Module 19 cloud computing

1 What is cloud computing

2 types of cloud computing

- ✓ Public Cloud
- ✓ Private Cloud
- ✓ Hybrid Cloud
- ✓ Community Cloud

3 what is container?

1 task lazys3 to brute force AWS s3 buckets using lazys3 tool

Task2 scanner the bucket file

Task3 perfrome Vulnerablity docker image using trivy

1 What is cloud computing

Cloud computing is a technology that allows users to access computing resources—such as servers, storage, databases, networking, software, and analytics—over the internet, instead of using local servers or personal devices. It offers on-demand availability of these resources, providing flexibility and scalability according to business needs.

Cloud computing operates on a pay-as-you-go model, which helps reduce costs by eliminating the need for heavy upfront investments in hardware and maintenance. There are different types of cloud services, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

Cloud environments can be public, private, or hybrid, depending on how resources are managed and who can access them. Key benefits of cloud computing include high availability, disaster recovery, automatic updates, and support for remote work. It enables organizations to innovate faster and focus on their core operations rather than managing IT infrastructure.

2 types of cloud computing

✓ Public Cloud:

Public cloud services are provided by third-party vendors (like AWS, Microsoft Azure, or Google Cloud) over the internet. The infrastructure is shared among multiple users (tenants), offering scalability, flexibility, and cost efficiency on a pay-as-you-go basis.

✓ Private Cloud:

A private cloud is dedicated to a single organization and can be hosted on-premises or by a service provider. It offers greater control, security, and customization, ideal for businesses with strict regulatory or data privacy needs.

✓ Hybrid Cloud:

Hybrid cloud combines public and private cloud environments, enabling data and applications to move between them. This provides flexibility, scalability, and better security control depending on the workload requirements.

✓ Community Cloud:

A community cloud is shared by multiple organizations that have common concerns, such as compliance, security, or mission. It is jointly managed and supports

collaborative efforts while keeping sensitive data protected.

what is container?

A **container** is a lightweight, standalone, and executable software package that includes everything needed to run an application—such as the code, runtime, system tools, libraries, and settings. Containers isolate applications from the host system and from each other, ensuring consistency across different computing environments.

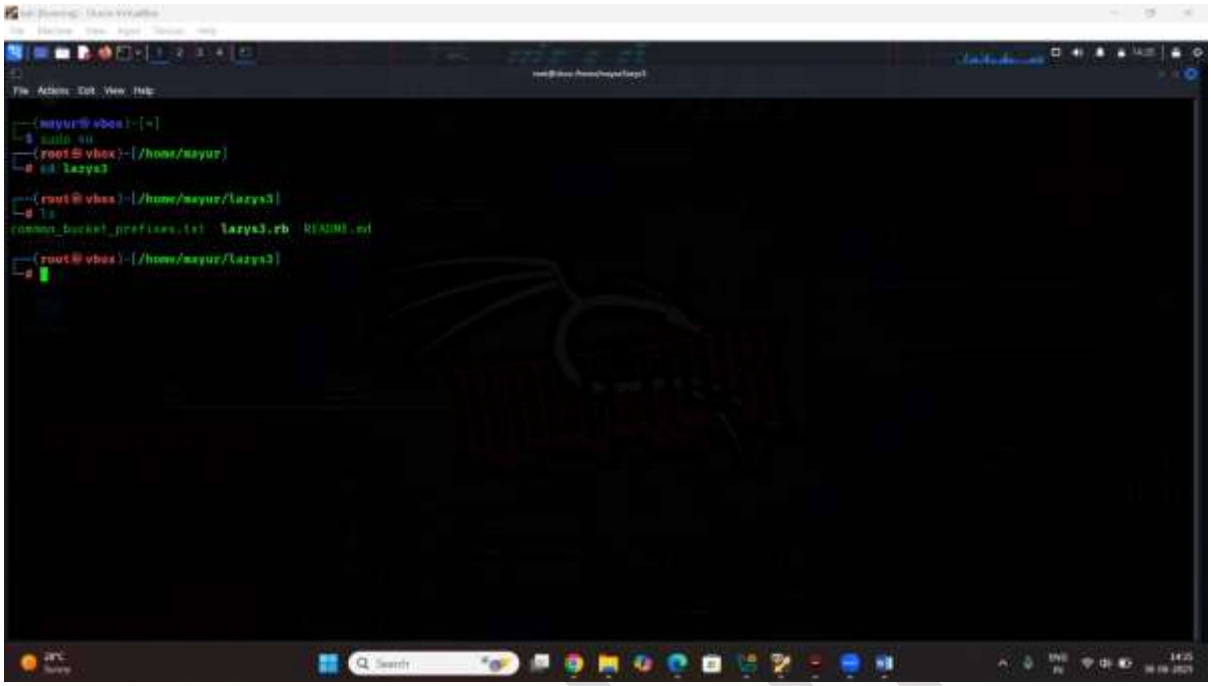
Unlike virtual machines, containers share the host operating system's kernel, making them faster to start, more efficient, and less resource-heavy. Tools like **Docker** and **Kubernetes** are commonly used to create, manage, and orchestrate containers in cloud and enterprise environments.

