Kalinga University

Course- BCSAIMLCS/BCAAIML **Sem-IV**
Subject- Cloud Computing and Its Security
Subject Code: BCSAIMLCS403 & BCAAIML402

Unit V

Shared responsibility in the cloud

As you consider and evaluate public cloud services, it's critical to understand the shared responsibility model and which security tasks the cloud provider handles and which tasks you handle. The workload responsibilities vary depending on whether the workload is hosted on Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), or in an on-premises datacenter.

Division of responsibility

In an on-premises datacenter, you own the whole stack. As you move to the cloud some responsibilities transfer to Microsoft. The following diagram illustrates the areas of responsibility between you and Microsoft, according to the type of deployment of your stack.

For all cloud deployment types, you own your data and identities. You're responsible for protecting the security of your data and identities, on-premises resources, and the cloud components you control. Cloud components you control vary by service type.

Regardless of the type of deployment, you always retain the following responsibilities:

- Data
- Endpoints
- Account
- Access management

The future of the cloud seems bright, Cisco predicts that by 2018, 59% of cloud workloads will be created from Software As A Service (SaaS). While these statistics are optimistic, we cannot ignore a few concerns that stifle cloud adoption efforts, such as data ownership.

Cloud Data Ownership

Most people would be inclined to say that they still own data in the cloud. While they may be right in some sense, this is not always the case. For instance, let us look at Facebook, which many people use as cloud storage to keep their photos. According to the Facebook end-user-agreement, the company stores data for as long as it is necessary, which might not be as long as users want. This sadly means that users lose data ownership. Worse still, the servers are located in different locations, in and out of the United States, subjecting data to different laws.

According to Dan Gray, as discussed in ‘*Data Ownership In The Cloud,’* the actual ownership of data in the cloud may be dependent on the nature of the data owned and where it was created. He states that there is data created by a user before uploading to the cloud, and data created on the cloud platform. He continues to say that data created prior to cloud upload may be subject to copyright laws depending on the provider, while that created on the platform could have complicated ownership.

In addition to cloud provider policies, certain Acts of Congress, although created to enhance data security and still uphold the nation’s security, have shown how data ownership issues affect businesses. Two of these, the Stored Communications Act (SCA) and the Patriot Act show the challenges of cloud data ownership and privacy issues, with regards to government access to information stored in the cloud.

Penetration Testing

What is penetration testing

A penetration test, also known as a pen test, is a simulated cyber attack against your computer system to check for exploitable vulnerabilities. In the context of web application security, penetration testing is commonly used to augment a web application firewall (WAF).

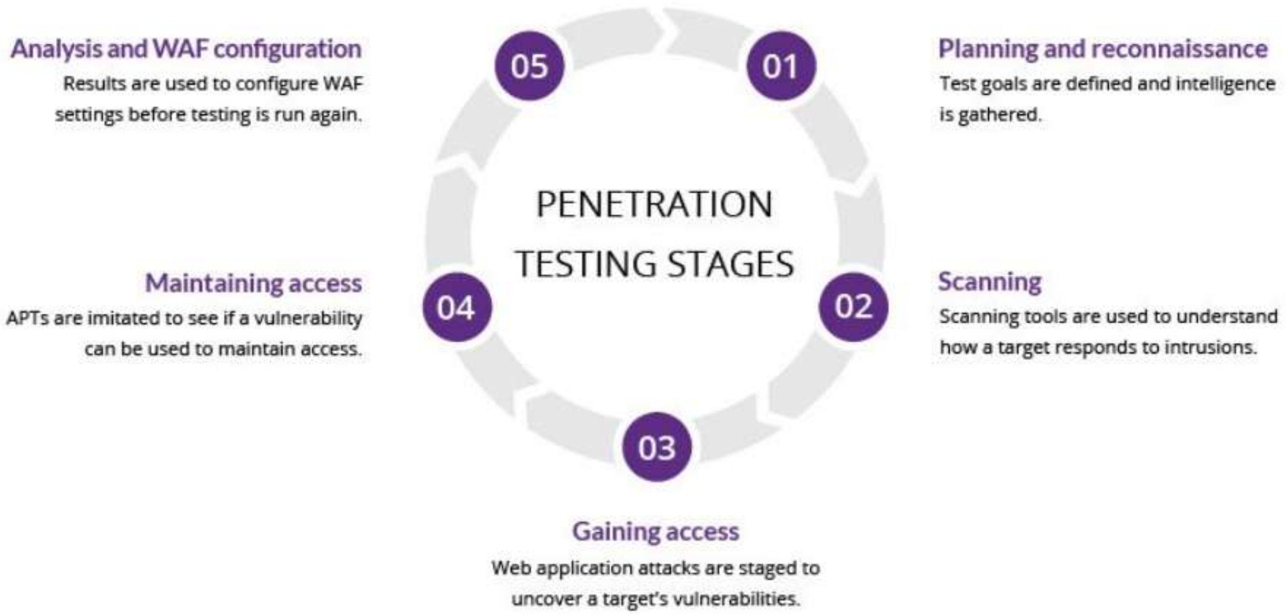
Pen testing can involve the attempted breaching of any number of application systems, (e.g., application protocol interfaces (APIs), frontend/backend servers) to uncover vulnerabilities, such as unsanitized inputs that are susceptible to code injection attacks.

