ADVASARY EMULATION PRACTICE

Notes:

Starting Caldera

- Navigated to the Caldera directory and started the server:
- python3 server.py --insecure --build
- Confirmed the server was accessible via browser on default port.
- Verified basic logging by appending test entries to Caldera log files.

Creating the Adversary

- Used Caldera GUI to create a custom adversary profile with test commands (CALDERA_TEST_ENTRY).
- Ensured the profile included multiple steps for emulation.

Deploying Agent

- Deployed a test agent on the host machine (manjira) via Caldera.
- Verified the agent connected successfully and was ready for emulation tasks.
- Generated log entries on the host system to simulate adversary activity.

Emulation Execution

- Ran the adversary against the deployed agent.
- Checked live log generation in Caldera:

  echo "CALDERA_TEST_ENTRY $(date)" | sudo tee -a /home/manjira/caldera/logs/caldera.log

- Observed log entries in real time; emulation successfully triggered the defined commands.

Log Collection with Filebeat

- Configured Filebeat to read caldera.log and test logs.
- Encountered initial issues:
- Small log files (<1 KB) were not being ingested.
- Filebeat registry preventing re-harvesting of files.
- Resolved by truncating logs to 2 KB and restarting Filebeat.
- Verified ingestion in Elasticsearch using a curl query:

  curl -u elastic:elkpass1 -s "https://192.168.1.39:9200/filebeat-*/_search?q=CALDERA_TEST_ENTRY&pretty" --insecure

Zeek Integration

- Appended test entries to /opt/zeek/logs/current/caldera_test.log.
- Verified Zeek successfully recorded entries.
- Filebeat configured to harvest Zeek log also faced small file issues; resolved as above.

Outcome

- Emulation was successful; adversary executed against the agent and produced observable log events.
- Attempts to capture screenshots of logs failed; screenshots got lost during process.

Observations

- Small log files need to exceed 1 KB for Filebeat filestream input to start ingestion.
- Filebeat registry may need clearing to pick up repeated test files.
- Zeek logs are a reliable alternative for log capture if Filebeat struggles.