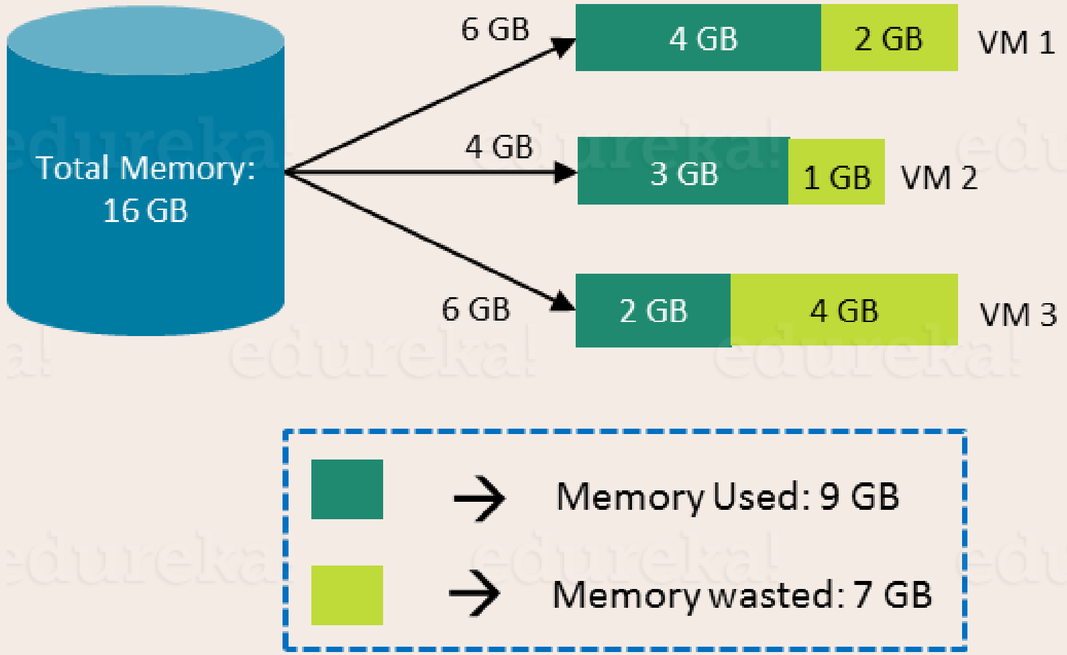
FORENSIC BASICS OF DOCKERS AND MALWARE

BY-ISHA
INTERN DIGTAL(4N6)

WHAT IS DOCKER?

- Docker is a tool designed to make it esaier to create, deploy and run applications by using containers.
- With the help of containers, the developer can be assured about the application being run on any other Linux machine regardless of the customised setting[differing from the mavhine used for writing and testing of code]
- A virtual machine but with a slight difference.
- Gives a significant performance boost and reduces the size of application.
- Open source.