Insights provided by the penetration test can be used to fine-tune your WAF security policies and patch detected vulnerabilities.

Penetration testing stages

The pen testing process can be broken down into five stages.

The pen testing process can be broken down into five stages.


PENETRATION TESTING STAGES
01
Planning and reconnaissance
Test goals are defined and intelligence is gathered.
02
Scanning
Scanning tools are used to understand how a target responds to intrusions.
03
Gaining access
Web application attacks are staged to uncover a target's vulnerabilities.
04
Maintaining access
APTs are imitated to see if a vulnerability can be used to maintain access.
05
Analysis and WAF configuration
Results are used to configure WAF settings before testing is run again.

1. Planning and reconnaissance
The first stage involves:

- Defining the scope and goals of a test, including the systems to be addressed and the testing methods to be used.
- Gathering intelligence (e.g., network and domain names, mail server) to better understand how a target works and its potential vulnerabilities.

2. Scanning
The next step is to understand how the target application will respond to various intrusion attempts. This is typically done using:

- **Static analysis** – Inspecting an application's code to estimate the way it behaves while running. These tools can scan the entirety of the code in a single pass.
- **Dynamic analysis** – Inspecting an application's code in a running state. This is a more practical way of scanning, as it provides a real-time view into an application's performance.

3. Gaining Access
This stage uses web application attacks, such as cross-site scripting, SQL injection and backdoors, to uncover a target's vulnerabilities. Testers then try and exploit these vulnerabilities, typically by escalating privileges, stealing data, intercepting traffic, etc., to understand the damage they can cause.

4. Maintaining access
The goal of this stage is to see if the vulnerability can be used to achieve a persistent presence in the exploited system— long enough for a bad actor to gain in-depth access. The idea is to imitate advanced persistent threats, which often remain in a system for months in order to steal an organization's most sensitive data.

5. Analysis

The results of the penetration test are then compiled into a report detailing:

- Specific vulnerabilities that were exploited
- Sensitive data that was accessed
- The amount of time the pen tester was able to remain in the system undetected

This information is analyzed by security personnel to help configure an enterprise's WAF settings and other application security solutions to patch vulnerabilities and protect against future attacks.

Penetration testing methods

External testing

External penetration tests target the assets of a company that are visible on the internet, e.g., the web application itself, the company website, and email and domain name servers (DNS). The goal is to gain access and extract valuable data.

Internal testing

In an internal test, a tester with access to an application behind its firewall simulates an attack by a malicious insider. This isn't necessarily simulating a rogue employee. A common starting scenario can be an employee whose credentials were stolen due to a phishing attack.

Blind testing

In a blind test, a tester is only given the name of the enterprise that's being targeted. This gives security personnel a real-time look into how an actual application assault would take place.

