

Homework

Three tasks to deepen your AI-assisted binary and crypto workflow.

Complete the lab first.

Task 1 — Strings Classifier

Objective

Automate strings triage.

Instructions

1. Write a Python script that takes strings output and bins each string into: URL, path, command, format string, version, crypto constant, base64/hex blob, or noise.
2. Output a summary count per category + the top 5 most interesting strings.

Deliverable

`strings_triage.py`.

Task 2 — Crypto Weakness Catalog

Objective

Build a reference for future crypto challenges.

Instructions

1. For each crypto weakness you found in the lab (ECB, key reuse, weak RSA, etc.), write a one-paragraph explanation, a one-line detection heuristic, and a one-line exploit technique.
2. Format as a markdown reference you could use in any future CTF.

Deliverable

`crypto-weaknesses.md`.

Task 3 — YARA Rule

Objective

Codify binary detection.

Instructions

1. Using strings and hex patterns from the lab binary, write a YARA rule that would detect it on an endpoint.
2. Include at least 3 strings and one condition that limits FPs.

Deliverable

`detect.yar`.