CMR INSTITUTE OF TECHNOLOGY

UGC Autonomous

(Approved by AICTE, Permanently Affiliated to JNTUH, and Accredited by NBA and NAAC with A+ Grade)

Kandlakoya (V), Medchal Road, Hyderabad-501 401

COURSE: IV - B.Tech / M.Tech / MBA I SEM

Date of Examination	: 25-04-2025
Regulation	: R18
Regular / Supply	: Supply
Branch	: CSE
Subject Name	: Ethical Hacking
Subject Code	: CS-PC 414
Name of the Moderator	: Kolari Rampriya.
Moderator's Emp. Id & Mobile No	: 15008 & 8978944747.

Part A

1. Who is considered a hacker in the context of ethical hacking?

A. In the context of ethical hacking, a hacker is typically someone who uses their technical skills to identify and fix security vulnerabilities in computer systems, networks or applications. Ethical hacking, hacker are also known as white hat hackers, operate with permission from the organization they are testing and aim to improve security rather than exploit weaknesses for malicious purpose.

2. What is the first step in the ethical hacking framework?

A. The first step in the ethical hacking framework is typically planning and Reconnaissance. This phase involves gathering information about the target system or organization to understand its structure, technology and potential vulnerabilities.

3. Mention one business challenge related to ethical hacking?

A. One significant business challenge related to ethical hacking is the potential for system interruptions or unintended consequences during testing. Ethical hacking, while intended to identify vulnerabilities, can sometimes disrupt normal operations if not carefully planned and executed.

4. What is the primary purpose of security policy?

A. The primary purpose of security policy is to establish rules and guidelines for protecting an organization's assets, including data, systems and physical infrastructure, from unauthorized

access, use disclosure, disruption, modification or destruction.

5. What is the importance of managing the engagement?

A. Managing engagement in ethical hacking is crucial for ensuring clear communication and expectations between the client and the ethical hackers. It establishes rules of engagement that guide the testing process, minimizes risks, and helps in effectively reporting findings to enhance the ~~see~~ organization's security posture.

6. What is the goal of technical preparation in ethical hacking?

A. The goal of technical preparation in ethical hacking is to ensure that the ethical hacking team is fully equipped and ready to conduct a thorough and effective security assessment of the target systems.

7. Give an example of password cracking tool.

A. Password Cracking tool is Hashcat. It is a powerful password recovery tool that supports a wide range of hashing algorithms, including MD5, SHA1, SHA-256 and many.

8. Name one operating system exploitation method.

A. A common operating system exploitation method is buffer overflow Attack. It occurs when a program writes more data to a buffer than it can hold.

9. Why is aligning findings important in a final report?

A. Aligning findings in a final report is crucial for several reasons,

* clarity & Understanding
* Prioritization of Risks.
* Compliance & Accountability
* Actionable Recommendations.
* facilitating communication.
* Continuous Improvement.

10. Name one component of defense planning.

A. One key component of defense planning is Risk Assessment. It involves identifying, analyzing and evaluating potential risks that could impact an organizations security posture.

Part B

11. A. Illustrate the planning process for an ethical hack using the framework provided.

A. **Ethical hacking planning framework**

1. Pre-engagement Phase.
   - Objective - Identify the specific goals of the ethical hacking engagement.
   - scope - Determine the systems, applications, and network to be tested.
   - Rules of engagement (ROE) - Establish guidelines for testing including acceptable methods and communication protocols.
2. Information Gathering.
   - Reconnaissance - Collect information passively or actively.
   - Asset Inventory - list of assets within the scope.

3. Threat Modeling Phase.

- Identify Threats - Analyze potential threats
- Vulnerability Identification.
- Risk Assessment - Evaluate the risk associated with the identified threats.

4. Engagement Planning

- Resource allocation - Assign roles and responsibilities for the engagement team.
- Timeline Development - Create a detailed timeline for the engagement, including key milestones and deadlines.

5. Communication Plan

- Establish communication protocols - how & when updates will be communicated to stakeholders.
- Final Reporting Structure - final report will be structured, including findings, recommendations and remediation steps.

