**Scenario:**

Lubana General Hospital, a mid-sized private healthcare provider, recently experienced a suspected data breach. Staff noticed unusual activity on the internal network, including unauthorized access to patient records, and system slowdown during off-hours. Initial investigation suggests a possible phishing attack followed by lateral movement within the network.

The hospital’s cybersecurity team must now investigate the breach, determine the scope of damage, identify how the attacker got in, and take steps to prevent future incidents. They also face pressure from media and regulators due to sensitive health data being potentially leaked.

**Task:**

As a cybersecurity consultant, you are hired to assist Lubana General Hospital. Prepare a written report covering the following:

* + Analyze how ethical hackers could have identified the vulnerabilities before the attack.
  + Describe how penetration testing or vulnerability scanning could have prevented the breach.
  + Describe how a forensic team should approach the investigation.
  + What types of evidence should be collected (e.g., log files, memory dumps, user access history)?
  + Outline a chain of custody process and explain its importance in case of legal action.

**Expected Deliverables:**

* A structured report (1500–2000 words)
* Diagrams or charts (optional)