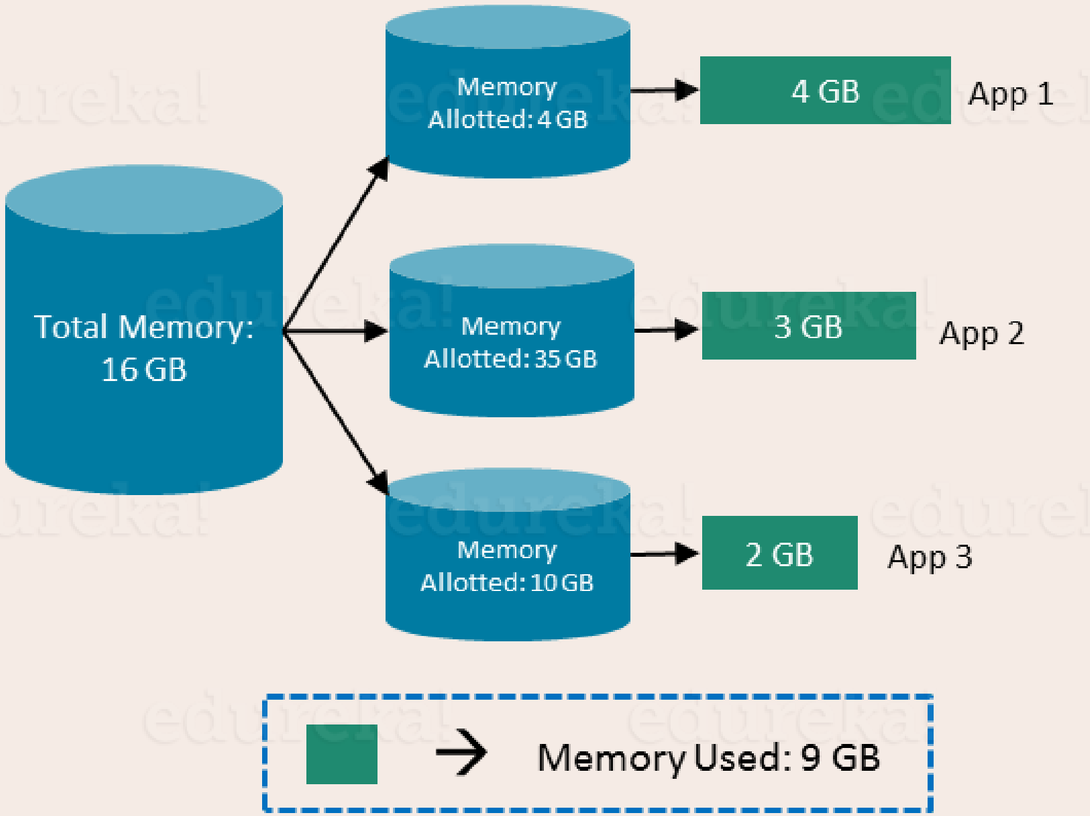
In case of Virtual Machines



7 Gb of Memory is blocked and
cannot be allotted to a new VM

In case of Docker

edureka!



Only 9 GB memory utilized;
7 GB can be allotted to a new Container

INSTALLATION OF DOCKER

When talking about Arch linux environment system, We can install using following commands:

$sudo pacman - S docker

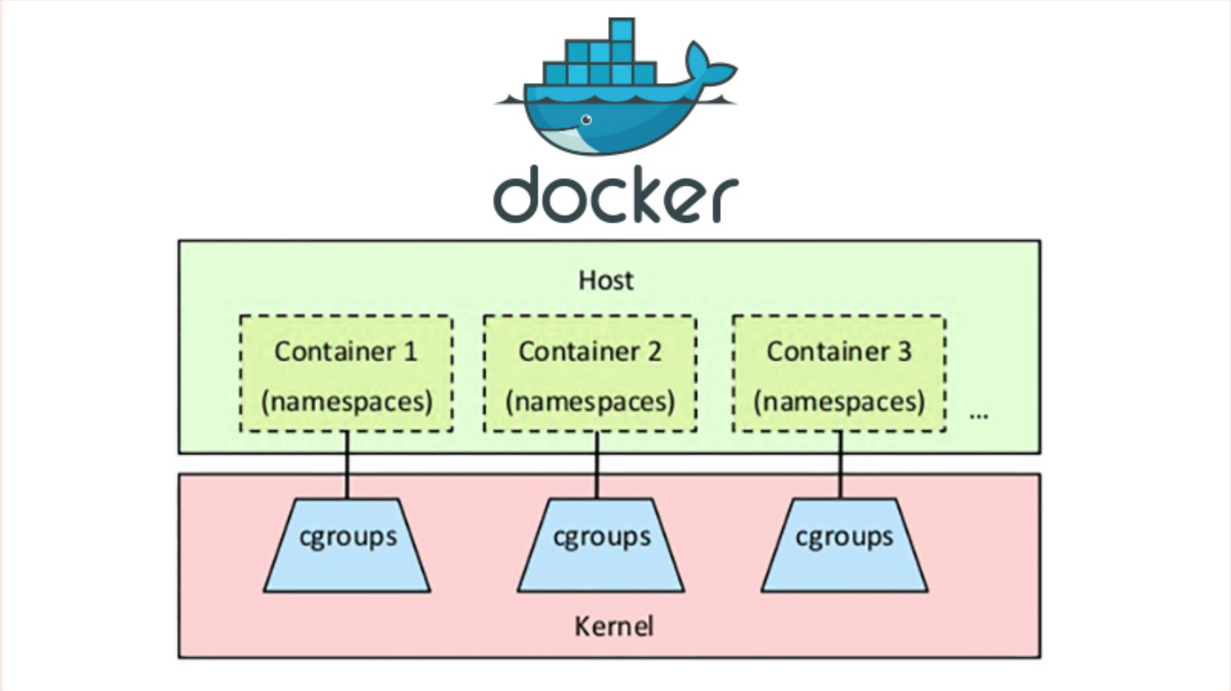
A system service unit would be created for Docker.

In order to start service

$ sudo systemctl start docker

In order to start Docker on system boot :

$ sudo systemetl enable docker



STANDARD "DOCKER VERSION"

APPLICATIONS USED

It is recommended to download the images using " docker pull <imagename> to the local storage .

