CEH v12 Lesson 12 : Introduction to Cloud Computing Vulnerabilities

Learning Outcomes

In this module, you will complete the following exercises:

- Exercise 1 — Cloud Computing Concepts
- Exercise 2 — Cloud Computing Threats and Protection

After completing this module, you will have further knowledge of:

- Cloud Computing Services
- Cloud Deployment Models
- Benefits of Cloud Computing
- Cloud Service Providers
- Container Technology
- Serverless Computing
- Differences between Serverless Computing and Containers
- Cloud Computing Threats
- OWASP Top 10 Cloud Security Risks
- Cloud Computing Hacking
- Cloud Security
- Cloud Security Considerations

Lab Duration

It will take approximately **30 minutes** to complete this lab.

Exercise 1 — Cloud Computing Concepts

Traditionally, organizations hosted servers on-premise and had one physical server for one particular task. Virtualization was the first step in reducing the number of physical servers and maintenance required since the infrastructure required to support the remaining physical servers remained. Moving to the cloud from on-premise removed the burden of maintaining this infrastructure. The cloud is simply a datacenter in which the entire infrastructure, electrical, safely, networking, security, etc...is supported by a cloud service provider. The client is basically renting the infrastructure will keeping access to all data and applications hosted in the cloud.

Virtualization is a concept that uses physical resources to run several virtual machines on the system. Each of these machines is a virtual representation of a physical system. Depending on the resources available, a physical system can host several virtual machines.

The concept of cloud computing is to make infrastructures, operating systems, and applications available to users in a remote environment. A user needs to have only a system and an Internet connection to access these resources. The concept of cloud computing runs on the on-demand allocation of resources.

In this exercise, you will learn about cloud computing concepts.

Learning Outcomes

After completing this exercise, you should have further knowledge of:

- Cloud Computing Services
- Cloud Deployment Models
- Benefits of Cloud Computing
- Cloud Service Providers
- Container Technology
- Serverless Computing
- Differences between Serverless Computing and Containers

Cloud Computing Services

There are different Cloud computing services. An organization's business requirements govern the type of cloud computing service implemented.

Some Cloud computing services are:

Software as a Service (SaaS)

In Software as a Service, an application is licensed to users after purchasing a subscription. The license holder must then renew their subscription to continue using the service. Without the subscription, only limited features may be available for users. Typically, users access the application through a web browser.

Examples include:

- Dropbox
- Microsoft OneDrive
- Microsoft Office 365
- Cisco WebEx
- Citrix GoToMeeting
- Google Apps

Infrastructure as a Service (IaaS)

"Infrastructure as a Service (IaaS) virtualizes the underlying network infrastructures, such as physical computing resources, location, data partitioning, scaling, security, backups, virtual machines, virtual network devices, and software-defined networking. This provides great flexibility to the client, and they can:

- Create virtual machines (VMs)
- Install operating systems in each VM
- Deploy middleware
- Create storage buckets

Examples include:

- Amazon EC2
- Cisco Metapod
- Microsoft Azure
- Google Compute Engine (GCE)

Platform as a Service (PaaS)

In Platform as a Service (PaaS), a platform for development is offered to users on a subscription basis. In this model, the service provider provides a set of development tools, which reduces the cost of purchasing these tools separately.

Examples include:

- Google App Engine
- Microsoft Azure
- Intel Mash Maker

Anything as a Service (XaaS)

Anything as a Service (XaaS) refers to IT functions delivered over the Internet as a service. It is acronymed as XaaS, where X stands for anything, ranging from Marketing as a Service to Healthcare as a service, and could be any IT function.

XaaS does not limit itself to IT functions only or digital products delivered as a service. For example, you could get medical consultation without leaving home. XaaS also includes various IT services delivered in PaaS, IaaS, and SaaS.

Cloud Deployment Models

There are different types of cloud, known as cloud deployment models. These types are as follows:

Private Cloud

Also referred to as a corporate or internal cloud, the private cloud is owned and operated by a single organization. If the infrastructure remains on-premise, the organization acts as its own cloud service provider (CSP).

The other option is to have the private cloud hosted by an external cloud service provider. Either way, the organization has total control over the computing resources as they are not shared or available to any other customers.

Organizations choose this model when they need total control over the security of their data. Government, highly-regulated, financial, and research & development companies are most likely to use this model.