1 task lazys3 to brute force AWS s3 buckets using lazys3 tool

Download the lazys3 github

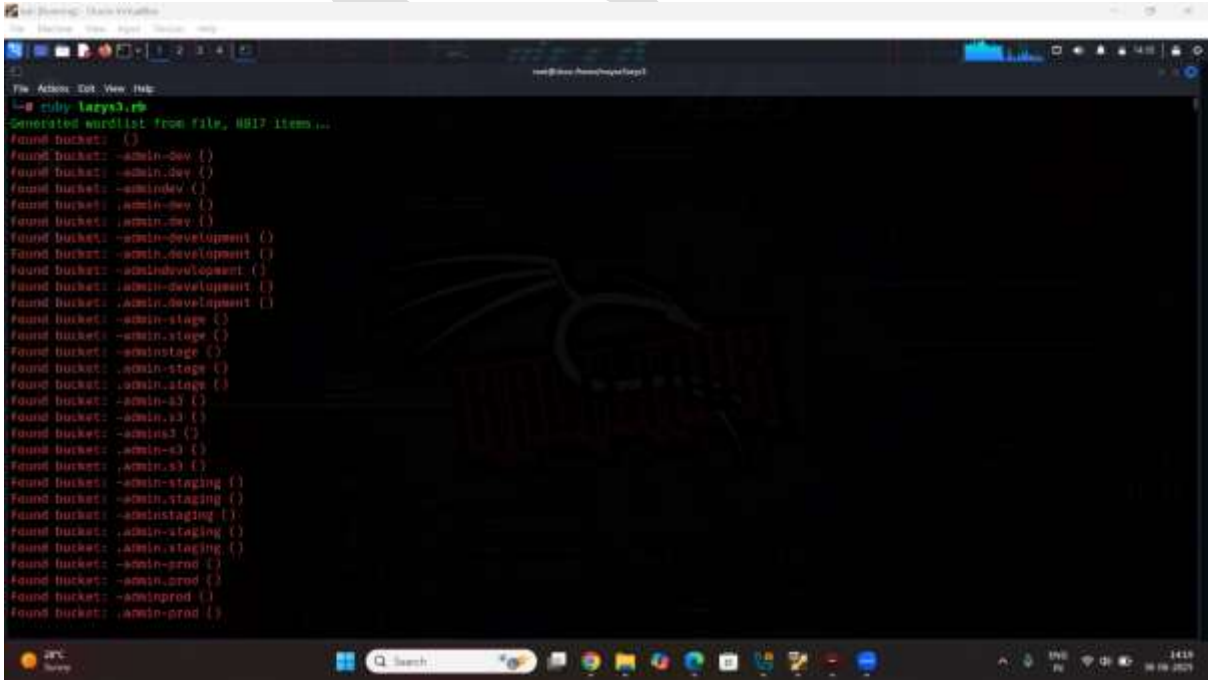
Step1 start the kali linux open the terminal

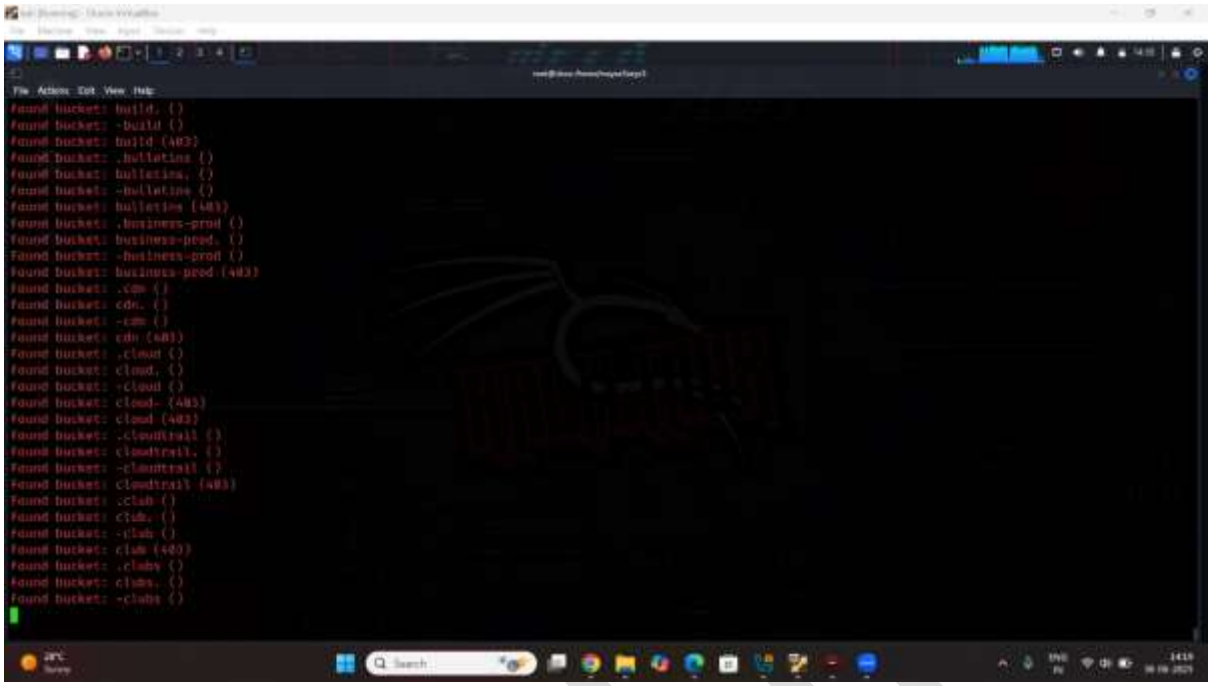
Step2 go to cd lazys3



Step3 chmod tx lazys3.rb

Step4: ruby lazys3.rb





S3Scanner

🔍 What is S3Scanner?

S3Scanner is an **open-source AWS S3 bucket enumeration tool** that helps **security professionals, penetration testers, and bug bounty hunters** identify publicly accessible or misconfigured **Amazon S3 buckets**.

