Session11 Assignment(Ethical Hacking Principles & Professional Conduct)

Ethical Hacking Policy

Organization**: Amazon**

Purpose

This policy establishes guidelines for ethical hacking activities conducted within Amazon to identify and mitigate potential vulnerabilities while ensuring the security of Amazon's systems, customer data, and intellectual property. It defines the scope of activities, permissions, confidentiality obligations, and reporting requirements to align with Amazon's security and compliance standards.

Scope of Ethical Hacking Activities

1. Authorized Systems:

-Ethical hacking activities are limited to systems, networks, applications, and data owned, managed, or explicitly authorized by Amazon. Examples include:

-Internal corporate networks and systems.

-Customer-facing platforms (e.g., AWS, Amazon.com).

-Amazon's mobile and web applications.

-Cloud infrastructure and third-party integrations (with explicit approval).

2. Types of Tests:

-Vulnerability Scanning: Identification of weaknesses in software, systems, and networks.

-Penetration Testing: Controlled exploitation of vulnerabilities to evaluate risk.

-Social Engineering: Testing employee awareness through phishing or other techniques.

-Network Security Testing: Assessing internal and external networks for threats.

-Application Security Testing: Analyzing code, APIs, and application behavior for security issues.

3. Exclusions:

-Testing of systems outside the authorized scope or testing without explicit approval is prohibited.

Requirements for Obtaining Permission

1. Rules of Engagement (ROE):

-Approved tools and techniques.

-Specific testing timelines.

-Reporting protocols and escalation procedures.

2. Authorization Process:

-Ethical hackers must obtain written approval from Amazon’s Security and Compliance team before conducting any tests.

-A formal agreement, including the ROE, must be signed by all parties involved.

-Unauthorized access or testing is strictly prohibited.

3. Accountability:

-A designated point of contact must oversee testing activities.

-Ethical hackers are required to document their methodologies and adhere to Amazon’s security policies.

Confidentiality Obligations for Ethical Hackers

1. Data Protection:

-Ethical hackers must safeguard sensitive information encountered during testing.

-No customer data, proprietary information, or sensitive material may be copied, stored, or shared outside authorized environments.

2. Non-Disclosure Agreement (NDA):

-All ethical hackers must sign an NDA before commencing testing activities.

-Unauthorized disclosure of findings, tools, or methodologies is prohibited.

3. Handling Test Results:

-All test results, including vulnerabilities, must be stored securely .

-Only authorized personnel may access test findings.

Reporting Procedures for Findings and Vulnerabilities

1. Immediate Reporting:

-Critical vulnerabilities or exploits discovered during testing must be reported immediately to the designated security contact.

2. Detailed Reports:

-Ethical hackers must produce a comprehensive report at the end of the testing, including:

-Identified vulnerabilities, their severity levels, and impacted systems.

-Proof-of-concept for vulnerabilities (if applicable).

-Recommendations for remediation and mitigation steps.

3. Follow-Up Actions:

-A review meeting must be conducted with stakeholders to discuss findings.

-Ethical hackers must verify the implementation of remediation measures.

-Compliance and Consequences

-Ethical hackers must adhere to this policy and all applicable laws and regulations.

-Violations may result in termination of engagement, legal action, or other consequences as deemed appropriate by Amazon.