Private CloudPrivate Business

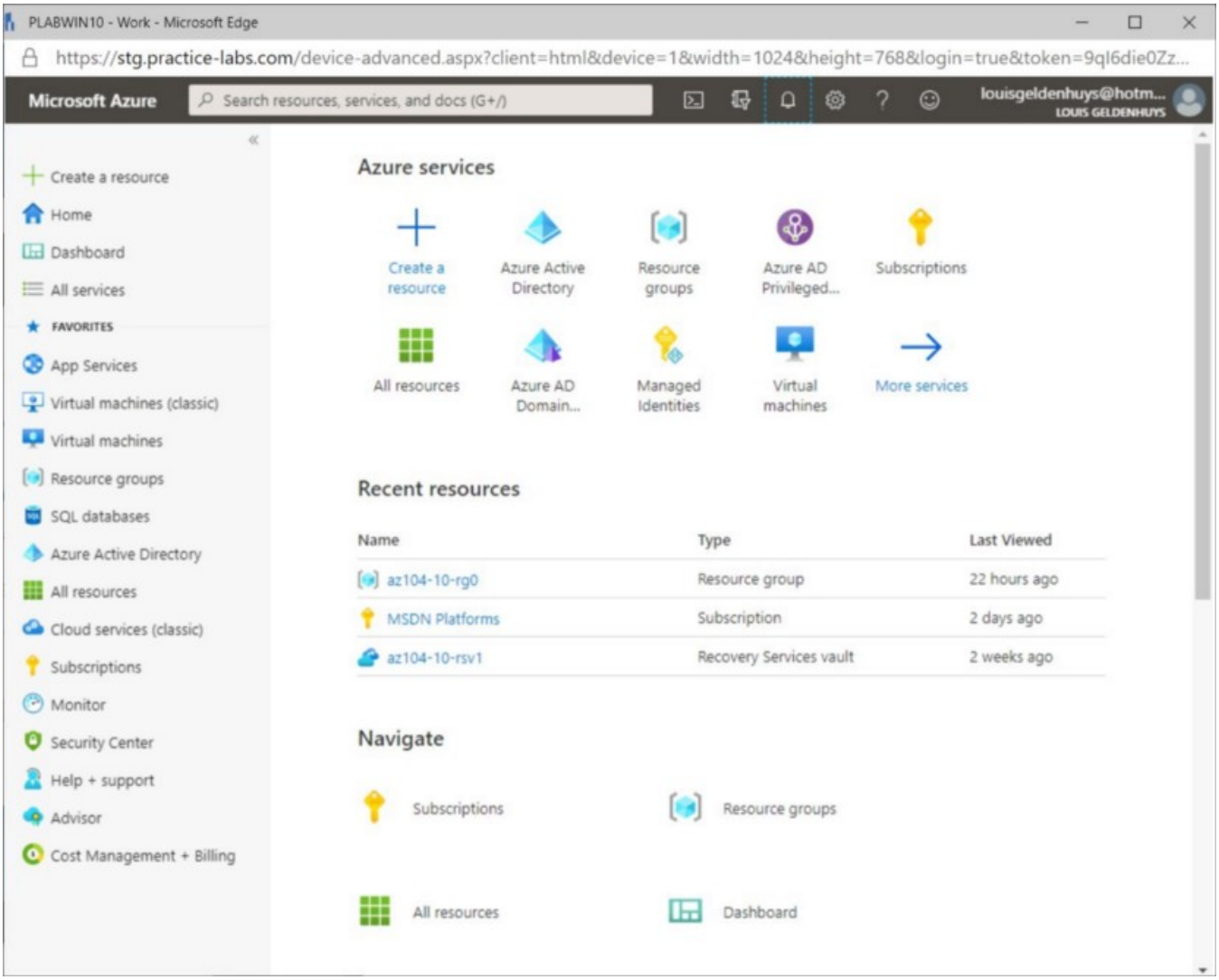
Figure 1.1: Showing the Private Cloud model, showing the cloud being utilized by a single professional organization.

Public Cloud

Services such as applications, servers, and data storage are made available by cloud service providers using this model. Clients share resources such as hardware by pooling all available resources and allocating only the amount each needs and is willing to pay for.

This is the most efficient manner to use available computing resources. Should a client need more resources, they simply ask for it. This can be a manual setting change or automated based or parameters set by the client. The Public Cloud model is completely off-site for clients and all infrastructure maintenance is provided by the CSP.

