965 | 968
C:78

Air University, Islamabad
Mid Semester Examination Spring 2025
Department of Cybersecurity

Subject:- Malware Analysis
Course Code: - CY328
Semester:- 4th (A+B)
Chair Department Signature:-

Total Marks:- 50

FM(s) Name:- Dr Syed Muhammad Sajjad
FM Signature:

Question 1	CLO 2	GA 5	Domain level Apply	Marks=[7*3] = 21

A financial institution has reported a suspicious email received by multiple employees. The email appears to be from the HR department, urging employees to download an attached PDF containing "updated salary details." One of the employees downloads and opens the attachment, which executes a hidden PowerShell script, creating a reverse shell connection to an external server. The attacker then moves laterally across the network, exfiltration customer financial data.
Using the Cyber Kill Chain framework, identify and explain each stage of the attack. What security controls could have mitigated this attack at different stages.

Question 2	CLO 3	GA 3	Domain level Analysis	Marks=[7 +7+6] = 20

An employee reports receiving a PDF attachment named "Urgent_Invoice.pdf" from an unknown sender. The security team decides to perform static analysis before opening the file. A tool like pdfid.py reveals the presence of /JS, /OpenAction, and /AA tags in the PDF structure.
Strings extraction detects encoded shellcode and suspicious function calls like Launch, SubmitForm, and getIcon().
The file hash is checked on VirusTotal, and 10 security engines flag it as malicious.
Using your knowledge of static malware analysis, answer the following:
a) What do the /JS and /OpenAction tags suggest about the PDF's behavior?
b) Why is strings analysis useful in identifying potential malicious activity in the PDF?
c) What are the next steps a security analyst should take to determine the full impact of this file?

Question 3	CLO 1	GA 1	Domain level Understanding	Marks=[5+4] = 9

a) Explain the concept of "packers" in malware. How do they affect analysis? Name two tools used for it.
b) What is static malware analysis? Name two tools used for the static analysis of malwares.