Mile2 Cybersecurity Certifications – C)PTE KSA Exam Blueprint

About CPTE

A Certified Penetration Testing Engineer systematically evaluates all potential methods a hacker might use to infiltrate a data system. You have to go beyond what you learned as an Ethical Hacker because pen testing explores technical and non-technical ways of breaching security to gain access to a system. Our CPTE course is built on proven hands-on methods utilized by our international group of vulnerability consultants.

In this course, you will learn 5 Key Elements of Pen Testing: Information Gathering, Scanning, Enumeration, Exploitation, and Reporting. Plus, discover the latest vulnerabilities and the techniques malicious hackers are using to acquire and destroy data. Additionally, you will learn more about the business skills needed to identify protection opportunities, justify testing activities, and optimize security controls appropriate to the business needs in order to reduce business risk.

The CPTE Common Body of Knowledge (CBK®) covers a wide array of topics, ensuring that it remains relevant to all areas within the information security field. Successful candidates will demonstrate proficiency in the following eighteen domains:

- Business & Technical Logistics of Pen Testing
- Information Gathering
- Detecting Live Systems
- Banner Grabbing and Enumeration
- Automated Vulnerability Assessment
- Hacking an OS
- Advanced Assessment and Exploitation Techniques
- Evasion Techniques
- Hacking with PowerShell
- Networks and Sniffing
- Hacking Web Tech
- Mobile and IoT Hacking
- Report Writing Basics

Mile2 Cybersecurity Certifications – C)PTE KSA Exam Blueprint

Experience Requirements

There are no minimum requirements needed to become a Certified Penetration Testing Engineer (CPTE). Candidates can pursue the CPTE certification without prior experience. This allows individuals from various backgrounds and levels of expertise to gain the knowledge and skills required to effectively design, engineer, and manage the overall security posture of an organization. Whether you are new to the field or looking to enhance your existing skills, the CPTE certification is accessible to all aspiring information security professionals.

Accreditation

CPTE was the first credential in the field of information security to meet the stringent requirements of ANSI/ISO/IEC Standard 17024.

Job Task Analysis (JTA)

Mile2 is committed to ensuring the CPTE certification remains relevant to its members. Regularly conducted Job Task Analyses (JTA) systematically and critically assess the tasks performed by security professionals in the CPTE field. The findings from these analyses are used to update the examination, ensuring that candidates are evaluated on the most pertinent topics and responsibilities faced by today's information security professionals.

CPTE Examination Information

We use ProctorU to conduct our exams. ProctorU is an online proctoring service that allows candidates to take their exams securely from any location. This service ensures the integrity of the examination process by monitoring candidates through a combination of live proctors and advanced technology. By using ProctorU, we provide flexibility and convenience while maintaining high standards of security and compliance for our certification exams.

Length of exam	**2 hours**
Number of items	100
Item format	Multiple choice
Passing grade	63 out of 100 points
Exam language availability	English
Testing center	ProctorU Platform

Mile2 Cybersecurity Certifications – C)PTE KSA Exam Blueprint

C)PTE Examination Weights

Domains	Number of Questions	Average Weight
01. Business and Technical Logistics of Pen Testing	20	20%
02. Information Gathering	12	12%
03. Vulnerability assessment	6	6%
04. Hacking operating systems	22	22%
05. Exploits	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%
	100	**100%**

Mile2 Cybersecurity Certifications – C)PTE KSA Exam Blueprint

Domain 01: Business and Technical Logistics of Pen Testing

- Risk management standards
- Standards and regulations requirements for pentesting
- Types of pentests
- Exploit and Vulnerability Lifecycle
- Penetration Testing Methodologies
- NDA
- Code Of Ethics
- Service Agreement and Authorization
- Pentest Report writing
- Risk analysis
- Executive summary
- Risk response
-

Domain 02: Information Gathering

- OSINT
- WHOIS
- DNS
- Shodan
- GHDB
- Scanning with Nmap
- Scanning with Hping
- Social engineering techniques and tools
- understanding TCP/IP
- Port scan
- Banner grabbing & tools
- Service Enumeration
- SNMP, SMTP, LDAP, NTP, SMB, RPC, NETBIOS
- Nmap scripting
- Scanning with PowerShell
- Enumeration with PowerShell

Domain 03: Vulnerability assessment

- Standards and regulations requirements for VA
- Types of Vulnerability Assessments
- CVE – NVD – Risk scoring
- Patch management
- Nmap scripting
- Automated scans
- Manual vulnerability identification
- Compliance scans

- Compliance reports
- Understanding VA report

Domain 04: Hacking operating systems

- Malware
- Rootkits
- Malicious PowerShell usage
- Password attacks
- Password Salt
- Encryption & encryption weaknesses
- ADS
- Steganography
- Clearing tracks
- Buffer overflow
- Rubber ducky
- Mimikatz

Domain 05: Exploits

- Exploit framework
- Exploit code sections
- Automated exploitation (i.e Metasploit)
- Manual exploitation
- Payloads
- Auxiliaries

Domain 06: Evasion techniques

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

Domain 07: Network attacks

- Packet sniffing
- Stream reassembly
- Passive sniffing
- Active sniffing
- ARP & ARP attacks
- DNS attacks
- Routing attacks
- SSL/TLS attacks
- VOIP attacks
- Switch attacks

Domain 08: Hacking Web Technologies

- OWASP
- CWE
- SQLi
- Blind SQLi
- Union SQLi
- Error based SQLi
- Stored XSS
- Reflected XSS
- DOM Based XSS

Domain 09: Mobile and IoT Hacking

- Android
- IOS
- IoT
- Constrained Devices
- IoT Risks and Threats
- Bluetooth attacks
- Pentesting mobile devices
- Pentesting IoT devices
- IoT standards
- Hardening mobile devices
- Hardening IoT devices