Below is an image of the Microsoft Azure portal web interface. This web interface is used to create and manage cloud services.



Hybrid Cloud

A Hybrid Cloud Infrastructure is a combination of a Public and Private cloud where the services that are provided are shared between the different infrastructures. The public and private infrastructures are connected to each other through the internet to ensure the resources are available.

This type of cloud infrastructure is used when the demand for resources fluctuates, and the Private Cloud can not meet these demands. The Public Cloud's Infrastructure is then used to seamlessly scale the resources to meet these demands.

Hybrid CloudPrivate CloudPublic Cloud

Figure 1.3: Showing the Hybrid Cloud model, showing it linked to Private and Public Clouds.

Community Cloud

In a community cloud, users share the same set of data and resources. Multiple parties access it. For example, a cloud-deployed for the students at a university or a college

would normally be a community cloud — accessed by all students.

Community CloudOrganization 1Organization 2

Figure 1.4: Showing the Community Cloud model, showing it being utilized by multiple organizations.

Benefits of Cloud Computing

The popularity of cloud computing is its benefits over on-premise computing. Below is the list of benefits that are offered by cloud computing:

On-Demand Self Service Clients and subscribers interact with the services rendered by CSP without any human interaction 24-hours a day, 365 days a year through the use of any browser-enabled computing device connected to the internet.**Rapid Elasticity**Cloud computing allows you to scale up or down your IT infrastructure on-demand. You can provision new servers or add or remove memory or any other component as and when required. For example, if you know that your web server will be overloaded in a busy time-period, you can scale up your infrastructure during that time and then scale down later on. All this can happen within a few minutes.**Security**A cloud service provider uses the latest security tools to monitor the data hosted by its clients. When you have in-house data, you need to hire skilled security professionals and purchase the security hardware and applications. When the data is hosted in the cloud, it is the cloud service provider's headache to protect your data.**Broad Network Access**With the increased use of mobile phones, tablets, and laptops, users require 24x7 access to their data. A user can be on the move, in the office, or at home when they want to access data. Access to data becomes difficult when it is stored in-house on file servers. However, if the data is stored in the cloud, it is easy to access using a mobile phone, tablet, or laptop.**Measured Services**Clients pay for only those services they consume in a "pay-per-use" method. Subscribers may pay monthly fees or according to the usage of resources such as storage, bandwidth, and processing power.**Resource Pooling**The CSP pools all available computing resources to serve multiple clients in a multi-tenant environment. Resources are dynamically assigned and re-assigned based on client demands.

Container Technology

Containers work on the concept of compartments. You can deploy multiple containers on a single host, and each container can run different applications. An important feature of containers is that the operating system is the same for all containers on a single

physical host. This contrasts with the virtual machine running different operating systems on the same physical machine.

Containers are quick to create, are lightweight, and start as soon as the operating system boots. This avoids any latency in setting up and running applications.

Container technology has a five-tier architecture:

- **Tier 1**: Developer machines
- **Tier 2**: Testing and accreditation systems
- **Tier 3**: Registries
- **Tier 4**: Orchestrators
- **Tier 5**: Hosts

Containers have a three stage life-cycle:

- **Phase 1**: Image generation and validation. The application or software components are developed and stored in images.
- **Phase 2**: Image storage and retrieval. Storage of images is done in registries. Tagging and cataloging for version control and reuse by developers is provided in the registry.
- **Phase 3**: Container Deployment and Management. Orchestrators are tools used to pull the latest version of an application from the registry and deploy it for use. Orchestrators also allow for monitoring of container resources.

The fundamental differences between virtualization and containerization include:

- **Speed**: Containers start with the operating system as it is loaded. Therefore, the start is immediate. However, virtual machines need to load the complete operating system.
- **Resources**: Containers start immediately with the operating system, and therefore, there is little system resource consumption. For example, a container consumes a small portion of memory on the startup. On the other hand, there can be multiple virtual machines running on a single physical host, and each virtual machine

requires its share of system resources. This can load the physical server, which ultimately impacts the virtual machines.