- Working on a PE scanner, , static analysis of microsoft portable executable files could be done; using
  $docker run --rm -it -v /files:/home/nonroot/workdir remnux/pescanner pescanner<malicious. exe>

- While using JSdetox, which is a Javascript malware tool . The command used is
  $docker run --rm -p 3000:3000 remnux/jsdetox

- Using a spider monkey, you can analyze malicious scripts using the command
  $docker run --rm -ir -v /files:/source nacyot/javascript-spidermonkey:latest js <malicious.js>

- VirusTotal is a command line API client , that uses a command:
  $ docker run--rm -it malice/virustotal --api <api_key> lookup <hash>

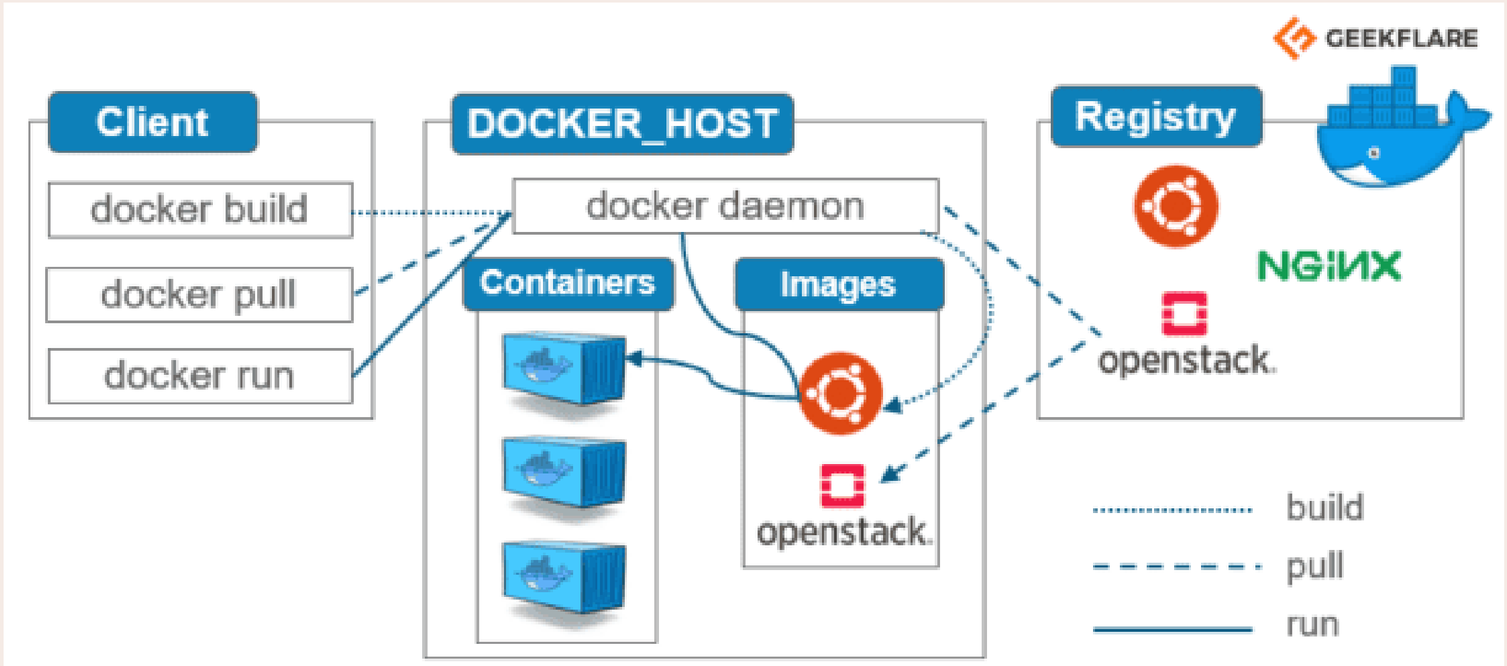
- Malcom , used in analysis network communications using graphical representations using network traffic & cross-reference using IoC sources, using command :
  $docker run -p 8080: 8080 -d --name malcom tomchop/ malcom -automatic

