Docker Security

Using Linux Kernel Features like

1)Namespaces – provide process isolation .

2)control groups – cgroups controls access to the resources .

3)Capabilities – allow granular specification of user capabilities and root user has access to every capability

4)TOMOYO –Linux kernel security module which implements mandatory access control.

5)AppArmor-s a Linux kernel security module that allows the system administrator to restrict programs's capabilities with per-program profiles. Profiles can allow capabilities like network access, raw socket access, and the permission to read, write, or execute files on matching paths.

6)SElinux(Security Enhanced Linux)- Security-Enhanced Linux (**SELinux**) is a Linux kernel security module that provides a mechanism for supporting access control security policies, including United States Department of Defense–style mandatory access controls (MAC).

7)Grsecurity – Linux security model.

Docker uses client and server architecture . Docker client sends a request to Docker Daemon . Uses TLS transport layer security foe secure communication.