6. Execution Preparation

- Tool selection - Identify and prepare the tools and techniques that will be used during the testing phase.
- Testing Environment Setup - Ensure testing environment is ready and that all necessary permissions are in place.

11. B. Explain how risk analysis contributes to ethical hacking.

A. Risk Analysis plays a crucial role in ethical hacking by identifying and assessing potential vulnerabilities and threats within an organization's system.

Risk Analysis in Ethical hacking contributes to

→ Identifying Vulnerabilities.

* Systematic Assessment – identify weakness in systems, applications and networks.
* Proactive Approach – By uncovering vulnerabilities before they can be exploited by malicious actors, organizations can take preventive measures.

→ Prioritizing Risks.

* Risk Evaluation – Ethical hackers assess the likelihood and potential impact of identified vulnerabilities, enabling them to prioritize which issues to address first.
* Resource Allocation – Allocate resources effectively, focusing on the most critical vulnerabilities that pose the highest risk.

→ Develop Mitigation Strategies.

* Tailored Solutions – Risk Analysis inform the development of targed mitigation strategies that address specific vulnerabilities and threats.

→ Compliance and Regulatory Requirements

* Conducting thorough risk analysis help organizations demonstrate compliance with laws and regulations, thereby avoiding potential penalties.

→ Enhance Incident Response.

* Understanding the risk associated with various vulnerabilities allows organizations to develop effective incident response plan.

→ Continuous Improvement.

* Risk analysis, should be conducted regularly to adapt to the evolving threat landscape.

12. A. Explain the criterial for selecting the right Security Consultant and tester.

A. Selecting the right security consultant and tester is crucial for ensuring that an organization effectively addresses its cybersecurity needs. The right professionals can provide valuable insights, identify vulnerabilities, and help implement robust security measures.

* Qualifications and Certifications.
  - → Relevant Certifications — such as
    - Certified Ethical Hacker (CEH) • CompTIA Security+
    - CISSP • OSCP • CISM.
  - → Educational Background
* Experience and Track Record.
  - → Industry Experience - Evaluate the consultant's experience in your specific industry sectors may have unique security challenges & regulatory requirements.
  - → Previous Engagements.
  - → Diverse Skill Set.
* Technical Expertise.
  - → Hands-On Skills — practical experience with security tools and techniques, including vulnerability scanning, penetration testing and threat modeling.
  - → Knowledge of current Threats.
* Methodology and Approach
  - → Structured Methodology ensures thorough and consistent evaluations.
* Communication Skills.
  - → Clear Communication and
  - → Reporting.

* Reputation and References.
  → client Testimonials and Industry reputation.
* Compliance Knowledge.
  → Regulatory awareness - Consultant is knowledgeable about relevant regulations and compliance standards (eg. GDPR etc.)
* Cost and Value
  → Budget Considerations.
  → Return on Investment (ROI) - consider potential ROI from their services, including risk reduction, compliance and improve security posture.
* Post-Engagement Support
  → Ongoing Support and long term partnership.

12. B. Illustrate the structure and logistics involved in teaming and planning a controlled hack.

A. Planning a controlled ethical hack involves a structured approach that includes team information, logistics and clear objectives.

→ Team Structure
* Red Team - Responsible for simulating attacks to identify vulnerabilities.
* Blue Team - focuses on defending against attacks.
* Purple Team - Acts as a bridge b/w the red and blue teams.
* Green Team - Works on improving the security of systems developed by the yellow team.
* Yellow Team - Comprises developers and engineers who build and design systems, focusing on functionality & security.

→ Planning Phase

* Define objectives of the ethical hack.
* Create a detailed scope document that specifies the systems, n/w and applications to be tested, along with the boundaries of the engagement.
* Rules of Engagement (ROE) – that defines an acceptable testing hours, techniques & emergency contacts to ensure all parties are aware.

→ Logistics

* Resource allocation – its need, including tools, technologies & personal. Ensure that the right tools for scanning exploitation and reporting are available.
* Setup communication channels for the teams to share findings, updates & coordinate efforts during the engagement.

