========== Cloud Hacking ==========

Infrastructure as a service (IaaS) : SYSADMIN
provides virtual machines and other abstracted hardware and operating systems which may be controlled through a service API

Platform as a Service (PaaS) : DEVELOPER
offers development tools, configuration managements, and development platforms on demand that can be used by the subscribers to develop custom application.
ex : Google App Engine, SalesForce, or Microsoft Azure.

Software as a service (SaaS) : END CUSTOMER
Offers software to subscriber on-demand over the internet
ex : Google Docs

Identity as a Service (IDaaS) :
Offers IAM service including SSO , MFA, IGA, and intelligence collection
ex. Onelogin

Security as a Service (SECaaS) :
Provides Penetration Testing , authentication, intrusion detection, anti malware, security incident, and event management services
eg. McAfee Managed Security Services

Container as a service (CaaS) :
Offers virtualization of container engines, and management of container, application and clusters through a web portal or API
ex. Google Kubernetes Engine (GKE)

Function as a Service (FaaS) :
Provides a platform for developing, running and managing application functionalities for microservices
eg. Google Cloud Function, Microsoft Azure Functions

Cloud Deployement Model :

Public Cloud : Open for Public use
Private Cloud : Single organization only
Community Cloud : Several organization from a specific community
Hybrid Cloud : Combination of two or more clouds
Multi clouds : Combines workloads across multiple cloud vendors

Containers Vs Virtual Machines :

Virtualization is the ability to run multiple operating system on a single physical system and share the underlying resources such as server, storage devices, or network.

Containers are placed on the top of one physical server and host operating system, and share the operating system's kernel binaries and libraries , thereby reducing the need for reproducing the OS

What is Docker ??

Docker is an open source technology used for developing, packaging, and running application and all its dependencies in the form of containers, to ensure that the application works in a seamless environment.

Docker provide a **Platform as a Service (PaaS)** through OS-level virtualization and deliver **containerized software packages**

What is kubernetes ??

Kubernetes , also known as **K8'**s is an open source , portable, extensible , orchestration platform developed by Google for **managing containerized application** and **microservices**.

Kubernetes provides a resilient framework for managing distributed containers, generating deployement patterns , and performing failover and redundancy for the application.

Kubernetes Features :
1. Service discovery
2. Load Balancing
3. Storage orchestration
4. Automated Rollout and rollbacks
5. Automatic Binpacking
6. Self healing
7. secret and configuration management

Cloud Attacks :

1. **Hijacking using Social Engineering**
2. **Service Hijacking Network Sniffing**
3. **Side Channel Attacks or Cross-guest VM Breaches**

4. **Wrapping Attack** : A Wrapping attack is performed during the translation of the **SOAP** message in the TLS layer where attacker **duplicate the body of the message** and send it to the server as a legitimate user.

5. **Man in the cloud (MITC) Attacks** :

- Man in the cloud attacks are an advanced version of man in the middle (MITM) attacks
- In the MITM attacks, an attacker uses an exploit that intercepts and manipulates the communication between two parties while the MITC attacks are performed by abusing cloud files synchronization service such as google drive or drop box for Data compromise, command and control(C&C), data exfiltration, and remote access.
- the attacker tricks the victim into installing a malicious code, which plants the attacker's synchronization token on the victim's drive.
- then the attacker steal the victim's synchronization token and uses the stole token to gain access to the victim's files
- later, the attacker restores the malicious token with the original synchronized token of the victim, thus returning the drive application to its original state and stays undetected .

6. **Cloud Hopper Attack :**

Cloud Hopper Attack are triggered at the **managed service provider (MSP)** and their users Attacker initiates **spear-phishing mails** with the custom-made malware to compromises the account of staff or cloud service firm to obtain confidential information.

7. **Cloud Cryptojacking** :

- Cryptojacking is the unauthorized use of the victim's computer to **stealthily mine digital currency**
- Cryptojacking attacks are highly lucrative , which involve both external attackers and rogue insiders

- To perform this attack, the attacker leverage attack vector like cloud misconfiguration, compromised websites, client or server-side vulnerability.

8. **Cloudborne Attack** :

- Cloudborne is a vulnerability residing in a **bare metel cloud** server that enables the attacker to implant a **malicious backdoor** in its firmware
- the malicious backdoor allow an attacker to bypass the security mechanism and perform various activities such as watching new user's acitivity or behaviour, disabling the application or server , intercepting or stealing the data

Other Cloud Attacks :

1. Session Hijacking using XSS attacks
2. Session Hijacking and Session Riding
3. Domain name system Attacks
4. SQL injection attacks
5. Cryptanalysis attacks
6. DoS and DDoS Attacks
7. Man in the Browser
8. Metadata spoofing attacks
9. Cloud Malware Injection Attacks

What is Cloud Hacking :

Attackers Exploit vulnerabilities existing in the cloud technologies to perform various targeted **high profile attack** on cloud storage systems, compromising the corporate and customer's data. The main objective of Hacking the cloud environment is gaining access to user's data and blocking access to cloud service

Enumerating S3 Buckets :

- **Simple Storage Service (S3)** is a scalable cloud storage service used by amazon AWS where files, folder, and objects are stored ia web APIs.
- Attackers often try to find the bucket's location and name to test its security and identify vulnerabilities in the bucket implementation.

Reverse IP Search :
Attackers uses search engines such as **bing** to perform a reverse IP Search to identify domains of target S3 buckets

Advanced Google Hacking :
Attackers use advanced Google search operators such as "inurl" to search for URL's related to target S3 Buckets