Jaypee Institute of Information Technology, Noida
T2 Examination, Odd Sem 2023
B. Tech. VIIth Semester

Course Name:Ethical Hacking and Prevention **Maximum Time: 1 Hr**
Course Code: 21B12CS418 **Maximum Marks: 20**

C432-9.1	Summarize the concepts of hacking, Malwares, Network attacks, Denial of Service and counter measure	Understand level (Level 2)
C432-9.2	Demonstrate foot printing and port scanning techniques using simple tools.	Apply Level (Level 3)
C432-9.3	Carryout vulnerabilities scanning, exploitation and countermeasures in operating system, network and web application	Apply Level (Level 3)
C432-9.4	Examine wireless Network and mobile system exploitation tools with prevention	Apply Level (Level 3)
C432-9.5	Explain legal aspects of ethical hacking and writing pen testing reports.	Analyze Level (Level 4)

Note: Attempt all Questions.
Answer questions in sequence

Q1. [C432-9.1: Understanding -Level 2: 4 Marks] Consider a hypothetical example of your choice of an enterprise that provides web-based email services, and demonstrate different types of DDoS attacks in detail by giving detailed example scenarios.

Q2. [C432-9.1: Understanding -Level 2: 4 Marks] Assume that you are required to perform penetration testing in an organization. During the course of testing you also have to test level of protection against malware. For each possible malware class identify how can it enter the organization, assess the damages that it can cause, identify the remediation measures and finally list the steps on how can the organization be cleaned of such attacks.

Q3. [C432-9.3: Apply -Level 3: 4 Marks] Consider a scenario that an attacker wants to steal information from a company portal by conducting CSRF, XSS and session hijacking. By comparing these attacks sketch an exploitation plan for each of these attacks with suitable tools to use in each step?

Q4. [C432-9.3: Apply -Level 3: 4 Marks] By listing frequent causes of compromised web servers, demonstrate the required steps to pen test the web servers with suitable tools.

Q5. [C432-9.3: Apply -Level 3: 4 Marks] Present the steps taken by an attacker to implement vulnerabilities exploitation on a web application? Demonstrate using suitable tools the ways in which an attacker can identify the vulnerabilities present in a web application?