Double-blind testing

In a double blind test, security personnel have no prior knowledge of the simulated attack. As in the real world, they won't have any time to shore up their defenses before an attempted breach.

Targeted testing

In this scenario, both the tester and security personnel work together and keep each other appraised of their movements. This is a valuable training exercise that provides a security team with real-time feedback from a hacker's point of view.

Cloud Security Standards

Cloud-based services are now a crucial component of many businesses, with technology providers adhering to strict privacy and data security guidelines to protect the privacy of user information. Cloud security standards assist and guide organizations in ensuring secure cloud operations.

What are Cloud Security Standards?

It was essential to establish guidelines for how work is done in the cloud due to the different security dangers facing the cloud. They offer a thorough framework for how cloud security is upheld with regard to both the user and the service provider.

- Cloud security standards provide a roadmap for businesses transitioning from a traditional approach to a cloud-based approach by providing the right tools, configurations, and policies required for security in cloud usage.
- It helps to devise an effective security strategy for the organization.
- It also supports organizational goals like privacy, portability, security, and interoperability.
- Certification with cloud security standards increases trust and gives businesses a competitive edge.

Need for Cloud Security Standards

- **Ensure cloud computing is an appropriate environment:** Organizations need to make sure that cloud computing is the appropriate environment for the applications as security and mitigating risk are the major concerns.
- **To ensure that sensitive data is safe in the cloud:** Organizations need a way to make sure that the sensitive data is safe in the cloud while remaining compliant with standards and regulations.
- **No existing clear standard:** Cloud security standards are essential as earlier there were no existing clear standards that can define what constitutes a secure cloud environment. Thus, making it difficult for cloud providers and cloud users to define what needs to be done to ensure a secure environment.
- **Need for a framework that addresses all aspects of cloud security:** There is a need for businesses to adopt a

Lack of Cloud Security Standards

- Enterprises and CSPs have been forced to fumble while relying on an endless variety of auditing needs, regulatory requirements, industry mandates, and data Centre standards to offer direction on protecting their cloud environments due to the lack of adequate cloud security standards.
- Because of this, the Cloud Security Alliance is more difficult to understand than it first appears, and its fragmented strategy does not meet the criteria for “excellent security”.

Best Practices For Cloud Security

1. Secure Access to the Cloud

Although the majority of cloud service providers have their own ways of safeguarding the infrastructure of their clients, you are still in charge of protecting the cloud user accounts and access to sensitive data for your company. Consider improving password management in your organization to lower the risk of account compromise and credential theft.

Adding password policies to your cybersecurity program is a good place to start. Describe the cybersecurity practices you demand from your staff, such as using unique, complex passwords for each account and routine password rotation.

2. Control User Access Rights

Some businesses give employees immediate access to a wide range of systems and data in order to make sure they can carry out their tasks effectively. For cybercriminals, these individuals’ accounts are a veritable gold mine because compromising them can make it simpler to gain access to crucial cloud infrastructure and elevate privileges. Your company can periodically review and revoke user rights to prevent this.

3. Transparency and Employee Monitoring

You can use specialized solutions to keep an eye on the behavior of your staff in order to promote transparency in your cloud infrastructure. You can spot the earliest indications of a cloud account compromise or an insider threat by keeping an eye on what your employees are doing while they are at work. Imagine your cybersecurity experts discover a user accessing your cloud infrastructure from a strange IP address or outside of normal business hours. In that situation, they'll be able to respond to such odd activity promptly because it suggests that a breach may be imminent.

4. Data Protection

This involves data protection against unauthorized access, prevention of accidental data disclosure, and ensuring ceaseless access to crucial data in the case of failures and errors.

5. Access Management

Three capabilities that are a must in access management are the ability to identify and authenticate users, the ability to assign access rights to users, and the ability to develop and enact access control policies for all the resources.

