Docker Run time security

Steps to Integrate AppArmor into a Nginx Container Image

1. **Understand AppArmor**: AppArmor is a Linux kernel security module that confines programs to a limited set of resources. It uses profiles loaded into the kernel to enforce security policies.

Create an AppArmor Profile:

- Start by creating an AppArmor profile specifically for Nginx. This profile will define what resources and capabilities Nginx can access.
- Here is an example of a basic AppArmor profile for Nginx (`nginx.apparmor`):

```
# Default profile for nginx
profile nginx /usr/sbin/nginx {
  # Allow read access to common libraries
  # (Example: adjust based on your Nginx configuration)
  /usr/lib/** r,
  /usr/sbin/nginx r,

  # Allow write access to logs and temporary files
  /var/log/nginx/** rw,
  /var/cache/nginx/** rw,
  /var/run/nginx.pid rw,
  /run/nginx.pid rw,

  # Allow network access if Nginx serves web traffic
  network inet,
  network inet6,

  # Allow access to necessary capabilities
  capability setgid,
  capability setuid,

  # Allow access to necessary devices (if applicable)
  /dev/log rw,
  /dev/null rw,

  # Deny everything else by default
  deny,

  # Include other AppArmor abstractions if needed
  # (e.g., to allow read access to other system resources)
  #include <abstractions/base>
}
```

Build or Modify Nginx Dockerfile:

- If you are building your own Nginx Docker image, you can include instructions to add your custom AppArmor profile (`nginx.apparmor`) to the image.
-

Example Dockerfile snippet:
FROM nginx:latest

Copy the AppArmor profile into the container
COPY nginx.apparmor /etc/apparmor.d/nginx

Set AppArmor profile to enforce mode
RUN ln -s /etc/apparmor.d/nginx /etc/apparmor.d/disable/
RUN apparmor_parser -r /etc/apparmor.d/nginx

Start Nginx
CMD ["nginx", "-g", "daemon off;"]

Run the Docker Container with AppArmor:

- When running the Nginx container, ensure that AppArmor is enabled and enforcing on your Docker host.
- Start the container with the `--security-opt` flag to specify the AppArmor profile:

docker run --rm -d --name mynginx --security-opt apparmor=nginx nginx:latest

Verify AppArmor Integration:

- Check the Docker container logs or use `docker inspect` to verify that the AppArmor profile (`nginx`) is applied and enforcing.By following these steps, you can integrate AppArmor into your base Nginx image container to enhance security by confining Nginx's access to system resources.

By following these steps, you can integrate AppArmor into your base Nginx image container to enhance security by confining Nginx's access to system resources.