- **Security and isolation**: Containers run within the operating system. The containers can isolate applications and their data only at the process level, and they are less secure. On the other hand, virtual machines run separately and in isolation. Therefore, virtual machines are more secure than containers. If the operating system is compromised, all the containers can also be compromised. This, however, is not true for various virtual machines running on a physical machine.
- **Portability**: Containers are much smaller in size, and therefore, they are easy to port. Porting a virtual machine includes porting configuration files and libraries as well. Therefore, the porting size of the virtual machines can be much larger, and portability can be a problem.
- **Operating System**: A virtual machine can run an independent operating system on a physical host. Containers can run only the operating system that the host is running.

Serverless Computing

Serverless architecture, also known as Function as a Service (FaaS), has a cloud-based application architecture meaning developer do not need to be concerned with the underlying server or any provisioning, load-balancing, securing, or patch management. The containers or functions are created by programs through a process called orchestration. Instances are completely created, provisioned, used, and destroyed on-demand based on user requests. Each function provides a single service to a client such as playing a movie. When they movie is done or shut down by the user, that instance is destroyed.

There is often confusion between PaaS and FaaS. Both these services are based on the concept of running an application in the cloud. However, the underlying architectures are fundamentally different. In PaaS, the entire application is run as a single unit, which means the scaling is done at the application level. However, in FaaS, the scaling is done at the function level because it is composed at the function level. As and when required, functions can be scaled individually. This saves many system resources because only selected functions might be consuming more resources than the others.

An existing application will need to be architected again to run as small independent functions. As such, serverless architecture is good to use when you have a limited

number of functions.

Advantages of Serverless Computing

There are several advantages of serverless computing, such as:

- **No Server Setup**: this burden is taken from developers who should focus on application development rather than server setup.
- **Faster Deployment**: developers do not have to worry about setting up an infrastructure. It is already available for them.
- **Reduced Infrastructure Cost**: there is no cost in setting up an infrastructure for developers.
- **Pay-per-use**: as serverless computing is in a cloud environment; developers only pay for what they use.
- **Quick Resource Provisioning**: resources can be quickly provisioned and de-provisioned.
- **No server administration or maintenance**: the underlying infrastructure is in the control of the cloud service provider, and therefore, developers do not need to worry about administration and maintenance.
- **Scalability**: developers can use as many resources as needed and scale up the resources. As this is a pay-per-use model, the developers pay only for the resources that they use.

Disadvantages of Serverless Computing

If there are advantages of serverless computing, there are disadvantages. Some of the key disadvantages are:

- **Vendor lock-in**: As serverless computing is within a cloud environment, developers might have difficulty moving from one cloud service provider.
- **Complex testing**: Developers may need to fine-tune the underlying infrastructure to test code. Testing scenarios may be complex since it is not in their control.
- **Security vulnerabilities**: Serverless infrastructure needs to be managed and maintained by the cloud service provider. If patches are not deployed on time or the vulnerability management process is not in regular practice, then vulnerabilities will

not just impact the underlying infrastructure but also the applications being developed.

Differences Between Serverless Computing and Containers

Users may confuse serverless computing and containers, although they are quite different. The differences are as follows:

Setup

- **Container**: is set up by developers who need to create the image and then execute a container from the image.
- **Serverless computing**: is set up by the cloud service provider. Developers do not have to set up, manage, or maintain it.

Execution

- **Container**: continues to run as long as required. Developers need to stop the container manually.
- **Serverless computing**: destroys the function after it completes its execution.

Timeout

- **Container**: does not have any timeout restrictions.
- **Serverless computing**: has timeout restrictions on the running code.

Underlying Infrastructure

- **Container**: requires the underlying infrastructure to be defined by developers.
- **Serverless computing**: does not require underlying infrastructure to be defined by a developer.

Storage

- **Container**: stores data in temporary storage. Containers can also store the data in mapped volumes.
- **Serverless computing**: stores the data in object storage.

Suitability

- **Container**: can be used for microservices as well as large applications.
- **Serverless computing**: is suitable for microservices.

Development Language

- **Container**: allows developers to choose the programming language and runtime for developing an application.
- **Serverless computing**: restricts the developers with specific programming languages and runtimes.

Exercise 2 — Cloud Computing Threats and Protection

Along with benefits, cloud computing also brings a wide spectrum of new security risks. Although, just as with other risks, you can use various methods to minimize and mitigate security concerns.

Even though the data resides in the cloud, it is still an administrator's responsibility to protect it. Therefore, you must use various methods to ensure protection against data loss or theft and minimize the threats to data privacy and its confidentiality.

In this exercise, you will learn about cloud computing threats and protection.

