

TABLE OF CONTENTS

Module No.	Title	Page No.
1	Foundations of Cybersecurity and Advanced ThreatLandscape	01-50
	1.1 Evolution of Cybersecurity	
	1.2 Information Security Principles	
	1.3 Cyber Threat Intelligence	
	1.4 Cyber Kill Chain Framework	
	1.5 Attack Surface Analysis	
	1.6 Advanced Persistent Threats (APTs)	
	1.7 Nation-State and Cyber WarfareThreats	
	1.8 Future Cybersecurity Challenges	
2	Advanced Cyber Attacks and Exploitation Techniques	51-104
	2.1 Malware Evolution and Advanced Malware	
	2.2 Ransomware Architectures and Operations	
	2.3 Supply Chain Attacks	
	2.4 Fileless and Living-off-the-Land Attacks	
	2.5 Zero-Day Vulnerabilities and Exploits	
	2.6 Advanced Social Engineering Attacks	
	2.7 AI-Powered Cyber Attacks	
	2.8 Real-World Cyber Attack Case Studies	
3	CryptographicFoundations for Cybersecurity	105-163
	3.1 ClassicalCryptography Fundamentals	
	3.2 SymmetricEncryptionAlgorithms	
	3.3 Public Key Cryptography	
	3.4 Hash Functions and Message Authentication	
	3.5 Digital Signatures and PKI	
	3.6 Key Management Systems	
	3.7 Cryptanalysis Techniques	
	3.8 Security Limitations of ClassicalCryptography	
4	Quantum Computing Fundamentals for Security Professionals	164-217
	4.1 Introduction to Quantum Computing	
	4.2 Qubits and Quantum States	

	4.3	Quantum Gates and Circuits	
	4.4	Quantum Superposition and Entanglement	
	4.5	Quantum Algorithms Overview	
	4.6	Quantum Computing Platforms	
	4.7	Quantum Programming Concepts	
	4.8	Quantum Threats to Cybersecurity	
5		Quantum Attacks on Classical Cryptography	218-274
	5.1	Quantum Threat Model	
	5.2	Shor's Algorithm and RSA Vulnerabilities	
	5.3	Quantum Attacks on ECC	
	5.4	Grover's Algorithm and Symmetric Cryptography	
	5.5	Quantum Cryptanalysis Techniques	
	5.6	Harvest Now, Decrypt Later (HNDL)	
	5.7	Impact on Internet Security Infrastructure	
	5.8	Quantum Risk Assessment	
6		Quantum Cryptography and Quantum Security	275-335
	6.1	Principles of Quantum Cryptography	
	6.2	Quantum Key Distribution (QKD)	
	6.3	BB84 and E91 Protocols	
	6.4	Quantum Random Number Generation	
	6.5	Quantum Secure Communication Networks	
	6.6	Quantum Authentication Techniques	
	6.7	Quantum Internet Concepts	
	6.8	Practical Challenges of Quantum Security	
7		Post-Quantum Cryptography (PQC)	336-393
	7.1	Introduction to PQC	
	7.2	NIST PQC Standardization Process	
	7.3	Lattice-Based Cryptography	
	7.4	Code-Based Cryptography	
	7.5	Multivariate Cryptography	
	7.6	Hash-Based Signatures	
	7.7	Isogeny-Based Cryptography Concepts	
	7.8	PQC Security Analysis	