are wrong: Metasploit's sessions are powerful, but its working model is an operator-driven exploitation console, not a shared web C2 built on .NET Grunts; Netcat is a raw connection utility with no implant management, tasking, or operator collaboration; sshuttle only forwards traffic through SSH; it issues no commands to implants at all.