Learning Outcomes

After completing this exercise, you should have further knowledge of:

- Cloud Computing Threats
- OWASP Top 10 Cloud Security Risks
- Cloud Computing Hacking
- Cloud Security
- Cloud Security Considerations

Cloud Computing Threats

Like the on-premises infrastructure, cloud computing is also prone to several threats. Some of the key threats to cloud computing are as follows:

Data Loss

Most cloud computing environments work with a multi-tenancy model. If data or an application on one tenant is compromised, it can put the data of the other tenants at risk. The data can be deleted or copied by an attacker. Data is also at the mercy of the cloud service provider, which can itself be a big threat. If an insider compromises the data, you may end up losing access.

Management Interface Failure

Cloud consumers use the management interface to manage their cloud infrastructure. If there is a failure in the management interface, the cloud consumer can no longer manage their infrastructure.

Management Interface Compromise

The management interface is accessed via remote access or through a web browser. The management interface compromise can occur in either case because of misconfigurations, operating system and application vulnerabilities, and improper access control.

Virtual Machine (VM)-level Attacks

The cloud environment has various types of VM technologies running in the background. If an attacker can find and exploit a vulnerability, especially in the hypervisor, the attacker can potentially control a tenant's virtual machines.

Compliance Issues or Risks

There can be a possibility that an organization may need to be compliant with a specific law, regulation, or standard. However, the cloud service provider does not need to be compliant with the same one. At the same time, even if it is compliant with a specific law, regulation, or standard, the cloud service provider may not be able to provide sufficient evidence.

Malicious Insider

If there is an insider with malicious intentions at the cloud service provider's end, tenants' (and their customers') data is at stake.

Jurisdiction Change

A cloud service provider may store data of cloud consumers in different jurisdictions that need to comply with different laws. If any law changes, the cloud service provider needs to ensure compliance.

Service Termination or Failure

A cloud service provider may terminate service due to non-payment. An organization may be suffering from a business loss and delays the payments or unable to make the payment. In this scenario, a cloud service provider may terminate their services, further impacting its business.

There can also be service failures at the cloud service provider's end, which eventually impact the organization's ability to serve customers.

Service Level Agreement (SLA) Issues

A cloud service has to provide certain service level commitments. If they are not met, it directly or indirectly impacts cloud consumers.

Loss of Encryption Keys

If data is encrypted in a cloud environment, a cloud consumer needs to safeguard encryption keys. If encryption keys are stolen, the set of encrypted data will be useless for the cloud consumer. If the keys are stolen, it becomes easy for the attacker to decrypt data.

Weak Authentication

A cloud consumer may use weak authentication, allowing the attacker to break through other potential defenses.

Physical Device Theft

If there is a physical device theft, such as a hard drive, it can directly impact cloud consumers, specifically those with data stored on the stolen hard drive. Any other physical device theft, such as a router, can help the attacker understand the configuration, which can then initiate an attack.

Network Failure

Network failures can happen in any organization. This can cause a major business impact on cloud consumers, where their applications and data may become unavailable to their customers and employees.

E-Discovery

If a cloud consumer has a legal case or needs to have their data reviewed by legal authorities, then the cloud environment can make the entire process more difficult. For example, data may be spread over different geographies. Different regulations and laws may apply in different geographies. Therefore, the entire process is much more complicated than on-premises infrastructure.

Hardware Failure

A cloud service provider is responsible for maintaining physical hardware. If a cloud service provider does not have adequate monitoring systems in place, hardware (such as a hard drive failure) can cause downtime for customers. Assuming a hard drive failure, the cloud consumers may lose data.

Improper Data Deletion Procedures

If you want to wipe your data, even securely, you cannot be sure that the data is securely deleted. In a cloud environment, the data is replicated across different geographies. When you delete data from your account, the data may not be deleted from other geographies, even though this is not transparent to the cloud consumer.

Lack of Proper Data Backup and Restore Procedures

After an attack, an attacker may gain access to the data and the backups. If a cloud service provider does not have proper backup and restore procedures, a cloud consumer may end up losing all data.

Unauthorized Billing

If a cloud consumer is hacked but is not aware of it, an attacker can conveniently use the resources. The cloud consumer will only become aware when the bill is received. An example can be excessive bandwidth use by using a server that acts as a bot or illegally storing data on a server or storage of a cloud consumer.

