Mile2 Cybersecurity Institute

Certified Penetration Testing Engineer Accredited CPTE-A KSA Exam Blueprint (2026)

Element	Description
Credential Name	Certified Penetration Testing Engineer Accredited
Credential Abbreviation	CPTE-A
Document Type	Exam Blueprint
Revision Date	2026.04.23
Document Use	Public-facing exam content specification and controlled component of the CPTE-A Certification Scheme
Exam Delivery	Online proctored through the ProctorU platform

1. Purpose of the CPTE-A Certification

The Certified Penetration Testing Engineer Accredited certification validates the knowledge, skills, and abilities required to support authorized penetration testing activities across the penetration testing lifecycle. The certification emphasizes business and technical planning, information gathering, vulnerability assessment, operating system attacks, exploitation concepts, evasion techniques, network attacks, web application attacks, and mobile and IoT security considerations.

Successful candidates demonstrate an understanding of how penetration testing activities are authorized, planned, executed, documented, and reported to support organizational risk management and security improvement.

2. Candidate Profile

The CPTE-A certification is intended for individuals seeking to validate knowledge of authorized penetration testing concepts, tools, techniques, and reporting practices. Candidates may include penetration testers, ethical hackers, vulnerability assessment professionals, cybersecurity analysts, security consultants, systems administrators, network administrators, and IT professionals preparing for penetration testing responsibilities.

3. Experience Requirements

There are no minimum experience requirements to sit for the CPTE-A certification examination. Candidates from various technical and professional backgrounds may pursue the certification to demonstrate knowledge of authorized penetration testing concepts and practices.

4. Accreditation Statement

CPTE-A is an accredited certification aligned with the requirements of ANSI/ISO/IEC 17024 for personnel certification. The certification is maintained through defined examination development, review, and governance processes intended to support fairness, validity, reliability, and continued relevance to the cybersecurity profession.

5. Job Task Analysis and Blueprint Maintenance

Mile2 maintains the CPTE-A certification through periodic review of the job role, body of knowledge, examination domains, and exam content. Job Task Analysis activities are used to evaluate the tasks, knowledge, skills, and abilities

relevant to penetration testing professionals and to ensure that the examination remains aligned with current industry practices and candidate expectations.

This blueprint is reviewed and updated as needed to maintain alignment with the approved CPTE-A Certification Scheme, job role expectations, examination requirements, and applicable certification body policies.

6. Relationship to the CPTE-A Certification Scheme

This CPTE-A Exam Blueprint is a controlled component of the broader CPTE-A Certification Scheme. The blueprint identifies the examination domains, content areas, item distribution, and assessment structure used to evaluate candidate knowledge, skills, and abilities.

The CPTE-A Certification Scheme remains the controlling document for certification scope, eligibility, competence requirements, assessment methodology, certification decision rules, recertification requirements, appeals, complaints, suspension, withdrawal, code of conduct, impartiality, examination security, and scheme maintenance.

7. Examination Information

Exam Element	Requirement
Exam duration	2 hours
Number of scored items	100
Item format	Multiple choice
Passing score	63 out of 100 points
Exam language	English
Delivery platform	ProctorU

8. CPTE-A Examination Domains and Weights

Domain	Number of Questions	Weight
01. Business and Technical Logistics of Penetration Testing	20	20%
02. Information Gathering, Scanning, and Enumeration	12	12%
03. Vulnerability Assessment	6	6%
04. Hacking Operating Systems	22	22%
05. Exploitation Concepts and Frameworks	7	7%
06. Evasion Techniques	2	2%
07. Network Attacks	19	19%
08. Hacking Web Technologies	10	10%
09. Mobile and IoT Hacking	2	2%
Total	**100**	**100%**

9. CPTE-A Exam Blueprint Outline

Domain 1: Business and Technical Logistics of Penetration Testing

Weight: 20% | Number of Questions: 20

Candidates are expected to understand the business, legal, ethical, authorization, risk, methodology, lifecycle, and reporting requirements that govern authorized penetration testing engagements.

- Risk management standards
- Standards and regulatory requirements related to penetration testing
- Types of penetration tests
- Exploit and vulnerability lifecycle
- Penetration testing methodologies
- Non-disclosure agreements
- Code of ethics
- Service agreements and written authorization
- Rules of engagement and testing scope
- Penetration test report writing
- Risk analysis
- Executive summary development
- Risk response and treatment
- Business justification for penetration testing
- Communication of findings to technical and non-technical stakeholders

Domain 2: Information Gathering, Scanning, and Enumeration

Weight: 12% | Number of Questions: 12

Candidates are expected to understand reconnaissance, open-source intelligence, scanning, banner grabbing, service enumeration, TCP/IP fundamentals, and the use of common tools and techniques for identifying targets and services during authorized testing.

