

Answers

Reference answers for Lesson 06.

Part 1 — Lab Answers

Exercise 1 — Strings Triage

Expected findings

- At least one URL or IP (C2 indicator).
- File paths indicating target OS.
- A base64 blob that decodes to a meaningful string.
- One library or syscall name indicating capability.

Exercise 2 — Hex Dump Interpretation

Expected findings

- Correctly identified file format from magic bytes (PE, ELF, ZIP, etc.).
- At least one high-entropy region signaling encryption or packing.
- An embedded secondary file signature if the lab includes an overlay.

Exercise 3 — Disassembly Reading

Expected pseudo-C

A short, readable function that the student can explain in one sentence. If the assembly contains AES S-box constants or SHA-256 round constants, the AI should identify the primitive.

Exercise 4 — Cryptographic Challenge

Expected solve

At least one plaintext recovered, with a one-sentence explanation of the break: reused IV, weak key, ECB mode pattern, small RSA modulus, etc.

Final Exercise — Behavior Reconstruction

Expected chain

Strings suggest C2 → hex dump shows encrypted config blob → disassembly shows decrypt routine → crypto challenge provides the key to decrypt the blob.

Part 2 — Homework Answers

Task 1 — Strings Classifier

Expected shape

~80 lines of Python using regex patterns per category. The top-5 output should include the same high-value strings you identified manually in Exercise 1.

Task 2 — Crypto Weakness Catalog

Expected entries

At minimum: ECB detection (repeated ciphertext blocks), IV/nonce reuse, small RSA e with no padding, password hashing with fast algorithms, hard-coded keys.

Task 3 — YARA Rule

Expected rule

A rule with 3+ unique strings (to avoid FPs) and a `condition` clause like `uint16(0) == 0x5A4D and all of them` for a PE, or equivalent for an ELF.