ETHICAL HACKING IN FINANCIAL MARKETS

(Creating Best of Minds)

Certificate in Ethical Hacking in Financial Markets

Course Code: BF_IP_I_0004/25

Duration: 40 Hours

Delivery Format: Hybrid

Target Audience:

- Freshers: Ideal for individuals new to cybersecurity who want to learn how to secure financial systems. No prior ethical hacking experience is required, though basic IT knowledge is helpful.
- Professionals: Designed for IT, cybersecurity, and finance professionals looking to specialize in ethical hacking for financial markets. It enhances skills in penetration testing, vulnerability assessments, and security audits.

Program Objectives:

- Understand the principles of ethical hacking in the context of financial markets.
- Learn the techniques used for penetration testing in financial systems.
- Perform vulnerability assessments to identify weaknesses in financial software and infrastructure.
- Conduct security audits to evaluate the security posture of financial organizations.

- Apply ethical hacking techniques to mitigate risks and protect sensitive financial data.
- Develop a proactive approach to cybersecurity in financial environments.

Detailed Syllabus

Module 1: Introduction to Ethical Hacking in Financial Markets

Objective: Introduce the fundamentals of ethical hacking and its importance in the financial sector.

Topics:

- Basics of ethical hacking
- Importance of cybersecurity in financial markets
- Overview of financial systems and their vulnerabilities
- Legal and ethical considerations

Activities:

- Discussions on the unique cybersecurity challenges in financial markets.
- Case studies of high-profile cyberattacks on financial institutions.

Assessments:

- Quiz on ethical hacking concepts and financial market terminology.
- Short report on the ethical and legal aspects of hacking in finance.

Module 2: Penetration Testing in Financial Systems

Objective: Learn and apply penetration testing techniques to assess the security of financial systems.

Topics:

- Understanding penetration testing methodologies
- Tools and techniques for financial penetration testing
- Hands-on exercises in penetration testing financial applications
- Case studies and analysis of real-world attacks in finance

Activities:

- Hands-on labs simulating penetration tests on financial applications.
- Group exercises to identify and exploit vulnerabilities in sample financial systems.

Assessments:

- Practical assessment: Conducting a penetration test on a simulated financial platform.
- Report detailing the findings and recommendations from a penetration test.

Module 3: Vulnerability Assessment and Risk Management

Objective: Learn to identify, assess, and manage vulnerabilities in financial systems.

Topics:

- Identifying vulnerabilities in financial software and infrastructure
- Tools for vulnerability scanning and analysis
- Risk assessment and prioritization
- Remediation strategies for financial systems

Activities:

- Using vulnerability scanning tools to analyze financial applications.
- Developing risk management plans based on vulnerability assessments.

Assessments:

- Assignment on conducting a vulnerability assessment and proposing remediation strategies.
- Presentation on risk management frameworks for financial systems.

Module 4: Security Audits in the Financial Sector

Objective: Develop skills in performing security audits to ensure compliance and identify security gaps.

Topics:

- Performing security audits in financial institutions
- Regulatory standards and frameworks (e.g., PCI DSS, GDPR)
- Conducting compliance assessments
- Creating audit reports and recommendations

Activities:

- Simulating security audits of financial systems and processes.
- Analyzing compliance requirements and developing audit checklists.

Assessments:

- Assignment: Creating a security audit plan for a financial institution.
- Report on the findings and recommendations from a security audit.

Module 5: Advanced Ethical Hacking Techniques for Financial Systems

Objective: Explore advanced ethical hacking techniques and countermeasures specific to financial systems.

Topics:

- Exploiting vulnerabilities in financial applications
- Securing web applications, databases, and networks in finance
- Countermeasures and best practices to prevent exploitation
- Incident response and handling security breaches

Activities:

- Advanced hands-on exercises simulating complex attacks on financial systems.
- Developing incident response plans and recovery strategies.

Assessments:

- Practical assessment: Applying advanced ethical hacking techniques in a simulated financial environment.
- Case study analysis of a major cyberattack on a financial institution.