(IaaS): a. Hypervisor Exploitation: Threat: Vulnerabilities in the hypervisor layer that manages virtualized resources in IaaS environments.Explanation: Weak passwords, phishing attacks, or compromised credentials can result in account takeover and unauthorized access to sensitive data within SaaS applications.Explanation: Inadequate access controls, misconfigured sharing settings, or insider threats can lead to data exposure or leakage within SaaS environments.b. VM Sprawl: Threat: Proliferation of unused or underutilized virtual machines, leading to increased attack surface and management complexity.Platform as a Service (PaaS): a. Container Security Risks: Threat: Insecure container configurations or vulnerabilities in container runtimes used within PaaS environments.Impact: Data breaches, loss of intellectual property, and reputational damage for organizations and users relying on SaaS solutions.Explanation: Unused VMs may contain outdated software or configurations, making them vulnerable to exploitation.Impact: Data breaches, compromise of containerized applications, and disruption of cloud-native services within PaaS platforms.b. API Vulnerabilities: Threat: Insecure APIs used to manage and interact with PaaS platforms and services.Impact: Loss of confidentiality, compliance violations, and legal consequences for organizations using SaaS applications.Attackers may target these VMs to gain a foothold in IaaS environments.Software as a Service (SaaS): a. Account Compromise: Threat: Unauthorized access to SaaS applications and user accounts.b. Data Leakage: Threat: Unauthorized exposure or leakage of sensitive data within SaaS applications.Impact: Compromise of VMs, unauthorized access to sensitive data, and disruption of IaaS services.Impact: Data breaches, service disruptions, and loss of customer trust in PaaS providers.2.3.Impact: Increased risk of security breaches, resource wastage, and difficulty in managing and securing virtualized infrastructure.