

Course 1: Web Application

- **Fundamentals Overview**
 - Networking /Linux
 - Understanding OSI Layer
 - HTML/Javascript
 - Default Ports and services – Nmap
 - Encryption/Hashing
 - Understanding CVE/NIST Databases
 - Vulnerability Assessment vs Penetration Testing
 - Understanding Basic Architectures (3-tier)
- **Web Security Concepts**
 - Overview of OWASP Top 10
 - Cross Site Scripting (XSS)
 - SQL injection
 - Authentication/Access control
 - XML External Entity (XXE)
 - Insecure Direct Object Reference(IDOR)
 - Parameter tampering (Business logic bypass)
 - Cross Site Request Forgery (CSRF)
 - Server Side Request Forgery (SSRF)
 - Malicious File upload
 - Session management
 - CVE Database and CVSS scoring
- **Penetration Test Approach**
 - How to Approach a penetration Test
 - Understanding Scope
 - Performing the Assessment (Black/Grey/White Box)
 - Assessment Methodology
 - Documenting Findings/Remediations
 - Sample Report Template Creation

- **Hands-On Labs**
 - Setting Up Tools
 - Demo of vulnerabilities using vulnerable applications.
 - Using Automated Tools (ZAP)
- **Tools**
 - Nmap - Port scanner
 - Burpsuite – Proxy
 - Wireshark - Packet analyser

Course 2: Network Vulnerability Scanning

- **Port Scanning**
 - Scanning Ports and Services
 - Identifying different software versions
- **Vulnerability Scan**
 - Identifying vulnerabilities - Manual
 - Automated Scanning - Nessus
 - Configuring the Scan
 - Generating Report
- **Exploitation**
 - Exploitation of Identified Vulnerabilities
 - Metasploit Demo
- **Tools**
 - Nessus - Vulnerability Scanner
 - Metasploit - Exploitation

Course 3: Thick Client

- **Fundamentals Overview**
 - Thick Client Overview
 - Architecture Types in Thick Client
 - Examples of Thick Client Applications
- **Thick Client Security Concepts**
 - Overview of OWASP Top 10 - Desktop Security
 - Reverse Engineering Thick client App

- Broken Authentication and Session management
- Sensitive Data Exposure
- Weak Cryptography
- Security Misconfiguration
- Insecure Communications
- Poor Code Quality
- Components with Known vulnerabilities
- **Hands-On Labs**
 - Setting Up Tools
 - Demo of vulnerabilities using vulnerable applications.
- **Tools**
 - Echo Mirage - Proxy
 - Process Hacker/Process Monitor - Analyze processes
 - Jd-GUI/dnSpy - Reverse Engineering

Course 4: API

- **Fundamentals Overview**
 - Overview of APIs
 - REST vs SOAP APIs
 - Understanding Different HTTP Methods
- **API Security Concepts**
 - Overview of OWASP Top 10 - API Security Risks
 - Broken Authentication
 - Broken Object Level Authroization
 - Sensitive Information disclosure
 - Security Misconfigurations
- **Hands-On Labs**
 - Setting Up Tools
 - Demo of vulnerabilities using vulnerable API
- **Tools**
 - Rest Client Plugin
 - Postman - API Management

- Burp Suite - Proxy

Course 5: Android Mobile Security

- **Fundamentals Overview**

- Android Architecture Overview
- Android Security Model
- Android Tool Kit
- Understanding Rooting

- **Android Security Concepts**

- Overview of OWASP Top 10 - Mobile Security
- Reverse Engineering Android App
- Broken Authentication
- Exploiting Activities and Content Providers
- Weak Cryptography
- Insecure Data Storage
- Insecure Communications

- **Hands-On Labs**

- Setting Up Tools
- Demo of vulnerabilities using vulnerable mobile applications.

- **Tools**

- Android Studio/Genemotion -Android Emulators
- Appie - Android security tools framework
- Apktool, ADB - Android platform tool
- Drozer - Exploitation Framework
- MobSF - Automated Scanner for APK