Scenario 1

Asset

- The daily CSV report containing customer account balances.

Entry Point

- Staff members download the report from the shared directory for support questions.

Weak Spot

- Access is over supplied, analysts are able to see information they shouldn't be able to

Damage

- Personal information is accessible by people who shouldn't have access to.

CIA:

- Confidentiality

Reflection

- The entry point was difficult here. I had a hard time deciding between the staff members access the files, or the process that creates the files.

Scenario 2

Asset

- The linux config file

Entry Point

- The linux service that reads the config file

Weak Spot

- The configuration directory permissions allow write access to non-admin users.

Damage

- Poorly configured config files cause environment to not have the right configuration, enabling features in some and not in others.

CIA:

- Integrity

Reflection

- The weak spot was difficult here. Since it was vague in what permissions were granted or already exited when it says they were "widened".

Scenario 3

Asset

- The deprecated pipeline binary.

Entry Point

- The scheduled validation task executes the binary.

Weak Spot

- The deprecated pipeline binary exists on the host file system.

Damage

- Transformed values show discrepancies compared to expected output.

CIA:

- Integrity

Reflection

- It was tough to find the right Asset and Entry point here. Since they were technically two pipelines, the main and the deprecated one.