Blockchain Security in Cyber Security – Course Content

Target Roles

- Blockchain Security Analyst
- Smart Contract Auditor
- Web3 Security Engineer
- Cyber Security Analyst (Blockchain)
- Bug Bounty Hunter (Web3)

Module 1: Fundamentals of Blockchain Technology

- What is Blockchain
- History & Evolution of Blockchain
- Centralized vs Decentralized Systems
- Distributed Ledger Technology (DLT)
- Blockchain Components
- Public, Private & Consortium Blockchains
- Blockchain Use Cases (Finance, Supply Chain, Healthcare)

Module 2: Blockchain Architecture & Cryptography

- Blocks, Transactions & Hashing
- Merkle Trees
- Digital Signatures
- Public & Private Key Cryptography
- Elliptic Curve Cryptography (ECC)
- Wallet Types & Security
- Key Management Best Practices

Module 3: Consensus Mechanisms & Security

- Proof of Work (PoW)

- Proof of Stake (PoS)
- Delegated PoS (DPoS)
- Proof of Authority (PoA)
- Byzantine Fault Tolerance (BFT)
- Consensus Attack Vectors
- Security Trade-offs in Consensus Models

Module 4: Blockchain Network & Infrastructure Security

- Node Architecture
- Peer-to-Peer (P2P) Networks
- RPC Endpoints Security
- Blockchain Network Attacks
- Sybil Attacks
- Eclipse Attacks
- Routing Attacks
- DoS/DDoS on Blockchain Nodes

Module 5: Smart Contracts Fundamentals

- What are Smart Contracts
- Smart Contract Lifecycle
- Ethereum Virtual Machine (EVM)
- Solidity Basics
- Smart Contract Deployment
- Gas, Transactions & Events
- Secure Smart Contract Design Principles

Module 6: Smart Contract Vulnerabilities (Core Module)

- Re-Entrancy Attacks

- Integer Overflow & Underflow
- Access Control Issues
- Front-Running & MEV Attacks
- Timestamp Dependence
- Delegatecall Vulnerabilities
- Denial of Service (DoS)
- Business Logic Flaws
- Case Studies (DAO Hack, Parity Wallet Hack)

Module 7: Web3 & DApp Security

- Web3 Architecture
- DApp Components
- Frontend + Smart Contract Interaction
- Web3.js & Ethers.js Security Issues
- Wallet Injection Attacks
- Phishing & Fake DApps
- API & Backend Security for DApps

Module 8: Blockchain Threat Modeling & Attack Surface

- Blockchain Attack Surface
- STRIDE for Blockchain
- Threat Modeling for Smart Contracts
- Attack Trees
- Risk Assessment & Impact Analysis
- Real-World Blockchain Breach Analysis

Module 9: Blockchain Penetration Testing & Auditing

- Blockchain Security Testing Methodology

- Manual Smart Contract Review
- Automated Auditing Tools
- Static vs Dynamic Analysis
- Gas Optimization Security
- Audit Reporting & Risk Rating
- Client-ready Audit Report Writing

Tools Covered:

- Slither
- Mythril
- Oyente
- Remix IDE
- Hardhat
- Foundry

Module 10: Blockchain Wallet & Exchange Security

- Hot vs Cold Wallet Security
- Custodial vs Non-Custodial Wallets
- Hardware Wallet Attacks
- Exchange Architecture
- Exchange Hacks Case Studies
- Secure Key Storage (HSMs)
- Multi-Sig Wallet Security

Module 11: DeFi Security

- DeFi Ecosystem Overview
- Liquidity Pools & AMMs
- Flash Loan Attacks
- Oracle Manipulation Attacks

- Rug Pulls & Scam Detection
- Governance Attacks
- DeFi Security Best Practices

Module 12: NFT & Metaverse Security

- NFT Architecture
- NFT Smart Contract Risks
- NFT Marketplace Vulnerabilities
- Fake NFT & Phishing Scams
- Royalty Manipulation
- Metaverse Security Challenges

Module 13: Blockchain Forensics & Incident Response

- Blockchain Transaction Tracing
- On-Chain Analysis
- Address Attribution
- Incident Response for Blockchain Breaches
- Evidence Collection
- Legal & Compliance Considerations

Tools:

- Etherscan
- Chainalysis (Conceptual)
- Blockchain Explorers

Module 14: Cloud & Infrastructure Security for Blockchain

- Blockchain on Cloud (AWS, Azure, GCP)
- Container & Kubernetes Security
- CI/CD Security for Smart Contracts

- Secrets Management
- Secure Node Deployment
- Monitoring & Logging

Module 15: AI in Blockchain Security (High-Demand Module)

- AI for Smart Contract Vulnerability Detection
- Machine Learning for Fraud Detection
- Anomaly Detection in Blockchain Networks
- AI-based Transaction Analysis
- LLMs for Smart Contract Review
- Limitations of AI in Blockchain Security

Module 16: Bug Bounty & Real-World Blockchain Attacks

- Web3 Bug Bounty Platforms
- Responsible Disclosure
- Writing High-Impact Bug Reports
- Finding Critical Vulnerabilities
- Live Attack Scenarios
- Red Team vs Blue Team in Web3

Module 17: Governance, Compliance & Regulations

- Blockchain Regulations (Global Overview)
- AML & KYC in Blockchain
- Smart Contract Legal Risks
- Data Privacy & Blockchain
- Compliance Challenges

Module 18: Career Preparation & Certification Roadmap

- Blockchain Security Job Roles
- Resume & GitHub Portfolio
- Interview Questions
- Freelancing in Web3 Security
- Certifications Roadmap
- Industry Expectations

Module 19: Capstone Project

- Smart Contract Security Audit Project
- DeFi Vulnerability Assessment
- Blockchain Penetration Testing Report
- Real-World Case Study Presentation

Course Outcomes

✓ In-depth Blockchain & Web3 Security Knowledge
✓ Hands-on Smart Contract Auditing Skills
✓ Job-ready for Blockchain Security Roles
✓ Bug Bounty & Freelancing Ready