Roll No.												

PRESIDENCY UNIVERSITY

BENGALURU

End - Term Examinations – May / June 2026

Date: 20- 05-2026 **Time:**01:00pm – 04:00pm

School: SOCSE	**Program:** B.Tech. Computer Science and Technology (DevOps)	
Course Code : CDV2511	**Course Name:** DevSecOps	
Semester: VI	**Max Marks**: 100	**Weightage**: 50%

CO - Levels	**CO1**	**CO2**	**CO3**	**CO4**	**CO5**
Marks	**22**	**28**	**28**	**22**	

Instructions:

(i) Read all questions carefully and answer accordingly.

(ii) Do not write anything on the question paper other than roll number.

Part A

Answer ALL the Questions. Each question carries 2marks. **10Q x 2M=20M**

1.	What are the responsibilities of a DevSecOps engineer?	**2 Marks**	**L1**	**CO1**
2.	Differentiate between sSDLC and traditional SDLC.	**2 Marks**	**L1**	**CO1**
3.	What is SonarQube and what type of testing does it support?	**2 Marks**	**L1**	**CO2**
4.	What does SCA scan for in a software project?	**2 Marks**	**L1**	**CO2**
5.	What is Clair and how is it used?	**2 Marks**	**L1**	**CO3**
6.	Define runtime security in the context of containers.	**2 Marks**	**L1**	**CO3**
7.	What is the difference between HIDS and NIDS?	**2 Marks**	**L1**	**CO4**
8.	Name any two open-source SIEM tools used in DevSecOps.	**2 Marks**	**L1**	**CO4**
9.	What is the role of AWS GuardDuty in cloud security?	**2 Marks**	**L1**	**CO2**
10.	What is policy-as-code and how does it relate to IaC security?	**2 Marks**	**L1**	**CO3**

Part B

Answer the Questions. **Total Marks 80M**

11.	**a.**	Trace the evolution from DevOps to DevSecOps. Discuss the need for embedding security in the development pipeline and the cultural shift required.	**4 Marks**	**L2**	**CO1**
	b.	Explain the sSDLC phases: requirements, design, development, testing, and deployment — with emphasis on security at each stage.	**3 Marks**	**L4**	**CO1**
	c.	Discuss the common security challenges in Agile environments. How does the DevSecOps approach mitigate these challenges?	**3 Marks**	**L2**	**CO1**
		Or			
12.	**a.**	Explain the concept of shared responsibility in DevSecOps. Discuss how developers, operations, and security teams collaborate.	**4 Marks**	**L2**	**CO1**
	b.	Describe the shift-left security concept with a diagram. Explain how it reduces vulnerabilities and cost of remediation.	**3 Marks**	**L4**	**CO1**
	c.	List and explain the roles and responsibilities of a DevSecOps team: security champion, DevOps engineer, and security architect.	**3 Marks**	**L2**	**CO1**

13.	**a.**	Explain how a complete secure CI/CD pipeline is built using SAST, DAST, and SCA tools. Discuss the integration points with Jenkins or GitLab CI.	**4 Marks**	**L3**	**CO2**
	b.	Discuss Trivy and Clair as container image scanning tools. Compare their scanning approaches and output formats.	**3 Marks**	**L4**	**CO2**
	c.	Describe SonarQube's role in static code analysis. How does it calculate technical debt and security hotspots?	**3 Marks**	**L3**	**CO2**
		Or			
14.	**a.**	Explain the methodology of DAST. Describe tools like OWASP ZAP and their integration with CI/CD pipelines.	**4 Marks**	**L2**	**CO2**
	b.	What is secrets sprawl? Explain how tools like HashiCorp Vault and AWS Secrets Manager prevent it.	**3 Marks**	**L3**	**CO2**
	c.	Discuss how Snyk performs SCA. What are the outputs of an SCA report and how are they prioritized?	**3 Marks**	**L2**	**CO2**