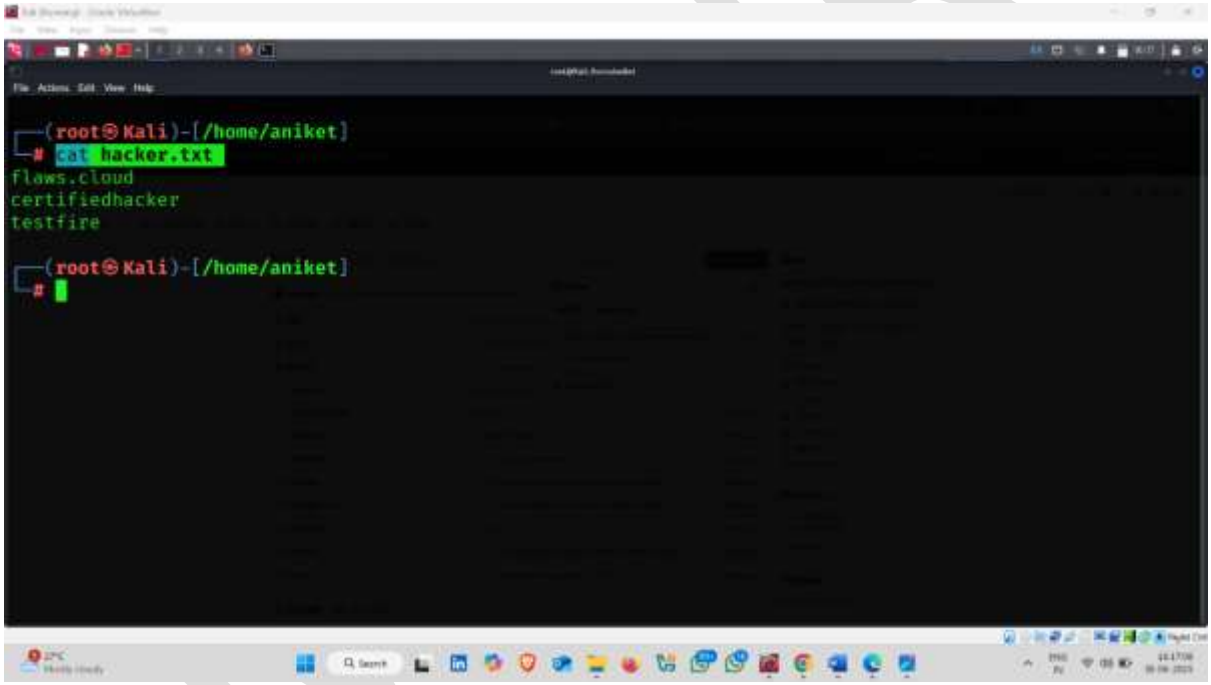
❓ Simple Definition:

S3Scanner scans a list of potential S3 bucket names and tells you which ones exist and whether they are publicly accessible.

🛠

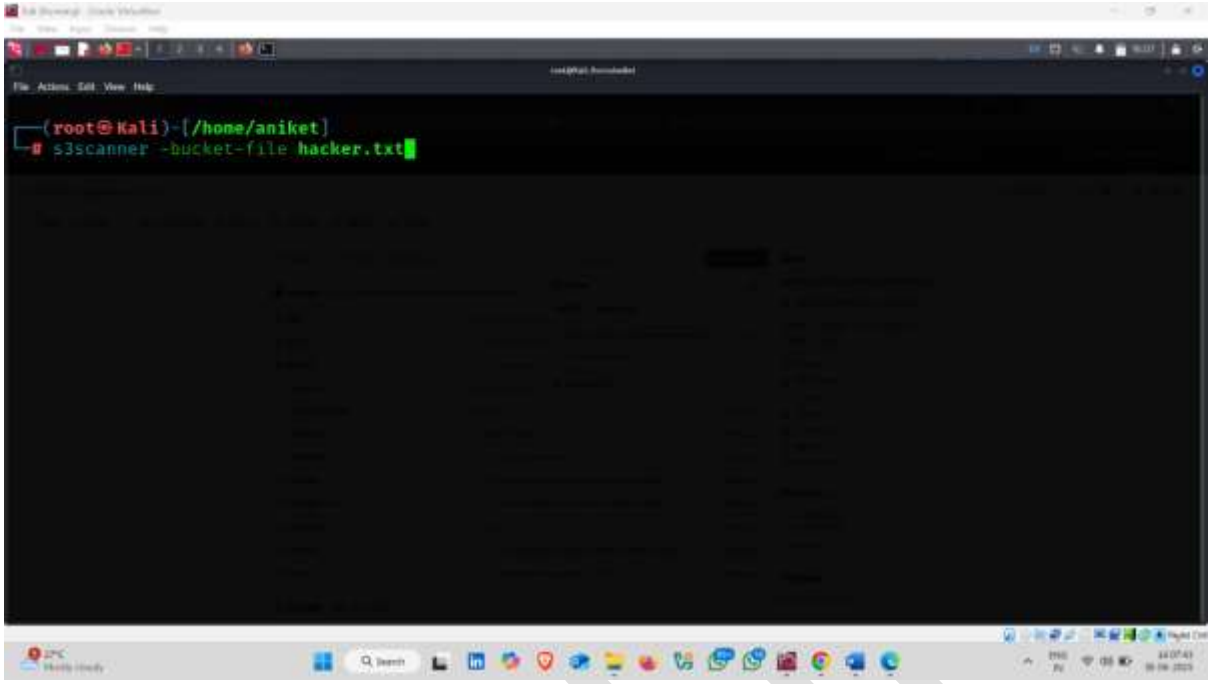
How to use it -:

- I have already one txt file that contain 3 websites

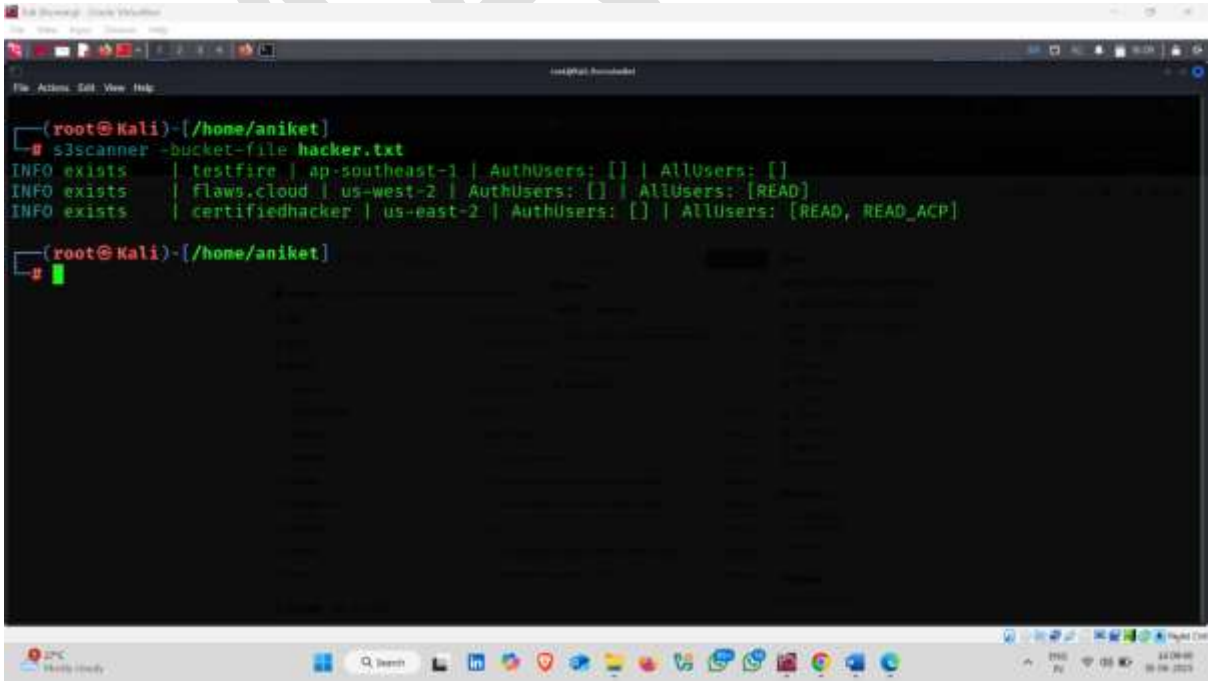


- Type following command

Command -: s3scanner -bucket-file hacker.txt

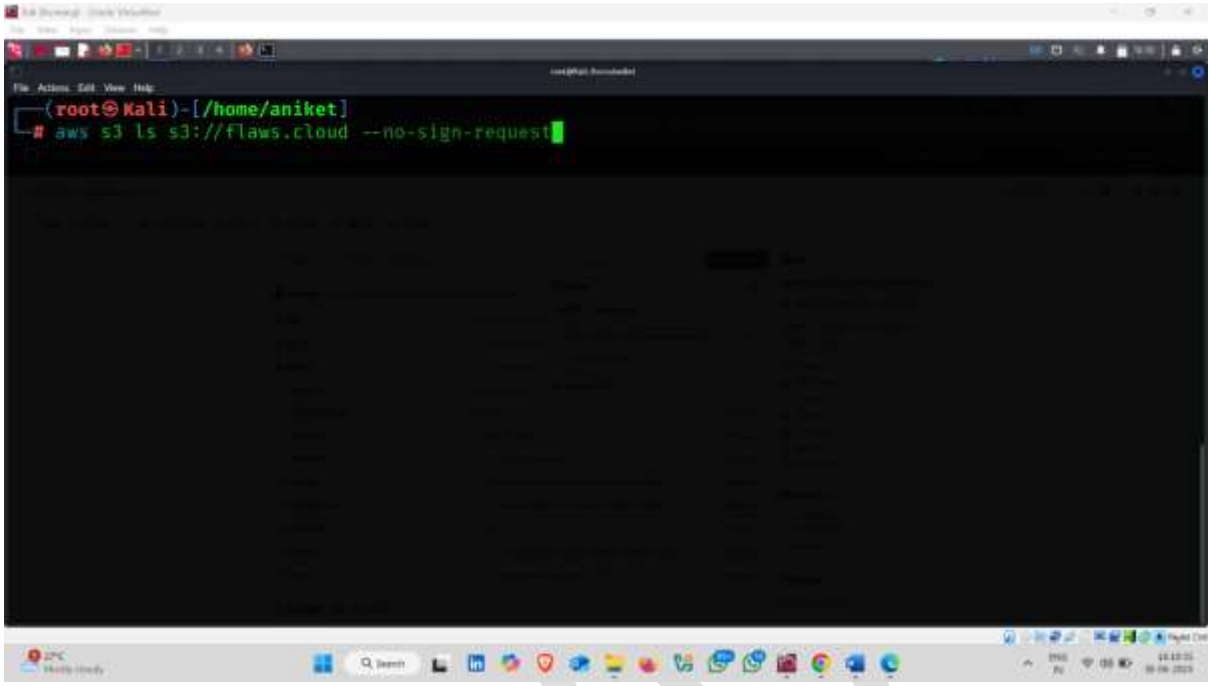


- **S3Scanner found** three existing S3 buckets: **flaws.cloud** and **certifiedhacker** are publicly readable, while **testfire** exists but is private. **certifiedhacker** also exposes its access control policy (READ_ACP).

