

Part 1 — Lab Answers

Reference solutions for the lab exercises. Use these only after attempting the exercises yourself.

Exercise 1 — Sandbox Report Review

Common verdicts: dropper family (e.g., Emotet-like) based on Office macro → PowerShell → download second stage. MITRE: T1566.001 (spearphish attachment), T1059.001 (PowerShell), T1105 (ingress tool transfer), T1547 (registry run key persistence).

Exercise 2 — Hash Reputation

Highest priority: any hash in `%TEMP%` or `%APPDATA%\Roaming` with an executable extension. Second: files with name-extension mismatch. Identical imphash across different filenames = code reuse → same family.

Exercise 3 — Strings Intelligence

IOC list should include: 1-2 URLs, at least one registry key (Run / RunOnce), one scheduled task name, and decoded base64 containing a PowerShell one-liner. That decoded payload is the highest-value artifact.

Exercise 4 — YARA Rule

```
rule Suspicious_Dropper_Family_X {  
  meta:  
    author = "SOC"  
    date = "2026-04-10"  
    ref = "synthetic lab sample"
```

```
strings:
    $s1 = "UniqueStagingPath\\loader" ascii
    $s2 = { 48 8B 05 ?? ?? ?? ?? 48 89 45 F8 }
    $s3 = "http://c2.example/gate.php" ascii
condition:
    uint16(0) == 0x5A4D and filesize < 2MB and 2 of ($s*)
}
```

Final Exercise — Classification Report

Verdict: malicious (high confidence). Family: dropper, second-stage downloader.
Capabilities: persistence, C2, credential theft. Recommended: quarantine + fleet hash sweep + block C2 domain at DNS.

Part 2 — Homework Answers

Model answers for the homework tasks. Your solution may differ and still be correct.

Task 1 — YARA Rule Extension

The strict rule should match the exact sample; the loose rule relaxes one of three strings or drops the byte pattern. Explain the FP-vs-coverage trade-off.

Task 2 — IOC Extraction Template

A JSON schema with arrays for hashes, domains, ips, paths, mitre_techniques, plus a `confidence` field per entry. Output should validate against the schema.

Task 3 — Classification Drill

Blind accuracy is usually 60-80% on first try. The gap is a learning signal: what context did you lose when you stripped the reports?