Task 1:

Task 2:

Foreshadow is a cpu attacker that attempts to access L1 cache data via the method of speculative execution. This attack can lead to the disclosure of personal information saved on machine or in the cloud. It targets primarily Intel CPU with Software Guard Extensions (SGX). To mitigate it, patches supplied by the manufacturer can be installed. The real solution, according to Intel, is to simply replace the vulnerable chip with a secure one.

Retbleed is a speculative execution attack on x86 processors. It exploits retpoline, which was a mitigation for other speculative execution attacks. All chips that were vulnerable to Spectre were also vulnerable to Retbleed. Patches from the chip manufacturers were enough to contain it.

Downfall, also known as Gather Data Sampling (GDS), is a vulnerability found in some Intel chips that uses a transient execution vulnerability to reveal the contents of the vector registers. Intels SGX is also affected by this bug. According to Intel, microcode patches fix this bug.

Task 3:

- Malware and Viruses

Malware or Viruses downloaded off the internet can provide the attacker access to personal and sensitive information on your machine. While this categories spans a wide range of uses, one possible result is the installation of ransomware onto your machine. Another possible result is the deletion of possibly important files. MacOS has a built-in antivirus scanner known as XProtect, which scans and blocks malware known to the OS. The “Gatekeeper” application, another built-in part of MacOS, only allows trusted software from the App Store or other trusted developers to be installed.

- Exploiting Software Vulnerabilities

While this is also a very broad section, most exploited vulnerabilities allow the attack to gain some degree of control over your system. This can lead to sensitive information being leaked or stolen. MacOS gets regular software updates to protect against well-known attacks. SIP, or System Integrity Protection, restricts the most important system files from being modified.

- Phishing and Social Engineering

Attackers may exploit human psychology to gain access to account by tricking users into giving away their account information. This can lead to bank account information landing in the hands of attackers, who can then transfer money away from the victims bank account. Safari warns users when they visit a possibly fake website. Further, it is possible for users to set up either native or 3rd party 2FA apps to protect their accounts.

- Drive-by Downloads

Drive-by downloads is software that is installed without the users knowledge (or consent). This can give the attacker access to sensitive information, or give him control over the system. Safari blocks some malicious scripts, and gatekeeper prevents untrusted applications from being downloaded.

- Zero-Day Exploits

Vulnerabilities can be exploited by attackers before patches become available, or even before they are known to exist. Again, this can lead to many results, but usually gives the attack control of the system or access to information. MacOS’ SIP and Kernel Integrity may help protect against such attacks. Further, the “Install Security Responses” option is on by default, which installs security patches even without the users input.

- USB/Removable Media Attacks

Infected USB devices that are plugged into your machine can install malware. This can either give the attacker control of your system or steal sensitive information. MacOS limits most USB

functionality if the device is locked, making it difficult to install malware through a USB without the users knowledge. Gatekeeper also scans applications on USB devices before they are executed.

- Password Cracking

Cracking passwords gives the attacker access to the users accounts. This can lead to possible identity fraud, or financial problems. Built-in or 3rd party 2FA can help mitigate the risk.

Task 4:

- Application Logs

These logs can contain a variety of information, including information about any application errors or crashes, actions performed in the application, or debugging information. While specific applications may have folders in other directories, MacOs generally saves application logs within "/Library/Logs/…" . These logs may reveal threats by exposing unexpected activities within the application, or larger than usual data transfers to and from the application.

- Event Logs

Event logs contain information about events, for example the startup or shutdown of the machine, login attempts, devices connections, and system updates. Logs can be found in "/Library/Logs/…", or in the Console.app application. Event logs can show failed login attempts or changes to user privileges.

- Service Logs

These logs detail the lives of background services, as well as service errors and performance data. They can be found either in "/var/log/…" or "/Library/Logs/…". Services can be exploited, and evidence to this can be found is the service log files.

- System Logs

System logs log most low-level system information. This includes CPU, RAM, and SSD utilisation, but also changes in system settings. They can be accessed via Console.app or through "var/log/system.log". Attempts to exploit the kernel might be found here. Other system breaches may also be contained.

The easiest way to monitor log files on MacOS is through the Console.app application. This enables the user to easily search and filter for specific logs. It is also possible to directly access the log files, either via Finder or by accessing the files via terminal commands.

- https://sharath-kumar.medium.com/types-of-logs-5cc6cdb40482
- https://support.apple.com/en-gb/guide/console/cnsl1012/mac