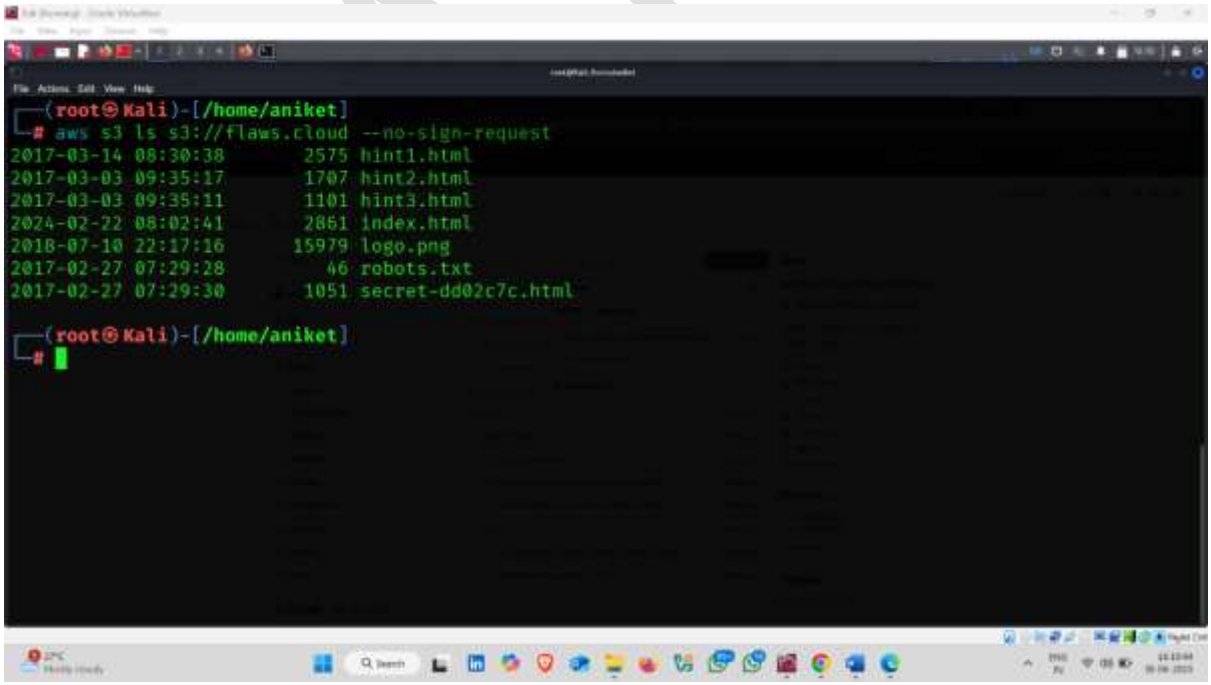


- Type next command

Command -: aws s3 ls s3://flaws.cloud –no-sign-request



- Result ☑ 👇



Task3 perfrom Vulnerablity docker image using trivy

Trivy (pronounced *"triv-ee"*) is a **free and open-source vulnerability scanner** used to find **security issues** in:

- 🐳 Docker containers
- 🎁 Operating systems & packages
- 📝 Infrastructure as Code (IaC) (e.g., Terraform, CloudFormation)
- ☁️ Cloud services (AWS)
- 📄 SBOMs (Software Bill of Materials)

❓ Simple Definition:

Trivy is a tool that quickly scans your container images, code, or cloud for **vulnerabilities and misconfigurations** before you deploy them.

How to use it -:

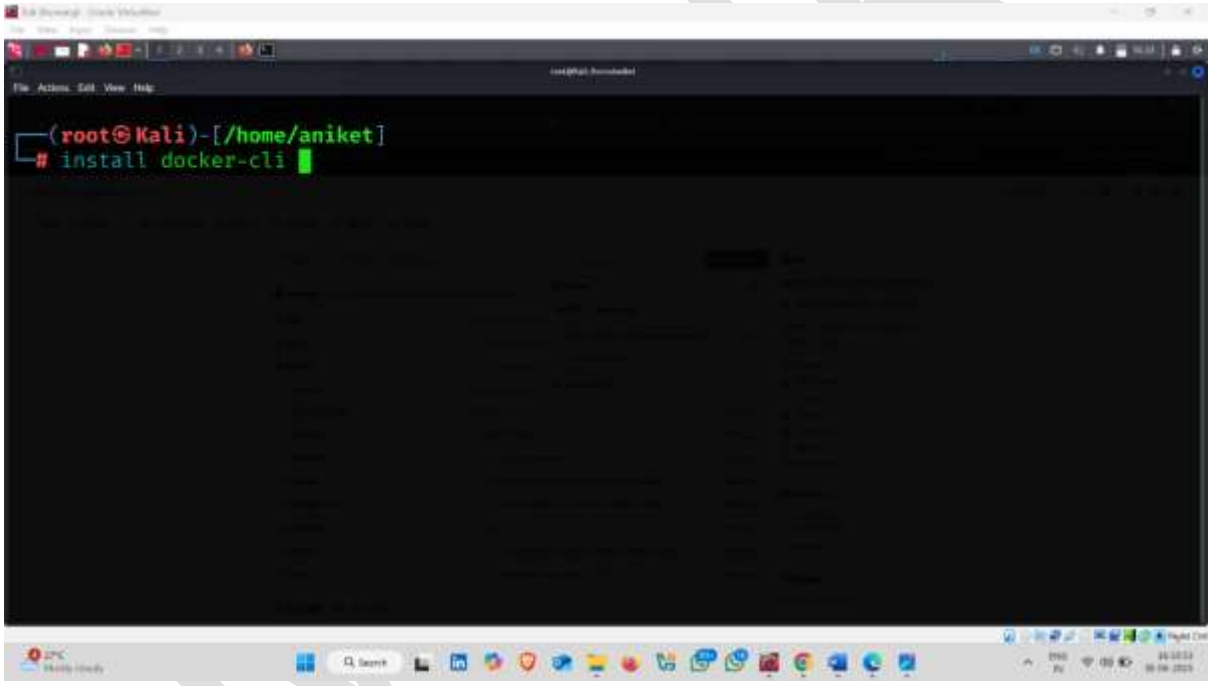
- Type following command

Command -: install docker-cli

Explanation -:

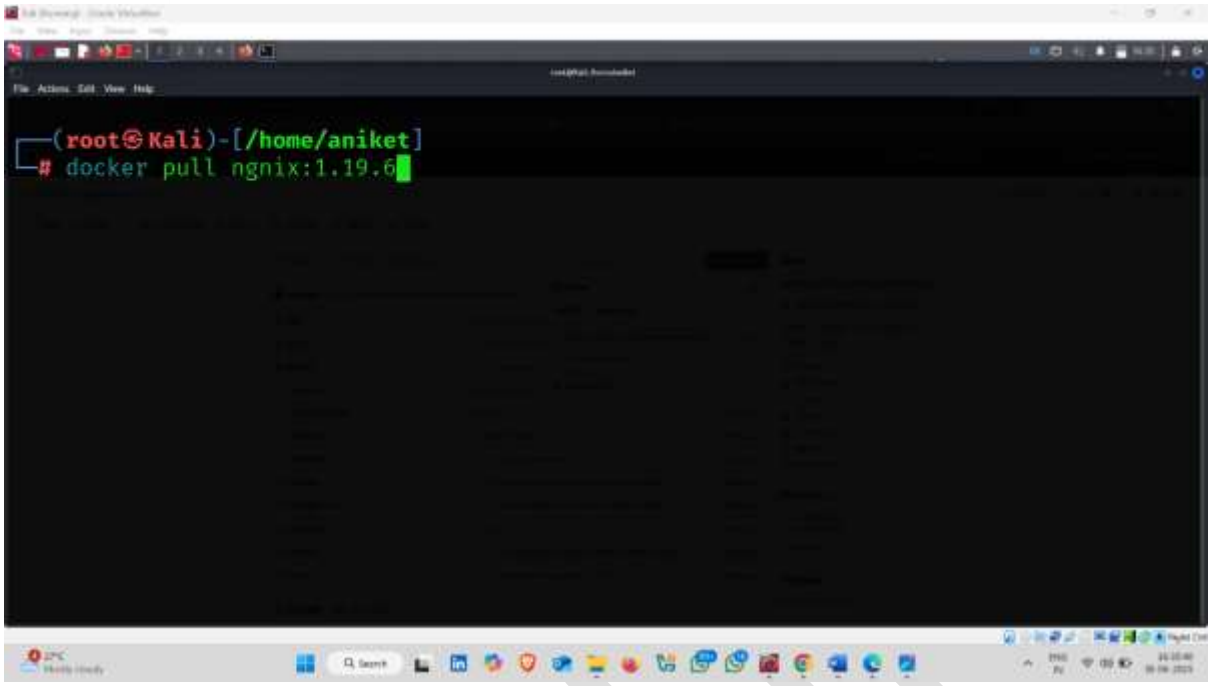
This command installs only the Docker Command Line Interface (CLI) — which means:

You can run docker commands (like docker pull, docker run, etc.) on the system.



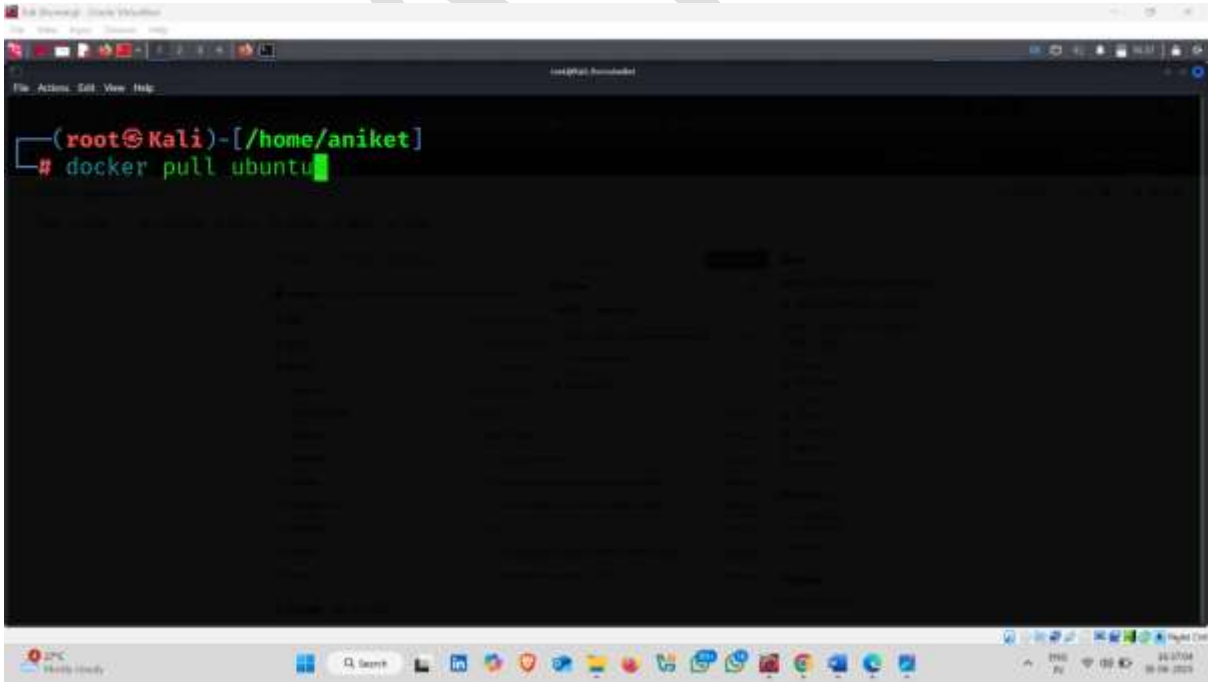
- Type next command

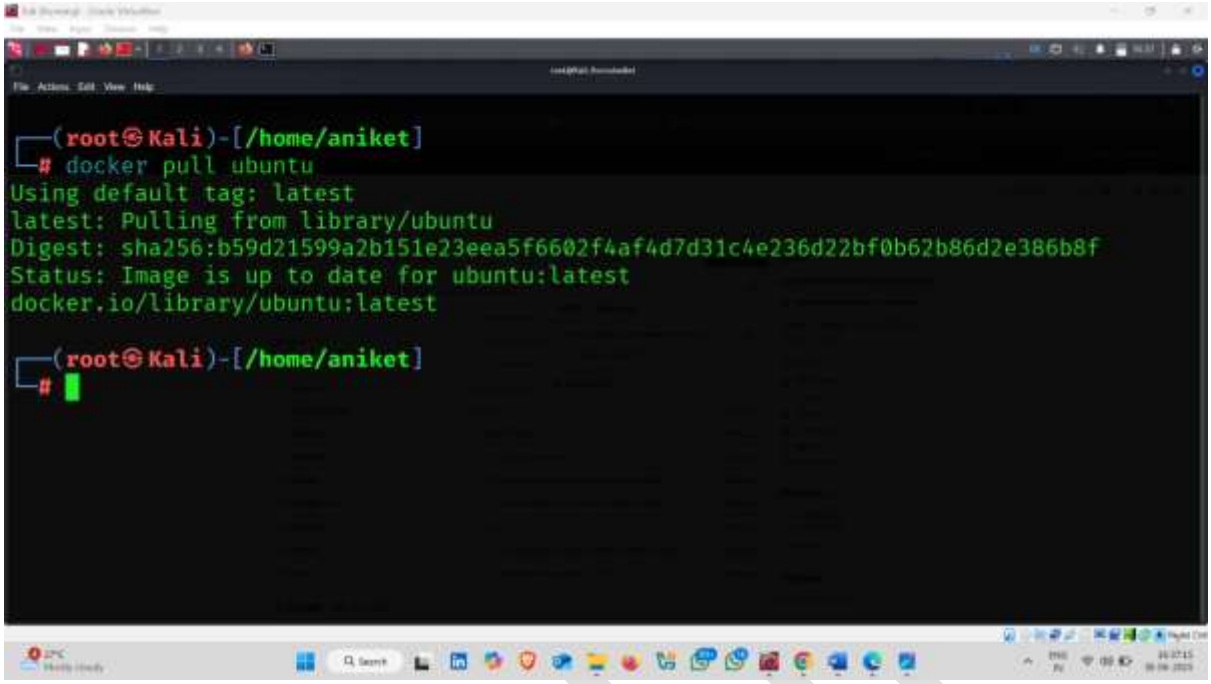
Command -: docker pull ngnix:1.19.6



- Type next command