15.	**a.**	Explain Docker's security features: namespaces, cgroups, seccomp, and capabilities. How do these contribute to container isolation?	**4 Marks**	**L3**	**CO3**
	b.	Describe Kubernetes RBAC and its role in access control. How does it complement Pod Security Policies?	**3 Marks**	**L2**	**CO3**
	c.	Explain the role of Azure Security Center in threat protection and security posture management.	**3 Marks**	**L3**	**CO3**
		Or			
16.	**a.**	Explain runtime security in Kubernetes using Falco. Describe its rule-based detection and alerting mechanism with an example scenario.	**4 Marks**	**L4**	**CO3**
	b.	Discuss OpenSCAP and its use in automating compliance checks. Describe how SCAP content is applied to systems.	**3 Marks**	**L3**	**CO3**
	c.	Explain Docker security best practices: using minimal base images, scanning for vulnerabilities, and restricting root access.	**3 Marks**	**L2**	**CO3**

17.	**a.**	Explain how Ansible is used to automate security hardening. Provide an example of a security playbook for a web server configuration.	**4 Marks**	**L4**	**CO4**
	b.	Describe how logging and monitoring are configured for security in a Kubernetes cluster. Name two tools used.	**3 Marks**	**L2**	**CO4**
	c.	Explain the integration of IDS with a DevSecOps pipeline. How does it detect and alert on suspicious activity?	**3 Marks**	**L4**	**CO4**
		Or			
18.	**a.**	Describe how SIEM tools like Splunk or ELK are integrated into a DevSecOps workflow. Explain the data ingestion, correlation, and alerting process.	**4 Marks**	**L3**	**CO4**
	b.	Discuss Terraform security scanning tools (e.g., Checkov, Terrascan). Explain how they detect policy violations in IaC code.	**3 Marks**	**L3**	**CO4**
	c.	Describe a real-world DevSecOps case study where SIEM and IDS integration improved incident response time and security posture.	**3 Marks**	**L5**	**CO4**

19.	**a.**	Discuss the DevSecOps philosophy, its principles, and how it brings together development, security, and operations. Describe the full lifecycle with all security integration points.	**8 Marks**	**L6**	**CO1**

	b.	Compare sSDLC and traditional SDLC from a security perspective. Explain how each phase in sSDLC introduces security controls and testing.	**6 Marks**	**L4**	**CO1**
	c.	Describe SAST and SCA as complementary security tools in CI/CD. Explain integration with pipelines and present sample scan outputs and how findings are triaged.	**6 Marks**	**L3**	**CO2**
		Or			
20.	**a.**	Explain all security challenges specific to Agile methodologies (sprints, continuous delivery, shared environments). How does DevSecOps address each challenge systematically?	**8 Marks**	**L4**	**CO1**
	b.	Discuss DAST and secrets management as critical security mechanisms in CI/CD. Explain tools, methodology, and integration steps in detail.	**6 Marks**	**L3**	**CO2**
	c.	Describe the roles of all stakeholders in a DevSecOps organization. Discuss how a security-first culture is built and sustained.	**6 Marks**	**L4**	**CO2**

21.	**a.**	Provide an in-depth explanation of container security: Docker security features, Kubernetes security layers, and how they work together to protect containerized applications.	**8 Marks**	**L4**	**CO3**
	b.	Discuss cloud-native security tools for both AWS (GuardDuty) and Azure (Security Center). Explain how compliance as code with OpenSCAP and Chef InSpec enhances security governance.	**6 Marks**	**L4**	**CO3**
	c.	Explain IaC security testing for Terraform and Ansible. Describe the automated scanning process, common issues found, and remediation strategies.	**6 Marks**	**L5**	**CO4**
		Or			
22.	**a.**	Describe an end-to-end DevSecOps security monitoring architecture: from log collection to SIEM correlation to incident response. Include tools for each layer.	**8 Marks**	**L4**	**CO4**
	b.	Explain Kubernetes runtime security using Falco and AppArmor profiles. Describe how security events are detected, logged, and responded to in real time.	**6 Marks**	**L4**	**CO3**
	c.	Present a detailed DevSecOps best practices framework covering automated security gates, policy enforcement, least privilege, and continuous compliance, supported by a case study.	**6 Marks**	**L6**	**CO4**