INT328:NETWORK VIRTUALIZATION AND CLOUD SECURITY

L:2 T:0 P:2 Credits:3

Course Outcomes: Through this course students should be able to

CO1 :: recognize foundational concepts and key principles of cloud computing security.

CO2 :: apply secure configurations to enhance the protection of cloud systems.

CO3 :: describe methods to ensure secure access and isolate cloud resources.

CO4 :: interpret factors affecting security operations and disaster recovery processes.

CO5 :: explain essential models and practices for ensuring data security in the cloud.

CO6 :: evaluate emerging trends and risks to enhance cloud security strategies.

Unit I

Understanding Cloud Security : Overview of cloud Security and methods, focusing on the shared responsibility model of cloud security, Highlight common cloud security challenges such as data breaches, insider threats, compliance risks, Identity and Access Management(IAM), Azure Active Directory(AAD) structure, user and group management, Multi-Factor Authentication (MFA), real time scenario based case studies.

Unit II

Secure Networking : Azure Virtual Network (AVN), NSGs, security groups, user defined routes, firewall configuration, Web application firewall (WAF), DDoS protection standard.

Unit III

Secure compute and storage : Azure bastion, just-in-time virtual machine access, Azure Kubernetes services (AKS), Network isolation, monitor services, authentication services, manage azure container registry

Unit IV

Manage security operation : Security policies, security settings by using azure blueprint, deployed security infrastructure, azure key vaults (AKV), hardware security module, role-based access control (RBAC), manage certificate, backup and recovery solutions in azure, Configure backup of a Virtual Machine using recovery service vault.

Unit V

Data Collection Rule (DCR) : Create log analytics workspace, Azure storage account, Configuring Microsoft Defender cloud, Microsoft Sentinel.

Unit VI

Emerging Trends and Best Practices in Cloud Security : Emerging Trends and Best Practices in Cloud Security by exploring the latest trends, such as artificial intelligence in cloud security, edge computing, quantum cryptography, Secure cloud deployment, including regular audits, vulnerability assessments, adopting a proactive security posture.

List of Practicals / Experiments:

- **Set Up a Cloud Environment**
  - Analyze shared responsibility models and security challenges.
- **Identity and Access Management in Azure**
  - Create and manage users, groups, and roles in Azure Active Directory (AAD).Enable Multi-Factor Authentication (MFA).
- **Configure Secure Networking in Azure**
  - Set up an Azure Virtual Network.Configure Network Security Groups (NSGs) and user-defined routes.
- **Advanced Security with Azure Firewall and WAF**
  - Set up Azure Firewall for enhanced security, Configure Web Application Firewall (WAF).
- **Secure Access Management for Azure Virtual Machines**
  - Configure Just-in-Time (JIT) access for Azure virtual machines.

- **Secure Container Orchestration and Instances**
  - Deploy and secure Azure Kubernetes Service (AKS).Secure Azure Container Instances (ACI).
- **Backup and Recovery Solutions in Azure**
  - Implement backup and recovery strategies.
- **Secure AWS S3 Storage and Data Transit**
  - Apply security measures to AWS S3.Configure secure data transit protocols.
- **Enable DDoS Protection in Azure**
  - Set up and manage Distributed Denial of Service (DDoS) protection.
- **Cloud Vulnerability Assessment and AI-Driven Security**
  - Conduct a cloud vulnerability assessment.Apply AI-driven security measures to address identified vulnerabilities.

References:

1. MICROSOFT AZURE SECURITY ENGINEER ASSOCIATE DOCUMENTATION by MICROSOFT CERTIFICATION, Microsoft