PHYSICS PRACTICAL SHEETS

Date: ..... CAMPUS
Class: .....
Roll No.: .....
Shift: .....
Object of the Experiment (Block Letter)

chapter 5

Experiment No.: .....
Group: .....
Sub.: .....
Set: .....

1. Write down the security issue/Risk of cloud.

(i) Data breaches:-
Data breaches might be the primary goal of target attack or might be the consequences of human mistake, application flaws and inadequate inadequate security policies.

(ii) Insufficient identity, credential and access management
It can allow for illegal data access and possibly huge damage to companies or end users.

iii) Data loss:-
our sensative data is in hand of somebody else and we don't have full control over our database.

iv) Insecure API's
Easiest way to communicate with cloud is ~~to break~~ using APIs. So it must be protected.

v) User Account Hijacking:-
If somehow the account of user or an org is hijacked by hacker. Then the hacker has full authority in perform Unauthorized Activities.

vi) changing service provider.
problem when shifting from one cloud vendor to another.

2. ~~Eg)~~ Explain software-as-a service security.

To address different security issue. saas providers will need to incorporate and enhance security practice used by managed service providers and develop new ones as the cloud computing environment envolves. The baselines security practices for a saas environment as currently formalated are discussed beloco:-

(I) Security management:-
Develop the charter for security organization and program this will foster a share vision among team of what leadership is driving towards and expects and will also foster, ownership in the success of collaberated team.

(II) Security governance:
There should be the proper attention of security of government otherwise the business requirement is not met. It may not limited to security monitoring, risk mngt, application security. Due to lack of governance. Security team is not focused on key security function and activities that are critical.

iii) Risk management:
Effective risk management entails identification of technology assets, identification of data and links to busines process, applications, data store, assignment of ownership & responsibility Action should includes maintaining assets owner have authority and accountability for information assets including protection requirments and implements of integrity, availability and privacy control.

iv) Risk assessment:
Security risk assessment is critical to helping the info security org make informed decisions when balancing the dueling priorities of business utility and protection of assets. Lack of attention to completing formalized risk assessment can contribute to an increase the information security audit finding can jeopardize certification goals and can lead to inefficient and ineffective selection of security control that may not adequately mitigate info security risks to an acceptable level. A formal info security risk mngt process should proactively assess info security risk as well as plan and manage them on needed basis.

v) Security monitoring and incident response:
centralized security information management system should be used to provide notification of security vulnerabilities and to monitor system continuously through automated technology to identify potential issues.

vi) Education and Training:
programs should be established to offer a foundation for teaching security team and their internal partners essential security and risk mngt skills and knowledge.

vii) Third-party Risk mngt:-
Lack of a third party risk mngt program may result in damage to the provider's reputation, revenue losses and legal action should the provider be found not to have performed due diligence on its third party.

3. Explain Security Architecture Design of cloud.

A security Arch. framework should be established with consideration of processes (enterprise authentication and authorization, access control, confidentiality, integrity, non repudiation, security mngt etc), operational procedures technology specifications, people and org mngt and security program compliance and reporting.

Technological and design approaches, as well as the security processes required to deliver the following services all technology levels, should include in the security architecture

- Authentication
- Availability
- Integrity
- privacy.
- Authorization
- confidentiality
- Accountability

The development of a secure architecture gives engineers, data centere operations staff and n/w operations staff a standardized blueprint for designing, building and testing the security applications and system.

Vulnerability Assessment:-

vulnerability assessment classifies n/w to more efficiently prioritize vulnerability mitigation programs such as patching and upgrading. It measures the effectiveness of risk mitigation by setting goals of reduced vulnerability exposure and faster mitigation. Vulnerability mngt should be integrated with discovery, patch mngt and upgrade mngt processes to close vulnerabilities before they can be exploid.

Data privacy:
A risk assessment and gap analysis of controls and procedures must be conducted. Based on data, formal privacy processes and initiatives must be defined, managed and sustained. As security, privacy controls and protection must an elements of a secure architecture design. Depending upon the size of org and scale of operation either in divrdual or a team should be assigned and given responsibility for maintaining privacy.

Data security:-
The ultimate challenge in cloud computing is data-level security and sensitive data is the domain of enterprise, not the cloud computing provider. Security will need to move to the data level so that enterprise can be sure their data is protected whenever it goes.

Application security:-
Application security is one of the critical success factor for the world-class saas company. This is where the security features and requirements are defined and application security test results are reviewed. Application security process, secure coding guidlines, training and testing scripts and tools are typically a collaborative effort between security and development team.

virtual machine security:-
In the cloud environment, physical servers are consolidated to multiple virtual machine instances on virtualized servers. Not only can data center security team replicate typical

security controls for the data center at large to secure VM; they can also advise their customer on how to prepare these machines for migration to cloud environment when appropriate. Firewalls, intrusion detection and prevention, integrity monitoring and log inspection can all be deployed as software on VM to increase protection and maintain compliance integrity of servers and applications as virtual resources move from onpremises to public cloud environments.

4. What is cloud security monitoring? List its benefits.
Cloud security monitoring is the practice of continuously supervising both virtual and physical servers to analyze data for threats and vulnerabilities. Cloud security monitoring solutions often rely on automation to measure and assess behaviour related to data application and infrastructure.

Benefits:-

i) Maintain compliance:-
Monitoring is a requirement for nearly every major regulation from HIPAA to PCI DSS.

ii) Identify vulnerabilities:-
Automated monitoring solution can quickly alert IT and security team about anomalies and help identify patterns that point to risky or malicious behaviour.

iii) prevent loss of business:-
Cloud security monitoring can help with business continuity and data security while avoiding a potentially catastrophic data breach.

iv) Increase security maturity:-
An org with mature infosec model has a proactive multilayer approach to security which will enable overall security of environment.

v) Scalability:- security monitoring tools should be able to monitor large amount of data across a variety of distributed locations.

5. What is multitenancy? List out its issues.
Multitenancy means that multiple customers of a cloud vendor are using the same computing resources. Despite the fact that they share resources & cloud customer aren't aware of each other and their data is kept totally seperate. It can help to better use of resources and lower costs.

Issues:-
i) Security:- There is always a risk of data loss, data theft and hacking.

ii) Performance:- Saas application are at different places, and it affects the response time. It usually takes longer to respond and are much slower than server applications.

iii) Less powerful:- It lacks many essential computing features ~~and it is~~

iv) Noisy neighbour effect:-
If tenant uses a lots of computing resources, other tenants may suffer because of their low computing power.

v) Monitoring:- constant monitoring is vital for cloud service provider to check if there is an issue in multitenancy system. If any problem arises, it must get solved immediately not to disturb the system efficiency.