Topic	Sub-Topic	Sub-Sub-Topic
Introduction to Cyber Security		
	What is Cyber Security? Statistics and Inferences	
	Need of Cyber Security	
	Common Terminologies	
	Career and Growth	
		Hacking as a Career
		Domains of Cyber Security
		Job Opportunities
	Threats to the Cyber World	
		Non-IT Threats
		IT Threats
	Hacking Phases	
		Reconnaissance
		Scanning
		Gaining Access
		Maintaining Access
		Clearing Tracks
Footprinting		
	Introduction	
	Need of Footprinting	
	Targets of Footprinting	
		IT Infrastructure
		Organizational Infrastructure
	Footprinting Techniques	
		Footprinting using search engine
		Footprinting using Google
		Footprinting using Shodan
		Footprinting Using WHOIS
		Footprinting Using DNS Queries
		Footprinting through Social Engineering
		Footprinting through command-line utilities
		Footprinting using Tools
		Footprinting using Source Code Examination
		Footprinting individuals
Network Scanning (Probing)		
	Introduction	
	Types of scanning	
	Objectives of scanning techniques	
		Scanning for Live Single Systems
		Scanning for Live Multiple Systems

Topic	Sub-Topic	Sub-Sub-Topic
	Port Scanning Techniques	
		TCP Connect / Open Scan,Half Open Scan,
		Strobe Scan, FIN | Null | Xmas Tree Scan,
		FTP Bounce Scan, UDP Scan
	Port scanner tools	
		Hping, NetScan Tool,
		Strobe (Super optimized TCP port surveyor)
		Scanning for System Information
	Vulnerability Scanning	
		Vulnerability Scanner Tools
	Determining Network Architecture,	
		Tools for mapping Network Architecture
	Conclusion	
Web Application Security		
	Basics of Web Application	
		Architecture of Web Applications
		Need and use of Web Applications
	Passive Information Gathering	
		Google Hacking
		Whois Lookup
		DNS Interrogation
	Active Information Gathering	
		1.Port Scanning
		2.Service Scanning
		3.OS Fingerprinting
		4.Enumerating Web Application framework
		5.Web App. Content Discovery
	Check Authentication Mechanism	
		Username
		Passwords
		Session
	Vulnerabilities in Authorization Mechanism	
		Directory Traversal (horizontal and vertical directory)
		Bypassing Authorisation Schema
		Privilege Escalation
		Insecure Direct Object reference
	Injection Attacks	
		Web Script Injection
		SMTP Injection
		SQL Injection

Topic	Sub-Topic	Sub-Sub-Topic
		LDAP Injection
		XPath Injection
		Command Injection Attack
	Web Application Vulnerabilities and its Defenses	
		Insufficient Transport Layer Protection
		Security Misconfiguration
		Insecure Cryptographic Storage
		Buffer Overflow
		Cross Site Request Forgery attack (CSRF)
		Cross Site Scripting (XSS)
		Redirection Attack
		Improper Error Handling
		Information Leakage
		Failure to Restrict URL Access
		Security Management Exploits
		Malicious File Execution
		Captcha Attacks
		Authentication Hijacking
		Network Access Attacks
		Cookie Snooping
	Web Application Security Scanner	
		Commercial Tools
		Software-as-a-Service Providers
		Free / Open Source Tools
		List of Tools
Injection		
	SQL Injection	
		Types of SQL injection
		SQL Injection tools
		HTTP GET and POST request protocols
		Basic queries of SQL injection
	Code Injection	
		Types of Code Injection
		Vulnerability of Code Injection
		Prevention of Code Injection
	File Inclusion Vulnerability	
		Types of File Inclusion
	Command Injection	
		How to perform command injection?

Topic	Sub-Topic	Sub-Sub-Topic
	How to prevent SQL Injection	
Pentesting		
	Penetration testing	
	Vulnerability Assessment vs Penetration testing	
	Importance of Penetration testing	
	Advantages of Pentesting	
	Methods of Pentesting	
		Black Box testing
		White Box testing
		Grey Box testing
		Bug Bounty
	Penetration Testing Execution Standard	
		OWASP Testing Guide
		NIST SP800-115
		New PCI DSS Guidance
		FedRAMP
		PTES
	Stages of Pentesting	
		1.Footprinting
		2. Scanning
		3. Enumeration
		4. Performing Penetration Tests
		Web Application Pentesting
		OWASP Top 10 for Mobile
		Servers
		Network Penetration Testing
	Reporting	
		Structure of a Report