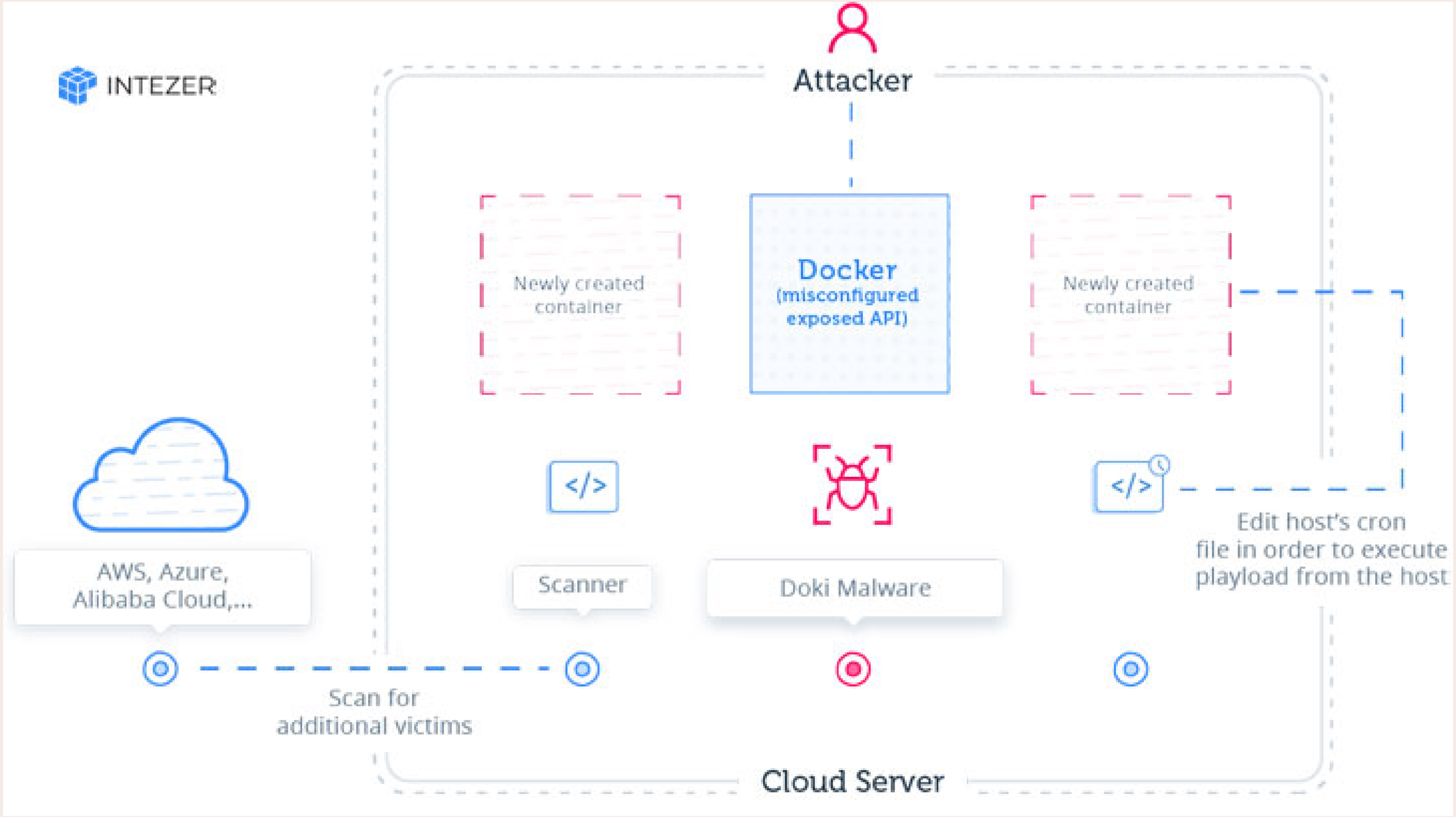
- Using YARA, pattern classification of files could be done; using the command

$docker run -it -v /evidences:/malware:ro \ -v /rules:/rules :ro blacktop/yara <suspicious _file>

- While using volatility, which is one of the most used memory forensics framework; using command :

$ docker run --rm -it -v ~/memdumps:/ home /nonroot /memdumps remnux/volatitlity bash




INTEZER
Attacker
Newly created container
Docker
(misconfigured exposed API)
Newly created container
AWS, Azure, Alibaba Cloud,...
Scanner
Doki Malware
Edit host's cron file in order to execute playload from the host
Scan for additional victims
Cloud Server

PLUS-POINTS OF USING DOCKER

- **Immutable:** Docker images are immutable, meaning they are unchanged over time. With a single configuration file, your analysis tools are is consistantly configured. This allow high confidence in the tool results and simplifies documenting the exact analysis tools used for court.

- **Portable:** Docker images run on Windows, macOS, Linux or on servers/in the cloud. This means forensic analysts can consistently run poewerful tools regardless of their operating system or deployment.

- **Isolated :** Docker has built in security, isolating the running containers from the underlying operating system and from each other. The containers can, though, be easily configured to share data where appropriate.

- **Traceable :** Docker provides a simple mechanism to understand the exact version of software you are running and how the Docker image is composed. This traceability simplifies documentation, reporting and consistency.

- **Scalable:** Docker has built in mechanisms to scale. With technologies such as Docker Swarm and Kubernetes (K8s), containers can be deployed, managed and scaled easily. These techniques can dramatically reduce the time needed for complex forensic analysis.

- **Lightweight:** Unlike traditional virtual machines, containers leverage the underlying operating system and are far more efficient using system resources. A forensic analysis can very quickly run a Docker containers while continuing to use their workstation.