→ Legal and Compliance

* Authorization – Written permission from stakeholders to conduct the ethical hack, ensuring compliance with legal and regulatory requirements

→ Execution Phase

* Reconnaissance – Information Gathering
* Scanning & Enumeration – Scan for vulnerabilities, open ports & services.
* Exploitation – Attempt to exploit identified vulnerabilities.

→ Post-Engagement Phase (or) Activities.

* Report – Comprehensive report detailing findings, including vulnerabilities, their potential impact, & recommended remediation steps.

13A. Explain the steps involved in technical preparation for a hack.

A. The steps typically involves for a hack are.

1. Knowledge Acquisition
   * Gather detailed information about target environment, including it's architecture, technologies & potential vulnerabilities.
2. Tool Selection.
   * Reconnaissance Tools – Nmap, Recon-ng. etc.
   * Scanning Tools – Nessus, OpenVAS.
   * Exploitation Tools - Metasploit, Burp Suite.
   * Reporting Tools – Dradis, Faraday.
3. Environment Setup.
   * Configure testing environments, include - virtual machines and isolated network to prevent unintended disruptions to production systems.
4. Legal Compliance
   * Written authorization.
   * Review & Understand the legal implications & compliance requirements. such as data protection laws.
5. Team Coordination.
   * Teams including
     - Red team members (attackers)
     - Blue team members (defenders)
     - Communication Leads.
6. Testing Plan Development.
   - Create a comprehensive testing plan.
7. Risk Assessment.
   - Conduct risk assessment to identify potential impacts of the ethical hack on the target organization.

8. Pre-Engagement Review

* Hold a pre-engagement meeting with all stakeholders to review the plan, clarify expectations and address any concerns.

13. B. Illustrate the importance of physical and internet reconnaissance in ethical hacking.

A. Physical and internet reconnaissance are crucial in ethical hacking as they enable hackers to gather essential information about a target's systems, networks and physical security measures.

Importance of physical Reconnaissance

→ Identify Vulnerabilities.

→ Information Gathering

→ Testing Response Protocols - By attempting to gain unauthorized access to physical locations, ethical hackers can evaluate the effectiveness of organization's security protocols & response strategies.

Importance of Internet Reconnaissance

→ Mapping the Network

- Gather data about target's online presence, including IP addresses, domain names and network architecture.

- Tools - Nmap & Shodan can be used to identify open ports.

→ Identify Digital footprints.

- Analyze the target's digital footprints through social media, websites, & public records to gather info about target

→ Assessing Security Posture.

- By performing vulnerabilities scan & penetration tests, ethical hackers can identify weaknesses in the targets online defenses, such as outdated s/w or misconfigured systems.

14 A. Explain the importance of intuitive testing and evasion technique. (6)

A. Intuitive testing and evasion techniques are vital in ethical hacking as they enhance the ability to identify vulnerabilities while avoiding detection by security systems.

Importance of Intuitive Testing

1. User-Centric Approach
   * focuses on understanding how users interact with systems, which help identify usability issues and potential security flaws that may arise from user behaviour.
2. Adaptability
   * Allows ethical hackers to adapt their testing strategies based on real time observations & feedback, making it easier to uncover hidden vulnerabilities.
   * Intuitive testing encourages creativity in finding new attack vectors, which can be crucial in identifying weaknesses that are not typically addressed in standard testing protocols.
3. Enhance Collaboration
   * Collaboration between security teams & end-users, leading to better understand of security needs & potential risks.

Importance of Evasion Techniques

1. Bypassing Security Measures
   * Enables ethical hackers to test the effectiveness of security ~~teams~~ systems by attempting to bypass detection mechanisms such as firewalls & intrusion detection systems.
2. Realistic Attack Simulation.
   * Simulate advanced persistent threats (APTs) & other sophisticated attacks, providing a more accurate representation of

of potential risks.

