University of Echahid Hamma Lakhdar
Faculty of Exact sciences
Level: 1st year IoT&Cyber Security Master degree

Module: System Security.
Date: 13-05- 2025.
Duration: 1 hr, 30 mins.

Final Exam

Exercise 1: (4.5 pts)

1- In Discretionary Access Control Policy, a user X has “rw” permission to File1 and File2 however user Y has no permission to File1.Explain how Y could steal File1’s data using a Trojan horse.

2- In Multi-Level Security, how many labels can be constructed from **N** security levels and **M** categories? Explain?

3- In Chinese Wall policy, Justify the second condition of writing.

Exercise 2: (6.5 pts)

In a hospital, various **roles** are defined to manage it. Each role has specific permissions associated with it, governing what actions they can perform.

- Receptionist: View demographic data, Schedule appointments.
- Medical Staff: View patient medical records (e.g., name, age, medical history).
- Emergency Room Doctor (ER Doctor): View and Modify all patient medical records in the facility,

Access emergency-specific records (Urgent care notes).

- Nurse: View patient medical records, Modify records only for patients under their care.
- Hospital Staff: No direct permissions (organizational role for grouping).
- General Doctor: View patient medical records, Modify all patient records in the facility.
- Administrative Staff: View demographic data (name, address, insurance).
- Pharmacist: View patient medical records, Modify prescription details.
- Billing Staff: View demographic data, View billing data.

Question:

1. Draw an RBAC Hierarchy Diagram (note: R1 → R2: R2 has also the rights of R1).
2. Can the following roles do the corresponding permission?

a) ER Doctor wants to modify a patient clinical note. b) Nurse tries to view insurance information. c) New Nurse tries to modify old patients records. d) Pharmacist attempts to view a patient’s address.	e) Billing Staff needs to access insurance ID. f) General Doctor tries to access ER-only trauma logs. g) Receptionist tries to consult a patient address. h) Receptionist schedules an appointment for a patient.

3. Provide one example of Static Separation of Duty and one example of Dynamic Separation of Duty.

Exercise 3: (05 pts)

Give key differences for each pair of concepts.

1) Behavior based IDS VS Signature based IDS.
2) Host-based IDS VS Network-based IDS.
3) Internal threat VS Hacker.
4) False positive VS false negative.

Exercise 4: (04 pts)

A company uses a firewall as a NAT with the internal IP range 192.168.0.0/24. It hosts 3 public-facing servers: HTTP, FTP, and SMTP with Ips:192.168.0.10:80, 192.168.0.20:25, and 192.168.0.30:21 consecutively. The public IP is 203.0.113.5. The company uses a screened subnet (DMZ) to isolate the servers. The Internal Protected Network uses the range 192.168.1.0/24.

1. Design the Network Architecture and label its components with their IP addresses and ports.
2. Write NAT rules to allow external access to public-facing servers using **port forwarding (external IP:port → Internal IP:port)**.

System security final Exam correction

Exercise 1: (4.5 pts)

1- **In Discretionary Access Control Policy, a user X has “rw” permission to File1 and File2 however user Y has no permission to File1.Explain how Y could steal File1’s data using a Trojan horse.**

Y gives X a program that: Creates File3, grants Y: read and X: write. Copies File1 to File3.

2- **In Multi-Level Security, how many labels can be constructed from N security levels and M categories? Explain?**

Total labels = $N \times 2^M$. Each label must include 1 security level (from *N* options).Categories are subsets of the *M* categories. The number of subsets for *M* elements is 2^M (including the empty set).

3- **In Chinese Wall policy, Justify the second condition of writing.**

The Chinese Wall policy’s second condition states: A subject can write to an object only if the subject cannot read any object in a different conflict-of-interest (COI) class. This condition prevents information leakage across competing entities. If a subject writes to an object after accessing data from a conflicting COI class, it risks transferring sensitive information

Exercise 2: (06 pts)

In a hospital, various **roles** are defined to manage it. Each role has specific permissions associated with it, governing what actions they can perform.

