**Cybersecurity Incident Response Report**

**Task 3:** Simulated Cyber Incident Response  
**Tools Used:** Splunk, Kibana, Wireshark

**1. Incident Overview**

* Incident Type: Unauthorized Access & Data Breach
* Date & Time of Detection: Tuesday, February 4, 2025, at 4:04 PM
* Affected Systems:
  + Corporate authentication server
  + Database storage
  + Internal network
* Impact Level: High (compromised user credentials, unauthorized data access, and potential regulatory implications)
* Detection Tools:
  + Splunk – SIEM logs analysis
  + Kibana – Log visualization
  + Wireshark – Packet capture and network traffic analysis

**2. Forensic Analysis & Log Investigation**

**2.1 Splunk SIEM Logs Findings**

* Detected multiple failed login attempts, followed by a successful login from an unrecognized IP address.
* Unusual login activity outside normal geographic patterns.
* Privilege escalation observed shortly after unauthorized access.

**2.2 Kibana Log Visualization**

* Log patterns revealed signatures of a brute-force attack.
* Firewall logs correlated external IP connection attempts with suspicious activity.

**2.3 Wireshark Packet Capture Analysis**

* Identified unusual network traffic attempting to communicate with external servers.
* Detected encrypted data exfiltration over TCP Port 4444, a common vector for remote shell attacks.

**2.4 Root Cause Analysis**

* Weak Passwords: Lack of Multi-Factor Authentication (MFA) enabled credential stuffing attacks.
* Unpatched Vulnerability: The authentication service was missing critical security patches.
* Phishing Attack: Employee credentials were compromised through a targeted phishing email.

**3. Incident Mitigation Steps Taken**

**3.1 Containment Measures**

* Immediately locked out affected user accounts.
* Blocked malicious IP addresses at the firewall level.
* Issued a company-wide security alert to inform employees about phishing risks.

**3.2 Remediation Actions**

* Enforced password resets for all users.
* Applied necessary security patches to the authentication servers.
* Enabled Multi-Factor Authentication (MFA) for all logins.

**3.3 User Awareness & Training**

* Conducted phishing awareness training for employees.
* Implemented email security measures such as SPF, DKIM, and DMARC to mitigate phishing risks.

**4. Recommendations for Preventing Future Incidents**

* Strengthen Authentication Security: Implement passwordless authentication alongside mandatory MFA.
* Continuous Monitoring: Utilize Splunk and Kibana for real-time anomaly detection.
* Regular Penetration Testing: Conduct quarterly security assessments.
* Phishing Simulations: Implement ongoing phishing awareness programs to educate employees.

**5. Conclusion**

This simulated cybersecurity incident highlights the critical role of proactive security measures, real-time monitoring, and rapid response. By enforcing multi-layered security controls, continuous log analysis, and user awareness training, organizations can significantly enhance their resilience against cyber threats and minimize risks.