Task 1

TPM is a small hardware chip that can securely store security keys. It plays an extremely important role in securing the computer from the time of boot-up by maintaining that only trusted software runs and no malware or anything nasty enters without prior knowledge to the owner. TPM can encrypt data and prevents unauthorized access to important files. The most important security feature of TPM is it can encrypt data and stop unauthorized people from accessing important files. The other good thing about TPM is that at the time of booting, it checks whether something has tampered with the system. This makes sure that hackers cannot modify anything. However, once booted and working, TPM does not give particularly good results. It's really focused on the boot process, so it doesn't offer much protection after that. Also, if one gains physical access to the computer, he might find his way to hack the TPM, though it is not easy to do.

Containers: Containers, on the other hand, are light and fast. Each container has its own files and dependencies, but they all share the same OS kernel. Containers are extremely popular because they are easy to establish and help developers transfer applications between diverse systems at runtime speed. From a security perspective, the isolation of applications from each other adds some protection. But all the containers share the same kernel; if there is a bug or problem in the kernel, it could affect all of them. Isolation isn't as strong in containers as in virtual machines, so a hacker could conceivably break out of one container and mess with others.

Sources:

1. Trusted Computing Group (TCG) - TPM Overview:
https://trustedcomputinggroup.org/resource/trusted-platform-module-tpm-summary/

2. Microsoft Documentation on TPM:
https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/tpm-recommendations

3. Docker Official Documentation: https://docs.docker.com/engine/security/security/