593,594

# Air University

(Final-Term Examination: Fall 2025)

| | | | |
|---|---|---|---|
| Subject: | Ethical Hacking and Defense | Total Marks: | 100 |
| Course Code: | CY-330 | Date: | |
| Class: | BS-CYS | Time: | |
| Semester: | V | Duration: | 3 Hours |
| Section: | A/B | FM Name: | Dr. Sajjad |

HoD Signatures:______________ FM Signatures:______________

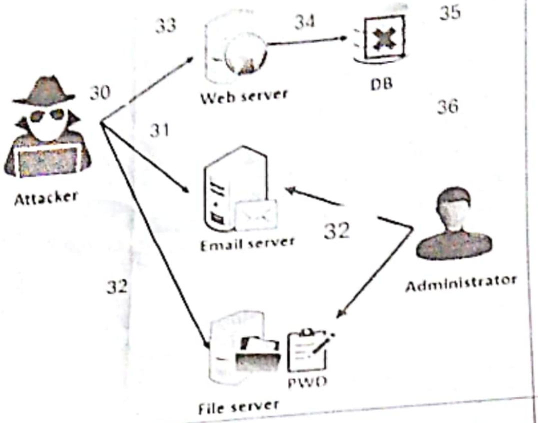
**Note:**

- **All questions must be attempted.**
- **This examination carries 45% weight towards the final grade.**
- **Understanding question is part of exam.**

| | | |
|---|---|---|
| | **(CLO 1)** | **20 Marks** |
| **Q. No. 1** | Explain the Following: (Diagrams are appreciated where needed)<br>a) Compare **MAC Spoofing** and **ARP Poisoning** in terms of attack method and impact.<br>b) Differentiate between **Firewall Evasion Techniques** and **IDS Evasion Techniques**.<br>c) Explain the difference between **OS Fingerprinting** and **Service Fingerprinting**.<br>d) What is **Banner Grabbing**? Explain its role in penetration testing. | 5+5+5+5 |
| | **(CLO 3)** | **30 Marks** |
| **Q. No. 2** | Mr. Umar works as a system administrator in **Global Tech Solutions**. Recently, the organization suffered a cyber incident where confidential business data was stolen and critical servers were rendered unusable.<br>A cyber forensic analyst, Mr. Fahad, was assigned to investigate the incident.<br>**Incident Description:**<br>The attacker began by performing network reconnaissance to identify active hosts and services. He discovered an exposed web application and an internal email service. The attacker then sent a fake invoice email to an employee, Ms. Ayesha, containing a malicious link.<br>Ms. Ayesha clicked the link and entered her login credentials on a spoofed webpage. Using these credentials, the attacker accessed the internal email system and found internal documentation referencing a shared file server. The attacker logged into the file server and obtained administrator credentials stored in a script file. | |

With administrator access, the attacker connected to the database server, copied sensitive records to an external location, and then executed commands that deleted the database and disabled backups.

**Question:**
Using the **MITRE ATT&CK framework**, map the above attack scenario to its relevant phases, write the phases for questions 30-36.



30 Marks

(CLO 3)

No. 3

Kerberos Version 4 and Version 5 are ticket-based authentication protocols designed to provide secure authentication over insecure networks. Both versions follow a structured authentication process consisting of multiple phases involving the **client, Authentication Server (AS), Ticket Granting Server (TGS)**, and the ***application server***.

a) Explain the **six (6) authentication phases of Kerberos V4 and Kerberos V5,** including:

1. **User Login / Initial Authentication**
2. **Authentication Server (AS) Request**
3. **Authentication Server (AS) Response**
4. **Ticket Granting Server (TGS) Request**
5. **Ticket Granting Server (TGS) Response**
6. **Service Server Authentication / Mutual Authentication**

For each phase, describe:

- **The entities involved**
- **The messages exchanged**
- **The tickets and keys used**
- How Kerberos V5 improves or extends the functionality compared to Kerberos V4 (e.g., encryption algorithms, ticket lifetime, mutual authentication, extensibility)

b) Highlight **key technical differences between Kerberos V4 and Kerberos V5** within these phases.

30

20 Marks

Q. No. 4 (CLO 3)

| | | |
|---|---|---|
| **Q. No. 4** | You are assigned the role of a **Cyber Security Instructor** to train new employees about malware threats and system defense.<br>a) Explain the **working phases of a computer virus**, including:<br>• Dormant phase<br>• Propagation phase<br>• Triggering phase<br>• Execution phase<br>b) Explain the **Trojan Horse attack lifecycle**, detailing:<br>• Infection vectors<br>• Installation techniques<br>• Backdoor creation<br>• Remote command execution<br>• Data theft or system damage | 20 |

**************** End of Question Paper ****************