Common Cloud Security Standards

1. NIST (National Institute of Standards and Technology)

NIST is a federal organization in the US that creates metrics and standards to boost competition in the scientific and technology industries. The National Institute of Regulations and Technology (NIST) developed the Cybersecurity Framework to comply with US regulations such as the Federal Information Security Management Act and the Health Insurance Portability and Accountability Act (HIPAA) (FISMA). NIST places a strong emphasis on classifying assets according to their commercial value and adequately protecting them.

2. ISO-27017

A development of ISO-27001 that includes provisions unique to cloud-based information security. Along with ISO-27001 compliance, ISO-27017 compliance should be taken into account. This standard has not yet been introduced to the marketplace. It attempts to offer further direction in the cloud computing information security field. Its purpose is to supplement the advice provided in ISO/IEC 27002 and various other ISO27k standards, such as ISO/IEC 27018 on the privacy implications of cloud computing, and ISO/IEC 27031 on business continuity.

3. ISO-27018

The protection of personally identifiable information (PII) in public clouds that serve as PII processors is covered by this standard. Despite the fact that this standard is especially aimed at public-cloud service providers like AWS or Azure, PII controllers (such as a SaaS provider processing client PII in AWS) nevertheless bear some accountability. If you are a SaaS provider handling PII, you should think about complying with this standard.

4. CIS controls

Organizations can secure their systems with the help of Internet Security Center (CIS) Controls, which are open-source policies based on consensus. Each check is rigorously reviewed by a number of professionals before a conclusion is reached.
To easily access a list of evaluations for cloud security, consult the CIS Benchmarks customized for particular cloud service providers. For instance, you can use the CIS-AWS controls, a set of controls created especially for workloads using Amazon Web Services (AWS).

5. FISMA

In accordance with the Federal Information Security Management Act (FISMA), all federal agencies and their contractors are required to safeguard information systems and assets. NIST, using NIST SP 800-53, was given authority under FISMA to define the framework security standards (see definition below).

6. Cloud Architecture Framework

These frameworks, which frequently cover operational effectiveness, security, and cost-value factors, can be viewed as best parties standards for cloud architects. This framework, developed by Amazon Web Services, aids architects in designing workloads and applications on the Amazon cloud. Customers have access to a reliable resource for architecture evaluation thanks to this framework, which is based on a collection of questions for the analysis of cloud environments.

7. General Data Protection Regulation (GDPR)

For the European Union, there are laws governing data protection and privacy. Even though this law only applies to the European Union, it is something you should keep in mind if you store or otherwise handle any personal information of residents of the EU.

8. SOC Reporting

A form of audit of the operational processes used by IT businesses offering any service is known as a “Service and Organization Audits 2” (SOC 2). A worldwide standard for cybersecurity risk management systems is SOC 2 reporting. Your company’s policies, practices, and controls are in place to meet the five trust principles, as shown by the SOC 2 Audit Report. The SOC 2 audit report lists security, availability, processing integrity, confidentiality, and confidentiality as security principles. If you offer software as a service, potential clients might request proof that you adhere to SOC 2 standards.

9. PCI DSS

For all merchants who use credit or debit cards, the PCI DSS (Payment Card Industry Data Security Standard) provides a set of security criteria. For businesses that handle cardholder data, there is **PCI DSS**. The PCI DSS specifies fundamental technological and operational criteria for safeguarding cardholder data. Cardholders are intended to be protected from identity theft and credit card fraud by the PCI DSS standard.

10. HIPAA

The Health Insurance Portability and Accountability Act (HIPAA), passed by the US Congress to safeguard individual health information, also has parts specifically dealing with information security. **Businesses that**

handle medical data must abide by HIPAA law. The HIPAA Security Rule (HSR) is the best choice in terms of information security. The HIPAA HSR specifies rules for protecting people's electronic personal health information that a covered entity generates, acquires, makes use of or maintains.

Organizations subject to **HIPAA regulations need risk evaluations** and risk management plans to reduce threats to the availability, confidentiality, and integrity of the crucial health data they manage. Assume your company sends and receives health data via cloud-based services (SaaS, IaaS, PaaS). If so, it is your responsibility to make sure the service provider complies with HIPAA regulations and that you have implemented best practices for managing your cloud setups.

