

Homework

Grow your malware triage toolkit: extend a YARA rule, build an IOC extraction template, and run a classification drill.

Task 1 — YARA Rule Extension

Objective: Take the YARA rule from Exercise 4 and create a variant family rule.

Instructions:

- Loosen the strings to catch a second variant
- Tighten the condition to avoid false positives on common binaries
- Add a metadata comment explaining the trade-off

Deliverable: Two YARA rules (strict + loose) in one file with explanation.

Task 2 — IOC Extraction Template

Objective: Build a reusable AI prompt that converts any sandbox report into a structured IOC list.

Instructions:

- Prompt should output JSON (hashes, domains, IPs, paths, mitre_techniques)
- Include a schema in the prompt so output is stable
- Test it on the Exercise 1 sandbox report

Deliverable: The prompt file plus the JSON output from your test run.

Task 3 — Classification Drill

Objective: Create a short blind test: give yourself 3 of your earlier IOC sets renamed, and classify them family + capability without looking at the original

reports.

Instructions:

- Relabel 3 of your earlier analyses as sample A / B / C
- After a day off, classify each from IOCs only
- Compare to your original verdict

Deliverable: A table showing blind guess vs. original verdict, plus a reflection on what you relied on.