- Open-source intelligence
- WHOIS research
- DNS research and analysis
- Search engine and internet exposure research, including Shodan
- Google Hacking Database techniques

- TCP/IP fundamentals
- Port scanning concepts
- Scanning with Nmap
- Scanning with Hping
- Banner grabbing and banner grabbing tools
- Service enumeration
- Enumeration of SNMP, SMTP, LDAP, NTP, SMB, RPC, and NetBIOS
- Nmap scripting
- Scanning with PowerShell
- Enumeration with PowerShell
- Social engineering concepts, techniques, and tools within authorized scope

Domain 3: Vulnerability Assessment

Weight: 6% | Number of Questions: 6

Candidates are expected to understand vulnerability assessment standards, assessment types, vulnerability scoring, automated and manual identification methods, patch management, compliance scanning, and vulnerability reporting.

- Standards and regulatory requirements related to vulnerability assessment
- Types of vulnerability assessments
- CVE, NVD, and vulnerability scoring concepts
- Patch management
- Nmap scripting for vulnerability identification
- Automated vulnerability scans
- Manual vulnerability identification
- Compliance scans
- Compliance reports
- Interpreting vulnerability assessment reports

Domain 4: Hacking Operating Systems

Weight: 22% | Number of Questions: 22

Candidates are expected to understand operating system attack concepts, password attacks, malware, rootkits, malicious scripting, memory and overflow concepts, post-exploitation concerns, and common tools used in authorized testing environments.

- Malware concepts
- Rootkits
- Malicious PowerShell usage
- Password attacks
- Password salts
- Encryption concepts and encryption weaknesses
- Alternate Data Streams
- Steganography
- Clearing tracks
- Buffer overflow concepts
- USB-based attack concepts, including Rubber Ducky-style attacks
- Credential extraction concepts and tools such as Mimikatz
- Operating system privilege and access considerations
- Post-exploitation risks and defensive awareness

Domain 5: Exploitation Concepts and Frameworks

Weight: 7% | Number of Questions: 7

Candidates are expected to understand exploit frameworks, exploit components, manual and automated exploitation concepts, payloads, and auxiliary modules used in controlled and authorized testing activities.

- Exploit frameworks
- Exploit code sections
- Automated exploitation concepts, including Metasploit-style workflows
- Manual exploitation concepts
- Payloads
- Auxiliary modules
- Exploit selection considerations
- Validation and documentation of exploitation results

Domain 6: Evasion Techniques

Weight: 2% | Number of Questions: 2

Candidates are expected to understand common evasion and traffic manipulation concepts used to avoid or test detection mechanisms during authorized assessments.

- IP spoofing
- Tiny fragments
- Tunneling
- Honeypots
- Flooding
- Obfuscation
- Fragmentation
- TTL manipulation
- Session splicing
- Session desynchronization

Domain 7: Network Attacks

Weight: 19% | Number of Questions: 19

Candidates are expected to understand packet capture, sniffing, traffic analysis, protocol attacks, switching and routing attacks, DNS attacks, SSL/TLS attack concepts, and network-based attack considerations.

- Packet sniffing
- Stream reassembly
- Passive sniffing
- Active sniffing
- ARP and ARP attacks
- DNS attacks
- Routing attacks
- SSL/TLS attack concepts
- Voice over IP attacks
- Switch attacks
- Network traffic analysis
- Man-in-the-middle concepts
- Network attack documentation and reporting

Domain 8: Hacking Web Technologies

Weight: 10% | Number of Questions: 10

Candidates are expected to understand web application security concepts, common vulnerability categories, OWASP and CWE references, SQL injection, cross-site scripting, and common application attack patterns.

- OWASP concepts
- CWE concepts
- Web application attack surface
- SQL injection
- Blind SQL injection
- Union-based SQL injection
- Error-based SQL injection
- Stored cross-site scripting
- Reflected cross-site scripting
- DOM-based cross-site scripting
- Input validation and output encoding concepts
- Web application vulnerability documentation

Domain 9: Mobile and IoT Hacking

Weight: 2% | Number of Questions: 2

Candidates are expected to understand mobile and IoT security risks, platform considerations, constrained devices, Bluetooth attacks, testing considerations, standards, and hardening practices.

- Android security concepts
- iOS security concepts
- IoT security concepts
- Constrained devices
- IoT risks and threats
- Bluetooth attacks
- Penetration testing considerations for mobile devices
- Penetration testing considerations for IoT devices
- IoT standards
- Hardening mobile devices
- Hardening IoT devices

10. Candidate Policy References

Candidates should refer to Mile2 certification policies for additional requirements related to exam registration, identification, proctoring, retakes, accommodations, appeals, complaints, certification use, code of conduct, recertification, suspension, and withdrawal.

11. Document Control Statement

This blueprint is maintained by Mile2 Cybersecurity Institute as a controlled examination specification for the CPTE-A certification. Updates to this blueprint are reviewed to ensure continued alignment with the approved CPTE-A Certification Scheme, examination requirements, candidate profile, job role expectations, and applicable certification body policies.