11. CIS AWS Foundations v1.2

Any business that uses Amazon Web Service cloud resources can help safeguard sensitive IT systems and data by adhering to the CIS AWS Foundations Benchmark. Intelligence analysts developed a set of objective, consensus-driven configuration standards known as the CIS (Center for Internet Security) Benchmarks to help businesses improve their information security. Additionally, CIS procedures are for fortifying AWS accounts to build a solid foundation for running jobs on AWS.

12. ACSC Essential Eight

ACSC Essential 8 (also known as the ASD Top 4) is a list of eight cybersecurity mitigation strategies for small and large firms. In order to improve security controls, protect businesses' computer resources and systems, and protect data from cybersecurity attacks, the Australian Signals Directorate (ASD) and the Australian Cyber Security Centre (ACSC) developed the "Essential Eight Tactics."

Are you ready to unleash the power of **DevOps** to streamline your **Software Development and Deployment**? Learn about our **DevOps Live Course** at GeeksforGeeks, created for all professionals in practice with continuous integration, delivery, and deployment. Learn about leading tools, industry best practices, and techniques for **automation** through an interactive session with hands-on **live projects**. Whether you are new to DevOps or looking to improve your skills, this course equips you with everything needed to streamline workflows and deliver excellent quality software in the least amount of time. Learn to take your skills in DevOps to the next level now, and harness the power of streamlined software development!

Cloud Compliance: How Do Major Compliance Standards Impact the Cloud?

The ISO has created standards for many kinds of systems and technologies, such as:

- **ISO/IEC 17789 (2014)** – this standard outlines cloud computing activities, functional components, and roles, including the way they interact.

- **ISO/IEC 19944-1 (2020)** – this standard specifies how data is transported via cloud service centers and cloud service users.
- **ISO/IEC Technical Specification 23167 (2020)** – this standard specifies techniques and technologies employed in cloud computing, such as VMs, containers, and hypervisors.
- **ISO/IEC 27018 (2019)** – this document describes guidelines founded on ISO/IEC 27002, emphasising the safeguarding of personal identifiable information (PII) within the public cloud.

C compliance for the cloud provider vs. compliance for the customer

Compliance as a Service (CaaS) in Cloud Computing

Cloud compliance issues occur as any cloud consumer make use of cloud storage and backup services. Cloud computing by its very nature extents various jurisdictions. The laws of the country of request from where it originates many not necessarily match the laws of the country in which the request is being processed, and probably laws of neither location match the laws of the country in which the service is delivered. Compliance is beyond than a basically provided an unidentified service token to an identity so that access to a resource can be obtain. Compliance is a difficult issue which needs considerable expertise. While **Compliance as a Service (CaaS)** seems in discussion, some examples which falls under service of this category exist as a general product for a cloud computing architecture. A Compliance as a Service (CaaS) application would need to oblige as a third party. CaaS may require to be architecture as its own layer of a Service Oriented Architecture (SOA) in order to be reliable. A CaaS may be needed to be able to manage cloud relationships, comprehend security rules and procedures, know how to operate data and administer privacy, deliver an incidence feedback, archive, and enable the system to be queried. This is a huge order, but CaaS has the capability to be a good value-added service. CaaS system built inside a private cloud in which the data is under control of a single entity, thus confirming that the data is under that entity's secure control and that transaction is audited. Indeed, major cloud computing compliance systems have been created with the help of private cloud. A well-implemented CaaS service may measure the risk of servicing compliance and ensure or indemnify tenancy against that risk. CaaS can be brought to bear as mechanism to guarantee that an e-mail conformed to particular standards, anything which may be new electronic service of a network of national postal system and something which may help in ending the scourge of spam. The major **services** that should provided additionally in a Compliance as a Service (CaaS) offering:

1. Database access control
2. Separation of duties
3. Annual risk assessment
4. Application management
5. Change control
6. Data discovery
7. Data masking
8. Incident response
9. Policy creation and enforcement
10. Real-time data protection
11. Repair of vulnerabilities
12. Personnel training
13. Service configuration