- Hospital Staff: No direct permissions (organizational role for grouping).
- Medical Staff: View patient medical records (e.g., name, age, medical history).
- General Doctor: View patient medical records, Modify all patient records in the facility.
- Emergency Room Doctor (ER Doctor): View and Modify all patient medical records in the facility,
- Access emergency-specific records (Urgent care notes).

Nurse: View patient medical records, Modify records only for patients under their care.

- Pharmacist: View patient medical records, Modify prescription details.
- Administrative Staff: View demographic data (name, address, insurance).
- Billing Staff: View demographic data, View billing data.
- Receptionist: View demographic data, Schedule appointments.

Question:

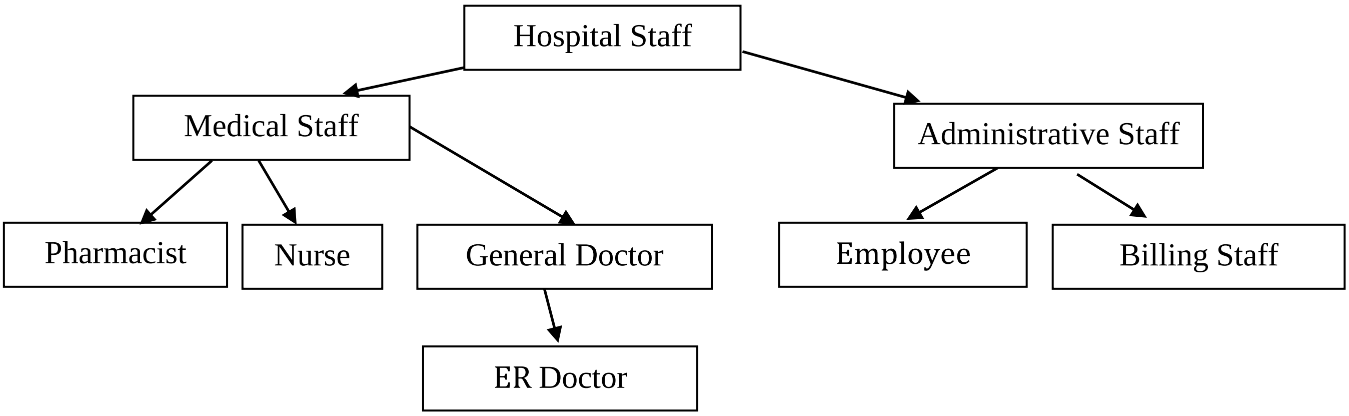
1. Draw an RBAC Hierarchy Diagram (note: R1 → R2: R2 has also the rights of R1).
2. Can the following roles do the corresponding permission?

a) Yes. b) No c) No d) No	e) Yes. f) No g) Yes. h) Yes.

3. **Provide one example of Static Separation of Duty and one example of Dynamic Separation of Duty.**

SSD: A user cannot be assigned both the Doctor and Billing Staff roles.
DSD: A user assigned to both roles can dispense medication (Pharmacist) and process billing (Billing Staff), but cannot process billing for prescriptions they personally dispensed.

1. Draw an RBAC Hierarchy Diagram (note: R1 → R2: R2 has also the rights of R1).



Exercise 3: (05 pts)

Give key differences for each pair of concepts.

1) Behavior-based IDS: Detects anomalies by comparing current activity to a baseline of "normal" behavior. Effective against unknown threats (e.g., zero-day attacks) but prone to false positives.

Signature-based IDS: Matches activity to predefined attack patterns (signatures). Effective against known threats but fails to detect new/unknown attacks.

2) Host-based IDS (HIDS): Monitors activity on a single device (e.g., logs, file changes). Focuses on internal threats and user actions.

Network-based IDS (NIDS): Analyzes network traffic for suspicious patterns. Detects external threats (e.g., intrusions, DDoS) across the network.

3) Internal Threat: Originates from within the organization (e.g., employees, contractors). Exploits legitimate access for malicious purposes (e.g., data theft, sabotage).

Hacker: External actor attempting unauthorized access. Relies on vulnerabilities or social engineering to breach defenses.

