Certified Cybersecurity Technician

Exam Blueprint

S. No.	Domain	Sub Domains	Topics	Domain %
1	**Information Security Threats and Attacks**	**Information Security Threats and Vulnerabilities**	Threats Sources	**26**
			Threat Actors/Agents	
			Malware and its Types	
			Vulnerabilities	
			Types of Vulnerabilities	
		Information Security Attacks	Information Security Attacks	
			Hacking Methodologies and Frameworks	
			Network-level Attacks	
			Application-level and OS-level Attacks	
			Social Engineering Attacks	
			Wireless Network-specific Attacks	
			IoT, OT, and Cloud Attacks	
			Cryptographic Attacks	
2	**Network Security Fundamentals**	**Network Security Fundamentals**	Information Security Fundamentals	**2**
			Network Security Fundamentals	
		Identification, Authentication, and Authorization	Access Control Principles, Terminologies, and Models	
			Identity and Access Management (IAM)	

3	**Network Security Controls**	**Network Security Controls - Administrative Controls**	Regulatory Frameworks, Laws, and Acts	**28**
			Information Security Governance and Compliance Program	
			Design and Develop Security Policies	
			Type of Security and Awareness Training	
		Network Security Controls - Physical Controls	Physical Security	
			Physical Security Controls	
			Workplace Security	
			Environmental Controls	
		Network Security Controls - Technical Controls	Network Security Protocols	
			Network Segmentation	
			Types of Firewalls and their Role	
			Types of IDS/IPS and their Role	
			Types of Honeypots	
			Types of Proxy Servers	
			Fundamentals of VPN	
			Other Network Security Controls	
			Load Balancing	
			Antivirus/Anti-malware Software	
		Network Security Assessment Techniques and Tools	Threat Hunting	
			Threat Intelligence Feeds and Sources	
			Vulnerability Assessment	
			Ethical Hacking	
			Penetration Testing	
			Configuration Management and Asset Management	
4	**Application Security and Cloud Computing**	**Application Security**	Secure Application Design and Architecture	**4**
			Software Security Standards, Models, and Frameworks	
			Secure Application, Development, Deployment, and Automation	

			Application Security Testing Techniques and Tools	
		Virtualization and Cloud Computing	Virtualization Essential Concepts and OS Virtualization Security	
			Cloud Computing Fundamentals	
			Cloud Security and Best Practices	
5	**Wireless Device Security**	**Wireless Network Security**	Wireless Network Fundamentals	**11**
			Wireless Network Encryption Mechanisms	
			Wireless Network Authentication Methods	
			Wireless Network Security Measures	
		Mobile Device Security	Mobile Device Connection Methods	
			Mobile Device Management Concepts	
			Common Mobile Usage Policies in Enterprises	
			Security Risks and Guidelines Associated with Enterprises Mobile Usage Policies	
			Enterprise-level Mobile Security Management Solutions	
			General Security Guidelines and Best Practices on Mobile Platforms	
		IoT and OT Security	IoT Devices, Application Areas, and Communication Models	
			Security in IoT-enabled Environments	
			OT Concepts, Devices, and Protocols	
			Security in OT-enabled Environments	
6	**Data Security**	**Cryptography**	Cryptographic Security Techniques	**10**
			Cryptographic Algorithms	
			Hash Functions and Cryptography Tools	
			PKI and Certificate Management Concepts	

			Other Applications of Cryptography	
		Data Security	Data Security	
			Data Security Controls	
			Data Backup, Retention, and Destruction	
			Data Loss Prevention	
7	**Network Monitoring and Analysis**	**Network Troubleshooting**	Network Troubleshooting	**11**
			Troubleshooting Basic Network Issues using Utilities and Tools	
		Network Traffic Monitoring	Network Traffic Monitoring	
			Baseline Traffic Signatures for Normal and Suspicious Network Traffic	
			Network Monitoring for Suspicious Traffic	
		Network Logs Monitoring and Analysis	Logging Concepts	
			Log Monitoring and Analysis on Windows Systems	
			Log Monitoring and Analysis on Linux	
			Log Management Tools	
8	**Incident and Risk Management**	**Incident Response**	Incident Response	**8**
			Role of First Responder in Incident Response	
			Incident Handling and Response Process	
		Computer Forensics	Computer Forensics	
			Digital Evidence	
			Roles and Responsibilities of a Forensic Investigator	
			Forensic Investigation Process	
			Forensic Investigation Phases	
			Digital Evidence Sources to Support Forensic Investigation	
			Collecting the Evidence	
			Securing the Evidence	

			Data Acquisition	
			Evidence Analysis	
		Business Continuity and Disaster Recovery	Business Continuity (BC) and Disaster Recovery (DR)	
			BC/DR Activities	
			Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)	
		Risk Management	Risk Management	
			Risk Management Phases	
			Risk Management Frameworks	