Cloud Service Provider Shutting Down

Due to going out of business or selling the business to another organization. One of the big reasons is a financial crunch, which may cause the cloud service provider to go out of business. This can leave the cloud consumers in a risky situation as they may be using the cloud service provider-specific applications, which may cause a vendor lock-in situation for them.

Intentional or Accidental Data Deletion

There can be intentional or accidental data deletion. An insider can intentionally delete the data at the cloud service provider or cloud consumer's end. An employee can accidentally delete the data. In both cases, the proper restoration of the data needs to occur. If the proper backup and restore procedures are not in place, a cloud consumer may lose the data.

Multi-tenancy

Multi-tenancy causes a big risk in that if there is a configuration issue from the cloud service provider, the data from one tenant may be visible to another tenant. Also, if a tenant is breached, the data may be a risk for the other tenants.

Misconfigurations

Misconfigurations are one of the major reasons for security attacks and breaches. Even if the cloud service provider implements the best of security, in some cases, such as Infrastructure As a Service (IaaS), it is the responsibility of the cloud consumer to secure their infrastructure. If there are misconfigurations, such as extra ports open, the infrastructure can be breached.

OWASP Top 10 Cloud Security Risks

OWASP stands for Open Web Application Security Project, a non-profit organization that provides information on various security aspects. They publish the top 10 threats or risks in different domains, such as applications, mobile, and cloud. OWASP published the top 10 cloud security risks, which are as follows:

1. **Accountability and Data Ownership**: is one of the key issues in the cloud environment. It can be difficult to define accountability and data ownership in the cloud environment. Recoverability of the data can be at risk.

2. **User Identity Federation**: needs to be controlled through identity management systems. Access control can be difficult to manage since the data is shared across several applications and application programming interfaces (APIs).
3. **Regulatory Compliance**: can be an issue if an organization is present in one country and data is stored in another country.
4. **Business Continuity and Resiliency**: is dependent on the cloud service provider. If the cloud infrastructure goes down, it can have a serious business impact even for a few minutes.
5. **User Privacy and Secondary Usage of Data**: can be a greater risk in the cloud environment. Users cannot ensure that the data is shared with third parties. The data is at the mercy of the cloud service provider.
6. **Service and Data Integration**: can be a challenge if the data is not secured using appropriate protocols, like Transport Layer Security (TLS).
7. **Multi-Tenancy and Physical Security**: is a big challenge in the cloud environment. With the data of tenants stored on servers, one cannot be sure that it is safe. If one tenant is attacked, it can impact the remaining tenants on the same server. Data is logically segregated, not physically. Also, physical security is the cloud service provider's responsibility, which, if not handled properly, can pose greater risks to the devices and servers.
8. **Incident Analysis and Forensic Support**: can be difficult to perform compared to the on-premises environment. In the cloud environment, the logs may be stored in different geographies.
9. **Infrastructure Security**: is dependent on the cloud service provider to a great extent. The risk assessment of the physical and logical infrastructure may be ignored, which eventually adds more risks.
10. **Non-Production Environment Exposure**: refers to the staging and development environments that may not be as secure as the production or live environments.

Cloud Computing Hacking

Just like an on-premises infrastructure, cloud computing is also prone to several types of attacks. The way vulnerabilities exist in an on-premises infrastructure; can also exist in

the cloud environment. Attackers can hack into a cloud environment for various reasons:

- Steal, corrupt, or delete data
- Gain access to the user credentials
- Misuse the cloud environment without cloud consumer's knowledge
- Use the cloud environment for crypt-mining
- Use the cloud infrastructure to perform attacks on other organizations — use of zombie or bot systems to conduct a Denial-of-Service (DoS) or Distributed DoS (DDoS)

Several attacks can be performed on the cloud environment. Some of the key ones are:

- Social Engineering attack
- XSS attack
- Domain Name System (DNS) attack
- SQL Injection attack
- Wrapping Attack
- Network Sniffing
- Session Riding
- Side Channel Attack or Cross-guest VM breaches
- Cryptanalysis attack
- DoS and DDoS attack
- OpenStack components attack
- Man-in-the-Middle (MITM) attack
- VM level attack

Most of these attacks are common to the on-premises IT infrastructure. For example, an XSS attack can be performed on an in-house hosted web application.

Cloud Security

Cloud security refers to the security implementation and deployment of various tools and technologies that can help safeguard the data resting in the cloud.

