Teaching Plan for UNIT-I: Security Issues

Day 1: Blockchain & EVM Security (3 Hours)

1️⃣ Blockchain Security Issues (60 min)

- What makes blockchain secure?
- **Common threats in blockchain networks**
  - 51% Attack
  - Sybil Attack
  - Eclipse Attack
- **Consensus Mechanism Vulnerabilities**
  - PoW vs. PoS security issues
  - Mining pool centralization risks

2️⃣ EVM & Smart Contract Execution Risks (60 min)

- **What is the Ethereum Virtual Machine (EVM)?**
- **EVM Bytecode Vulnerabilities**
  - Gas Limit Exploits
  - Storage Collision
  - Unchecked Call Return Values
- **Trusted Execution Environments (TEE)**
  - How TEEs improve blockchain security
  - Limitations & concerns with TEEs

3️⃣ Real-Life Blockchain Security Attacks (60 min)

- **Bitcoin Gold 51% Attack (2018) – $18M Stolen** *(Related to 51% Attack)*
- **Ethereum Classic 51% Attack (2020) – $5.6M Double Spend Attack** *(Demonstrates Consensus Exploits)*
- **BZX Protocol Hack (2020) – Oracle Price Manipulation** *(Shows risks in smart contract dependencies)*

Day 2: Smart Contract & Solidity Security (3 Hours)

1️⃣ Solidity & Smart Contract Vulnerabilities (60 min)

- What is Solidity?

- Why smart contracts are vulnerable
- Overview of major smart contract risks

2️⃣Common Solidity Security Issues (75 min)

- **Reentrancy Attack** *(With simple explanation & example)*
- **Integer Overflow & Underflow** *(Errors due to improper number calculations)*
- **Denial of Service (DoS) Attack** *(How attackers block contract execution)*
- **Default Visibility Issues** *(Why functions should not be public by default)*
- **Randomness Issues in Smart Contracts** *(Why generating random numbers is risky in Solidity)*

3️⃣Real-Life Smart Contract Hacks (45 min)

- **Bancor Vulnerability (2018) – $23M loss** *(Related to Default Visibility Issues & Reentrancy Attack)*
- **Fomo3D Game Exploit (2018) – Ethereum Locked in a Ponzi Scheme** *(Demonstrates Randomness Issues in Smart Contracts)*
- **PancakeSwap & Cream Finance DNS Hijacking (2021) – Phishing Attack Exploiting Visibility & Access Issues** *(Related to Default Visibility & External Dependencies)*

ALTERNATIVE

Day 1: Introduction to Blockchain Security Issues (2 Hours)

1️⃣Introduction to Security in Blockchain (20 min)

- Why is security important in blockchain?
- How blockchain is considered secure but not 100% foolproof
- Examples of security incidents in blockchain

2️⃣Blockchain-Related Security Issues (40 min)

- **51% Attack** (How miners can manipulate blockchain)
- **Sybil Attack** (Fake identities disrupting networks)
- **Eclipse Attack** (Isolating a node from the network)
- **Double-Spending Attack** (How people try to spend the same cryptocurrency twice)

3️⃣ Case Studies of Blockchain Attacks (30 min)

- **Bitcoin Gold 51% Attack (2018)**
- **Ethereum Classic 51% Attack (2020)**
- **Real-world losses due to blockchain attacks**

4️⃣ Defense Mechanisms (30 min)

- How blockchains defend against Sybil attacks (PoW, PoS)
- Network monitoring & early attack detection
- Limitations of existing security models

Day 2: Smart Contract Security & Solidity Issues (2 Hours)

1️⃣ Solidity & Smart Contract Vulnerabilities (30 min)

- What is Solidity?
- Why smart contracts are vulnerable
- Overview of major smart contract risks

2️⃣ Common Solidity Security Issues (45 min)

- Reentrancy Attack (Explained in simple terms with example)
- Integer Overflow & Underflow (Errors due to improper number calculations)
- Denial of Service (DoS) Attack (How attackers block contract execution)
- Default Visibility Issues (Why functions should not be public by default)
- Randomness Issues in Smart Contracts

3️⃣ Real-Life Smart Contract Hacks (45 min)

- Bancor Vulnerability (2018) – $23M loss *(Related to Default Visibility Issues & Reentrancy Attack)*
- Fomo3D Game Exploit (2018) – Ethereum Locked in a Ponzi Scheme *(Demonstrates Randomness Issues in Smart Contracts)*
- PancakeSwap & Cream Finance DNS Hijacking (2021) – Phishing Attack Exploiting Visibility & Access Issues *(Related to Default Visibility & External Dependencies)*

Day 3: EVM Bytecode, TEEs & Advanced Security Issues (2 Hours)

1️⃣ EVM Bytecode Security Issues (40 min)

- What is Ethereum Virtual Machine (EVM)?
- How EVM executes smart contracts
- **Attack Vectors:**
    - Bytecode manipulation
    - Self-destruct function exploitation
    - Front-running attacks

2️⃣ Trusted Execution Environments (TEEs) (40 min)

- What are TEEs?
- How TEEs protect blockchain applications
- Limitations of TEEs

3️⃣ Advanced Threats & Future of Blockchain Security (40 min)

- **Cross-Chain Attacks** (Bridges & security flaws)
- **Privacy & Confidentiality Issues in Blockchain**
- **Quantum Computing & Blockchain Security**
- **Future Research & Trends in Securing Blockchain**

Outcome of This Unit:

By the end of **6 hours**, students will:
✅ Understand major security issues in blockchain.
✅ Learn about **real-world attacks** & their impact.
✅ Gain insights into Solidity vulnerabilities & smart contract security.
✅ Be aware of **emerging threats** like quantum computing & cross-chain attacks.