Task 2

Meltdown: This vulnerability uses weaknesses in speculative execution to access privileged memory unauthorized. Speculative execution is an optimization some CPUs use to predict the outcome of instructions before actually executing them. Meltdown bypasses these normal protections by causing speculative instructions to read sensitive data and leaks it to attackers. It mostly affects most pre-2018 Intel processors and a few AMD models. The mitigation widely used is Kernel Page Table Isolation, or KPTI; disabling speculative execution will have quite severe performance degradation.

Spectre: Spectre is another speculative execution attack, which exploits branch prediction vulnerabilities. Spectre, in turn, makes processors execute instructions along an incorrect code path, thus leaking data. It actually materialized in most Intel, AMD, and ARM processors since 1995 . Spectre does not target kernel memory but manipulates user-space programs in attempts to access sensitive information. Mitigation of Spectre is complicated because both hardware and software fixes are needed. This can be attenuated a bit by speculative execution barriers, browser security updates which reduce, for example, the resolution of timers without completely disabling speculative execution.

Foreshadow: It is a cache side-channel attack against Intel's Guard Extensions, leveraging the CPU's L1 cache in order to deduce sensitive data from protected enclaves. Most Intel CPUs starting from 2011 are affected. Foreshadow can break secure computation environments relying on sensitive data. Fixes involve microcode updates that stop speculative execution of the processor from leaking data. Sometimes, for complete mitigation, SGX may be disabled, but this affects applications relying on secure enclaves.

Each one targets various portions of speculative execution, including kernel memory that Meltdown takes advantage of, manipulated branch prediction in Spectre, and the exploited SGX cache mechanisms by Foreshadow.

Source : https://en.wikipedia.org/wiki/Transient_execution_CPU_vulnerability