Air University
Mid Semester Examinations: Fall 2025

Student ID: _____

Subjective Part
(To be solved on Answer Books only)

Subject: Ethical Hacking and Defense
Class: BS CyS Morning F-23
Section(s): Morning F-23 (A & B)
Course Code: CY-330

Time Allowed: 120 Minutes
Max Marks: 50
FM's Name: Dr Syed M Sajjad
FM's Signature:

INSTRUCTIONS

- Attempt responses on the answer book only.
- Nothing is to be written on the question paper.
- Rough work or writing on question paper will be considered as use of unfair means.
- Tables / calculators are allowed ~~/not allowed~~.

Question 1	CLO :01	GA :01	Domain level : Understand	Marks = 10

A. An attacker's process is described below:

1. The attacker sends a crafted email to an employee.
2. The employee clicks a link, which installs a backdoor.
3. The backdoor communicates with a C2 server.
4. The attacker uses the backdoor to run whoami and scan the internal network.
5. The attacker finds and exfiltrates a sensitive customer file.

Map these 5 actions to the Cyber Kill Chain. Explain your mapping for each stage.

Question 2	CLO :02	GA :05	Domain level : Understand	Marks = 10

During the reconnaissance phase, you gather the following OSINT data on a target company:

- Email format: f.lastname@targetcorp.com
- LinkedIn: 20 employees, including "Jane Doe – Senior Network Engineer."
- Subdomains: dev.targetcorp.com, mail.targetcorp.com, vpn.targetcorp.com
- A public PDF file listing internal IP addresses (e.g., 10.1.5.x)

Explain how each of these four findings can guide your planning and execution of the next phase – Network Scanning in an authorized ethical-hacking engagement.

Question 3	CLO :03	GA :03	Domain level : Analysis	Marks = 10

You run an Nmap scan against a target IP and receive the following partial output:

```
Nmap scan report for 192.168.10.5
Host is up (0.012s latency).
PORT    STATE SERVICE    VERSION
21/tcp  open  ftp        vsftpd 2.3.4
22/tcp  open  ssh        OpenSSH 4.7p1 Debian 8ubuntu1
```

80/tcp open http Apache httpd 2.2.8
139/tcp open netbios-ssn Samba smbd 3.X
445/tcp open netbios-ssn Samba smbd 3.X
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5

From this output, analyze and identify three (3) potential vulnerabilities. Justify your reasoning for each vulnerability by linking the service, version, and the likely attack you would attempt next.

Question 4	CLO :04	GA :04	Domain level : Evaluation	Marks = 20

You have just been appointed Head of Cybersecurity at a private investment bank, covering all computer security aspects. You have been given a completed self-audit and observation of the operations, processes, policies, and behaviours, with computers, network, and cybersecurity in focus. The summary of the findings is as follows:

- Workstations are renewed every four or five years, and they are kept very up-to-date
- The server room is secured under lock and key, and the key is kept in the staff room, behind the door.
- The cleaner also has access to the room, unsupervised, and the room is actually kept clean. The cleaning is provided through a contractor, who seem to have good recruitment policies.
- Firewall – there is a very good firewall in place, as part of the Intrusion Prevention System, which is state-of-the-art.
- Antivirus – the virus database is regularly and automatically updated by the current provider. A Machine Learning-based antivirus has not been considered to keep the cost down.
- Cloud services – The customer database and all data services have been moved in the cloud, with a cloud provider, and they provide the security aspects as well. This was to reduce cost and increase efficiency.
- Staff training – training is being regularly provided online, once a year, through prerecorded videos and activities, and the newly recruited staff get the cybersecurity training in the next scheduled event. Training mostly consists of how to keep the passwords secure, not to browse the internet during working hours, and not to share sensitive information outside the company.
- There are quite a few staff policies in place about computer use. You asked about the use of social media by staff, but the answer was that "the company do not interfere with private matters of their staff".
- Staff are requested to regularly change their passwords every six months, and line managers are made responsible to enforce this on staff, for this to happen on a regularly basis.
- The members of staff who undertook the security self-audit and observation could not think of any other matters to report.

Your task:

You need to evaluate the findings and the current situation you have inherited in your new role, identify the strengths and weaknesses, and write a report to the Board of Directors, including a list of recommendations that you have about any improvements that are needed.

The list of the findings above is not exhaustive, and it is down to you to evaluate what important things may already be missing or that are not happening. It is safe to make assumptions as well, about any things that you consider very important but are not being applied or not happening, or are not being done properly in the organisation. In your evaluation, concentrate on the server room, antivirus, the cloud contract, staff policies and training, including the password policy, plus any assumptions, that you might want to make. You will need to justify your recommendations, especially if costs are associated with them, either as subscriptions, or as one-off payments.