3. Improving Incident Response.

* Evasion techniques can reveal gaps in incident response protocols, allowing organizations to refine their strategies & improve their ability to detect & respond to breaches.

14 B. Illustrate the process of identifying vulnerabilities in operating systems & network services.

A. The process of identifying vulnerabilities in operating systems & network services in ethical hacking typically involves several key steps.

1. Reconnaissance - Information gathering

* Passive Information gathering - Collect data without direct interaction, such as searching public records, social media, & domain registration details.

* Active Information Gathering - Engaging with the target to gather information through techniques like port scanning & network mapping

* OSINT (Open Source Intelligence) - Utilizing publicly available info to build a comprehensive profile of the target.

2. Scanning.

* Port Scanning - To identify open ports & services running on the target system to understand potential entry points.

* Vulnerability Scanning - Tools like Nessus or OpenVAS to detect known vulnerabilities in software & services.

3. Gain Access:

* Exploiting Vulnerabilities - Attempting to exploit known S/W Vulnerabilities, such as buffer overflow or SQL injection. to gain unauthorized access.

* Brute force Attacks. - Systematically trying combinations (+) of usernames & passwords to access accounts.

4. Maintaining Access
* Backdoors - Create hidden entry points to ensure continued access
* Privilege Escalation - Elevating user privileges to gain higher-level access & control over critical resources.

5. Analysis & Reporting.
* Documentation - a detailed report of vulnerabilities discovered, methods used, and the level of access archieved.
* Recommendations for Remediations - Actionable insights & strategies for addressing identified vulnerabilities to enhance security posture.

15A. Explain the structure and components of an ethical hacking deliverable.

A. An ethical hacking deliverable is a comprehensive report or pesentation that outlines the findings from a penetration test or security assessment. The structure & components of an ethical hacking deliverable & crucial for effectively communicating vulnerabilities, risks & recommendations to stakeholders.

1. Executive Summary
- Provides a high-level overview of the assessment for non-technical stakeholders such as executives & management.

2. Scope of Engagement.
- Defines the boundaries of the assessment, clarifying what was tested & what was excluded.
* Description of the systems, applications & network tested.
* Testing methodologies used.
* Timeframe of the assessment.

3. Methodology

* Outlines the approach taken during the assessment, providing transparency and context for the findings.

* Phases of the assessment
* Tools & techniques Used.

4. Findings

→ Details the vulnerabilities identified during the assessment, categorized by severity and impact.

* Vulnerability description.
* Affected Systems
* Risk rating.
* Evidence.

5. Recommendations.

→ Provides actionable steps for remediation to address identified vulnerabilities.

6. Conclusion. – Summarizes the overall findings & emphasizes the importance of addressing identified vulnerabilities.

7. Appendices – Additional information that supports the main report.

15. B. Illustrate how integration lead to an improved security posture within an Organization.

A. Integration in ethical hacking enhances an organization's security posture by enabling a cohesive approach to vulnerability management & threat detection.

1. Holistic Security framework.

- Integration allows for a comprehensive security framework that encompasses various security measures including ethical hacking, threat intelligence & incident response.

2. Enhance Threat Detection.

* Integrating security tools enables continuous monitoring of systems, allowing for the immediate detection of suspicious activities.

* Automated alerts – Systems can notify security teams of potential threats, reducing response times & minimizing damage.

3. Vulnerability Management

* Integration facilitates regular penetration testing and vulnerability assessments, ensuring that security measures are up to date & effective.

* By analyzing vulnerabilities in the context of overall security posture, organizations can prioritize remediation efforts based on risk level.

4. Incident Response

* Integrated systems allow for the development of coordinated incident response plan that can be executed swiftly in the event of security breach.

5. Improved Compliance & Risk Management.

* Regulatory Alignment – helps ensure that security practices align with regulatory requirements, reducing the risk of non-compliance.

* Risk Assessment – Unified approach allows for comprehensive risk assessments, identifying potential threats & vulnerabilities across the organization

6. Cultural Shift towards Security.

* Employee Training about security awareness

* Shared responsibility between the departments in security initiatives.