Solved Capstone Project - Cybersecurity Assignments

Exercise 1:
1. Use encryption (e.g., AES) to secure cloud data, and transform it using encryption-at-rest and in-transit.
2. Hybrid cloud preferred: combines flexibility (public) and control (private).
3. Classify data into categories: Public, Internal, Confidential, and Restricted based on sensitivity.
4a. No, forensic integrity requires non-alteration of the original evidence.
4b. The analyst may have wanted to perform memory analysis or malware behavior inspection.
5. This PowerShell script is base64 encoded.

Decoded Analysis:
1. URL: http://badwebsite.com/xap_102b-AZ1/704e.php?l=zyteb4.gas
2. File: HSTHjnhc.exe
3. Folder: CommonApplicationData (C:\ProgramData)
4. ShellExecute runs the file as a new process in Windows.

Exercise 2:
1. Process injection: hiding malicious code in legitimate processes. Used in Emotet, Dridex, etc.
2. Methods: DLL Injection, APC Injection, Reflective DLL Injection, Process Hollowing.

Exercise 3:
1. Tools: Procmon, Process Explorer, Strings.
- Procmon: shows registry and file activity.
- Process Explorer: detailed info about running processes.
- Strings: extracts readable strings from binaries.
- All are used in dynamic analysis.

2. a. PE file structure with UPX-packed binary.
b. Sections define code, data, imports, etc.
c. UPX: executable packer.
d. Entropy: measures randomness, high entropy may suggest obfuscation.
e. Import: external functions used by the binary.
f. Functions: CreateFile, WriteFile, etc.

Exercise 4: Notification Summary
Emotet malware was delivered via phishing emails to users at Acme Inc.
Each email contained a malicious document which installed Emotet.
Systems ABC, CDE, and FGH were compromised.
Action: Disconnect infected systems, scan for malware, block malicious domain, educate users.

Scenario 1: First, conduct a risk assessment, patch critical systems, implement firewalls and SIEM monitoring.
Scenario 2: Block domain at gateway, update email filters, train users to spot phishing.
Red Team: Perform vulnerability assessment, use tools like Metasploit, report flaws with proof-of-concept.