Incident Response Report

Week 3 - Technical Analysis (Containment, Eradication, and Recovery)

1. Root Cause Analysis

Attack Type: Phishing Email Attack (Social Engineering via Link)

Attack Description: The phishing email impersonated IT Support, requesting the user to click a link to reset and verify the account. The email contained a hidden tracking image and a malicious URL.

- **Delivery Method:** Emails generated from Kali machine via MailHog simulation environment.
- **Sender:** training@lab.local (spoofed as 123hhkhaled@gmail.com)
- **Email Content:** HTML email with Reset Password button and hidden tracking image.
- **Vulnerabilities Exploited:**
    - Lack of user awareness on phishing attacks.
    - Insufficient email filtering allowed malicious emails to reach inbox.
    - Links in email not blocked by network security tools.
    - Absence of proper DMARC/SPF/DKIM validation for email authenticity.
- **Indicators of Compromise (IoC):**
    - X-Mailer: gophish
    - Message ID: P1CfMUPkFhehkFxm5n5Y6eYXcdoWfuThbbPCcKyfgI8=@mailhog.example
    - Malicious link: http://192.168.159.130?rid=JZKrRyr
    - Hidden tracking image: http://192.168.159.130/track?rid=JZKrRyr

2. Containment & Recovery

Containment Steps:

- Move malicious emails to a quarantined folder for investigation.
- Lock emails to prevent further user interaction.
- Block sender domain/IP to prevent additional emails.
- Block malicious URLs in network proxy and security filters.

- Notify employees not to click the links and preserve evidence.

Recovery Steps:

- Delete the malicious emails from all affected mailboxes after preserving evidence.
- Scan all devices with antivirus/endpoint protection (Windows Defender / ClamAV).
- Check for suspicious processes, scheduled tasks, and system modifications.
- Isolate affected systems and restore from clean backups if necessary.
- Verify all restored systems are clean and operational.
- Update email filters and URL blocklists to prevent recurrence.

Post-Recovery Recommendations:

- Enhance email filtering and block suspicious URLs automatically.
- Regular phishing awareness training for employees.
- Implement DMARC, SPF, DKIM for email authentication.
- Use sandboxing for automatic analysis of links and attachments.
- Test backup and restoration procedures regularly.

3. Evidence Inventory

Evidence Type	Description
Mailhog SMTP Logs	Full SMTP session logs capturing email delivery and protocol states.
Phishing Email .EML	Original email messages including headers and body for analysis.
Email Headers	All message headers showing sender, recipient, message IDs, and X-Mailer.
Email Body (HTML)	HTML content of phishing emails, including links and hidden tracking images.
Suspicious URLs	List of all URLs used in the phishing emails.
Mailhog API Export	Exported data from MailHog API containing message metadata.
Screenshots	Screenshots of MailHog interface showing delivered emails.
Evidence Hashes	SHA256 hashes of all evidence files to ensure integrity.

Device Scan Results	Results from antivirus/endpoint scans of all affected devices.
Timeline	Chronological log of email delivery, detection, containment, and recovery steps.