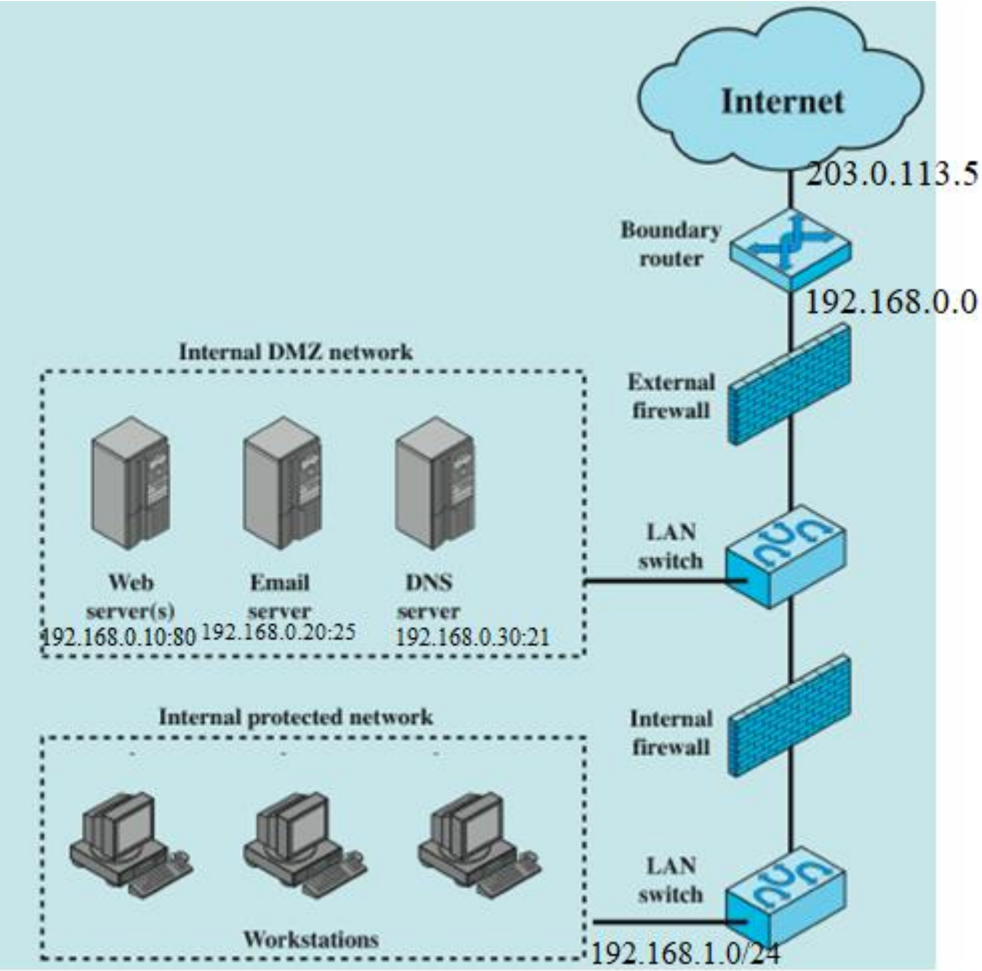
4) False Positive: Alert triggered by benign activity (no real threat). Wastes resources and reduces trust in the system.

False Negative: Failure to detect an actual threat. Leaves the system vulnerable to undetected attacks.

Exercise 4: (04 pts)

A company uses NAT with the internal IP range 192.168.0.0/24. They host a web server (192.168.0.10:80), email server (192.168.0.20:25), and FTP server (192.168.0.30:21). The public IP is 203.0.113.5. The company uses a screened subnet (DMZ) to isolate public-facing servers. Internal Protected Network 192.168.1.0/24.

1. Design the Network Architecture and label its components with their IP addresses and ports.



2. Write NAT rules to allow external access to public-facing servers using **port forwarding (external IP:port → Internal IP:port)**.

- Web Server: Forward 203.0.113.5:80 → 192.168.0.10:80
- Email Server: Forward 203.0.113.5:25 → 192.168.0.20:25
- FTP Server: Forward 203.0.113.5:21 → 192.168.0.30:21