Teaching Plan for UNIT-II : Security tools for smart Contracts

Day 1: Introduction to Smart Contract Security Tools (2 Hours)

1️⃣ Why Do We Need Security Tools? (30 min)

- Importance of smart contract security
- Common security risks in smart contracts
- Why manual auditing is not enough?
- How security tools automate vulnerability detection

2️⃣ Overview of Smart Contract Security Tools (30 min)

- Categories of security tools:
    - **Static Analysis Tools** (Analyze code without execution)
    - **Dynamic Analysis Tools** (Test contracts in a simulated environment)
    - **Symbolic Execution Tools** (Find logical vulnerabilities)
- Introduction to the tools covered in this unit

3️⃣ Ovente & Securify – Static Analysis Tools (60 min)

Ovente

- Working mechanism
- Advantages: **Fast detection, simple UI, lightweight**
- Disadvantages: **Limited detection capabilities, false positives**

Securify

- How it scans for security vulnerabilities
- Advantages: **Comprehensive rule-based analysis, checks Solidity best practices**
- Disadvantages: **High false positives, requires manual verification**

Day 2: Maian & Manticore – Advanced Security Tools (2 Hours)

1️⃣ Maian – Smart Contract Vulnerability Detection (60 min)

- How Maian detects vulnerabilities
- **Types of vulnerabilities it detects**:
    - **Suicidal contracts** (Self-destruct risks)
    - **Prodigal contracts** (Unintended fund loss)
    - **Greedy contracts** (Locked funds)
- **Advantages**: High accuracy, effective for self-destruct vulnerabilities
- **Disadvantages**: Cannot detect logic errors

2️⃣ Manticore – Symbolic Execution Tool (60 min)

- How Manticore analyzes smart contracts
- **Advantages**:
    - Finds execution paths leading to vulnerabilities
    - Works for both Ethereum & binary applications
- **Disadvantages**:
    - **Slow execution**, not ideal for large contracts
    - **Resource-intensive** (requires powerful hardware)

Day 3: Mythril, SmartCheck, and Verx – Comprehensive Analysis Tools (2 Hours)

1️⃣ Mythril – A Popular Security Analysis Tool (60 min)

- How Mythril uses symbolic execution & taint analysis
- **Advantages**:
    - Detects many security flaws (reentrancy, overflows, uninitialized storage)
    - **Open-source & widely used**
- **Disadvantages**:
    - **False positives**, requires manual verification
    - **Resource-intensive** for large contracts

2️⃣ SmartCheck – Detecting Solidity Vulnerabilities (30 min)

- How SmartCheck scans Solidity code
- **Advantages**:
    - **Beginner-friendly**, integrates with IDEs
    - Detects **code smells** and security issues
- **Disadvantages**:
    - Cannot detect runtime vulnerabilities
    - Misses complex logic-based issues

3️⃣ Verx – Advanced Formal Verification (30 min)

- What is **formal verification**, and how does Verx use it?
- **Advantages**:
    - Detects vulnerabilities at a mathematical level
    - Highly accurate
- **Disadvantages**:
    - Complex to use
    - Requires deep technical understanding

Day 4: Secure Key Management & Quantum-Resilient Keys (2 Hours)

1️⃣ Secure Key Management in Blockchain (60 min)

- Why is **key security critical** in blockchain?
- **Types of keys** in smart contracts (private keys, session keys)
- **Key management best practices**:
    - Hardware security modules (HSM)
    - Multi-signature wallets
    - Threshold cryptography
- **Challenges in secure key storage**

2️⃣ Quantum Resilient Keys – The Future of Blockchain Security (60 min)

- What is **Quantum Computing**?
- How can **quantum computers break blockchain encryption**?
- Introduction to **Quantum-Resilient Cryptography**
    - Post-quantum cryptographic algorithms (Lattice-based, Hash-based cryptography)
    - Blockchain projects working on quantum resistance (Bitcoin, Ethereum 2.0)
- Future security risks & how developers can prepare

Final Thoughts

This plan ensures:
✅ **All topics are covered with a structured flow**
✅ **Each session builds on the previous one**

✅ **Tools are explained along with their advantages/disadvantages**
✅ **Secure key management & quantum security is given sufficient focus**

This structure provides **a balanced, comprehensive, and engaging** theory-based teaching plan for **Unit II**. 🚀