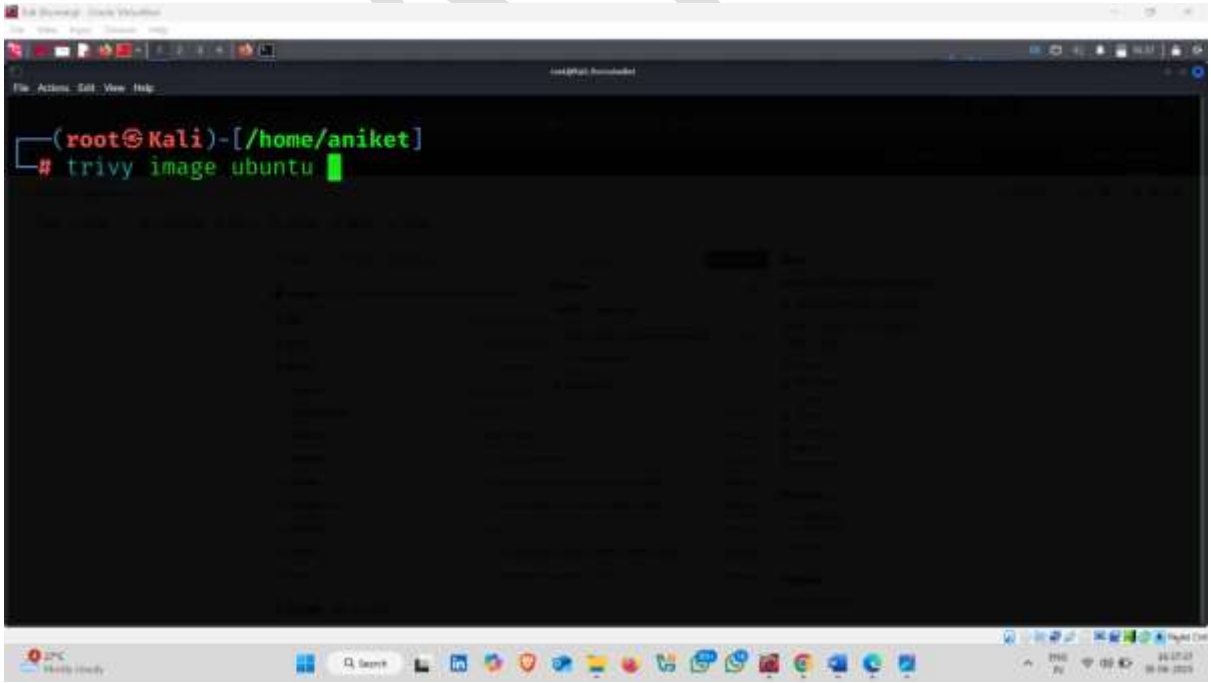
Command -: docker pull ubuntu

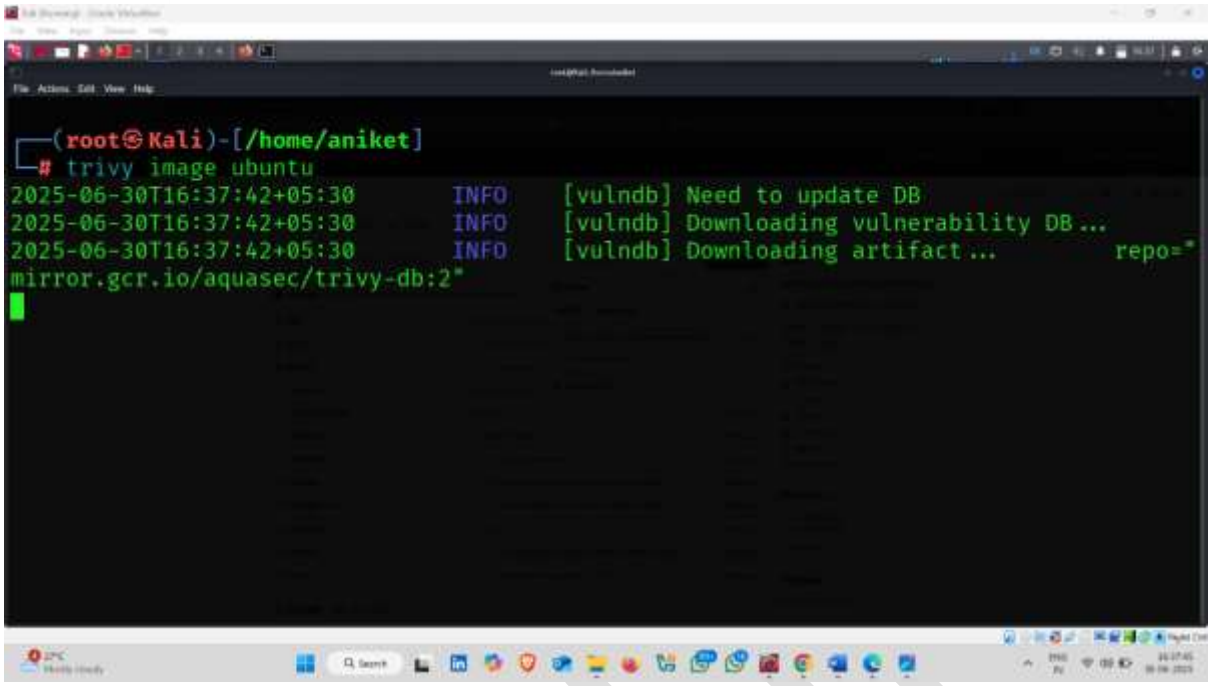




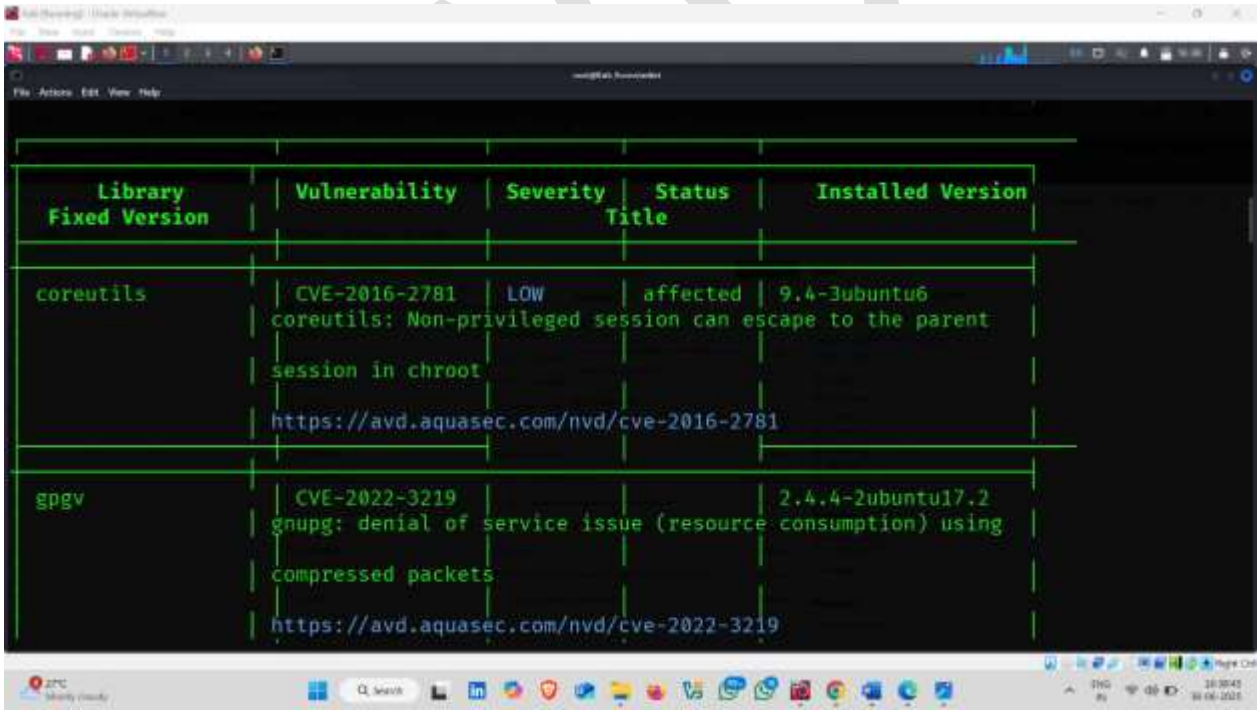
- Next command

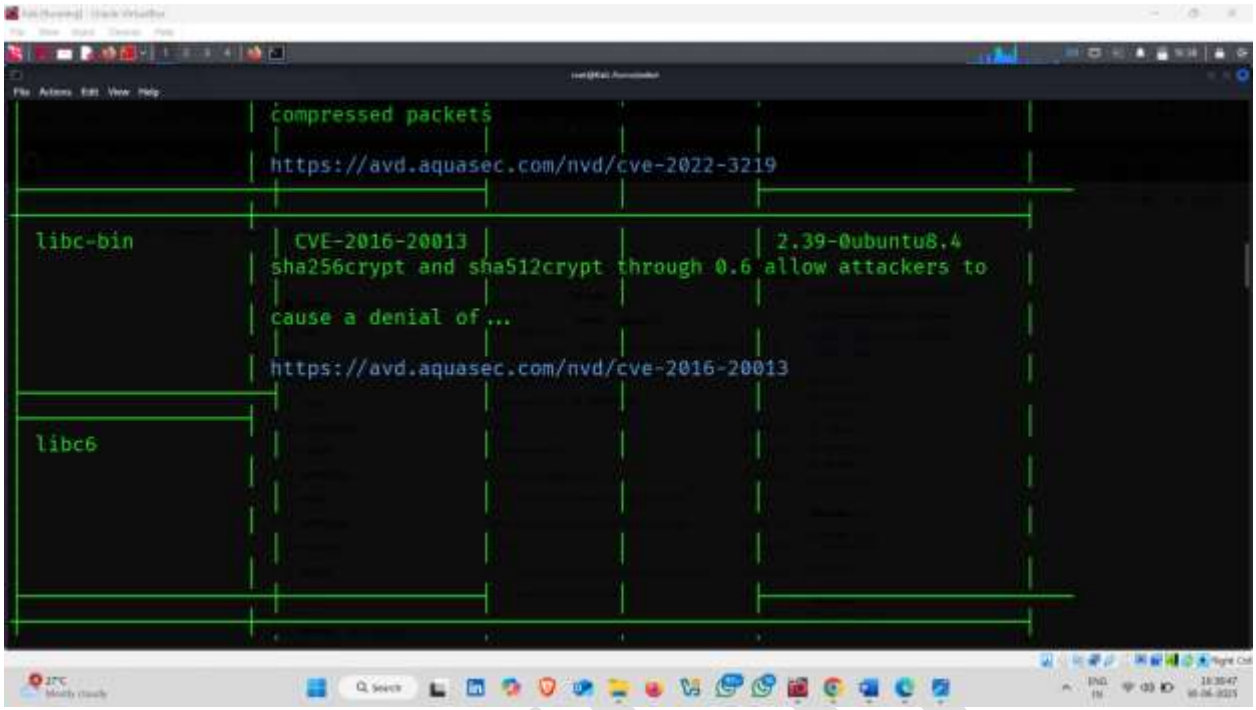
Command -: trivy image ubuntu





- Result – vulnerabilities found 👇✓




compressed packets
https://avd.aquasec.com/nvd/cve-2022-3219
libc-bin
CVE-2016-20013
2.39-0ubuntu8.4
sha256crypt and sha512crypt through 0.6 allow attackers to
cause a denial of ...
https://avd.aquasec.com/nvd/cve-2016-20013
libc6