1. What kind of attack has happened and why do you think so?

Type of Attack:

- **Phishing Attack combined with Credential Harvesting and Potential Malware Infection (Ransomware or Trojan)**

Reasoning:

- The **email impersonating HR** is a classic **phishing technique** used to trick users into clicking a malicious link.
- The **fake portal collecting credentials** indicates a **credential harvesting** attempt.
- The **server error page** following login is a common tactic used to make users believe it was just a technical issue, hiding the fact that credentials were stolen.
- Later reports of **file-share access issues and Word documents not opening** could indicate the presence of **malware**, possibly **ransomware** or another form of **payload** designed to disable access or encrypt files after being downloaded from the phishing site.

---

2. As a cyber security analyst, what are the next steps to take?

Immediate Actions:

- **Contain the attack**:
    - Isolate affected machines from the network to stop the spread of malware.
    - Disable accounts that entered credentials into the fake portal until passwords are reset.
- **Notify stakeholders**:
    - Inform IT management, incident response team, HR, and legal/compliance teams.
- **Begin incident documentation**:

    - Record timelines, user reports, affected systems, and actions taken.

Analysis & Investigation:

- **Identify the scope**:
    - Determine how many users clicked the link, entered credentials, and/or downloaded the malicious file.
- **Check logs**:
    - Email gateway logs, firewall logs, and endpoint logs to trace the attack vector.
- **Scan systems**:
    - Run antivirus and EDR scans on affected endpoints.

---

3. How would you contain, resolve, and recover from this incident?

Containment:

- Disconnect infected devices from the network.
- Block the phishing domain and related IP addresses at the firewall and email gateway.
- Revoke any session tokens or credentials suspected to be compromised.
- Change passwords for affected accounts and enforce multifactor authentication (MFA).

Eradication:

- Remove malware from infected machines using updated antivirus/EDR tools.
- Delete the malicious email from all user inboxes via email quarantine or admin console.

Recovery:

- Restore access to systems after full scans confirm they are clean.

- If files were encrypted, restore them from backups (if ransomware is confirmed).
- Monitor for any further signs of compromise.
- Reset and secure user credentials.
- Patch any vulnerabilities exploited during the attack.

---

4. What activities should be performed post-incident?

Post-Incident Activities:

- **Conduct a Post-Incident Review (PIR):**
    - What happened, why it happened, how it was detected, and how it was resolved.
- **Update incident response playbooks** based on lessons learned.
- **Provide user awareness training** to prevent future phishing success.
- **Review and enhance security controls**:
    - Improve email filtering, implement stricter authentication, and increase endpoint protections.
- **Report to regulatory bodies** if required (e.g., GDPR or financial sector regulators).
- **Monitor systems closely** for signs of persistent threats or reinfection.