Application Layer

Cloud consumers can use the OWASP security standards for web applications. OWASP publishes the top 10 attacks on applications and provides remediation methods. At the application layer, you need to deploy the web Application Firewall (WAF) that will help you filter the traffic to the web application. The key methods to protect the application layer are binary analysis, WAF, and transactional security.

Network Layer

Various tools can be deployed to protect information at the network layer. Some of the key tools are:

- Next-Generation IDS/IPS devices
- Next-Generation Firewalls
- DNSSec tools
- Anti-DDoS tools
- OAuth configuration
- Deep Packet Inspection (DPI) tools

The Root of Trust (RoT)

Each component of hardware and software is validated and used. If a hardware or software component is not validated, it cannot be used. The cloud environment must have auditability and integrity measures implemented.

Computer and Storage

Computer and Storage can be secured using various methods, such as:

- Host-based Intrusion Detection (HIDS)
- Host-based Intrusion Prevention Systems (HIPS)

- Integrity checks
- File system monitoring
- Logfile analysis
- Kernel level detection
- Encryption

Physical Security

Physical security is the most critical part of securing information. No matter what you use to secure your information, every security method will fail if the device holding the information is not secure.

Information Layer

The information must be protected using various controls, such as:

- Administrative
- Technical
- Physical

It is important to note that security controls may not protect information in isolation. Therefore, they should be implemented in layers to create defense-in-depth. For example, you can encrypt the data at rest and transmission. At the same time, you can use Data Loss Prevention (DLP) to ensure that confidential data does not go out of the network.

Some of the key protection methods at this layer are DLP, content filtering, encryption, and database monitoring.

Management Layer

The management layer is an important component in a cloud computing environment. It must be safeguarded with various security controls, such as Identity and Access Management (IAM), patch management, monitoring and governance, configuration management, and change management.

Cloud Security Considerations

While working with cloud computing, you should keep the following security considerations in mind:

Geo-resilience When opting for cloud services from a cloud service provider, you must ensure that it offers enough security services to protect your data. You need to be assured that the cloud service provider can provide Geo-resiliency in any disaster, such as a fire or flood. You must also ask where the service provider has its data centers. This becomes crucial because if the cloud service provider has only a limited number of data centers, you may not want to risk your data by hosting it in their data center. Rather, you should opt for a service provider with a global presence and data replicated to multiple data centers.**Encryption**

You need to ensure that it is encrypted when data is moved to the cloud or between two clouds. Without encryption, data is vulnerable at rest and in transit. If no encryption is used, there is a high risk of data loss or exposure of confidential data to an attacker.

Access Control

When the data is in the cloud, you must enforce role-based access control. This can prevent unwanted access.

Network Segmentation

Most cloud service providers use multitenant environments. When opting for a cloud service, you need to evaluate the cloud service provider's type of segmentation and how your data will be segmented from the other customers in the same multitenant environment.

It is best to use the zone approach that can help you isolate the following:

- instances
- containers
- applications
- full systems

Identity and access management

To protect your data, you must implement identity and access management policies. Strict access to data must be implemented through policies that use access control lists. You also need to ensure that the privileges are role-based. Each access to data must be monitored and tracked.

Monitoring

After moving an application and its data to the cloud, users will use them. You must ensure that user actions are being monitored, especially looking for malicious actors that may be trying to seek a gap in your defense.

Password Usage

You must apply password policies in a cloud environment. You must ensure that users are not using simple passwords, and passwords must change after a certain duration. You should also implement account lockout policies. Most cloud service providers allow you to configure password policies.

Vulnerability management

Most cloud service providers perform vulnerability management of their environment. If that is being done, you should check the report. If you have deployed a custom web application in the cloud environment, you must ensure that you perform a vulnerability assessment.

Patch Management

Each cloud service provider uses one or the other method to perform patch management. While the cloud service provider will take care of the usual applications and the operating system updates, you will have to focus on the deployed custom applications. You need to ensure that all vulnerabilities are patched with the latest updates.

Alerts and Reporting

You need to check the available reporting with the cloud service provider. You can also use tools like SIEM to raise alerts based on the events.

Incident Response Plan

You must ensure that the cloud service provider has an incident response plan to tackle any incident that may occur. A cloud service provider must have the ability to detect and respond to security incidents.

There are no screenshot items for this exercise.