

Ghaymah Systems

Attack Simulation (Red/Blue Team) - Incident Response Report

1. Timeline Analysis

Based on the scenario, the attack kill chain occurred as follows:

- **Reconnaissance:** The attacker identifies the API endpoint (e.g., ghaymah.systems/api/login) and gathers Open-Source Intelligence (OSINT) or uses a phishing attack targeting an employee to steal initial credentials.
- **Attack (Credential Stuffing/Brute Force):** Using automated tools to try thousands of passwords or previously breached credentials against the API.
- **Initial Access:** A successful login attempt occurs, and an access token (JWT or API Token) is issued to the attacker.
- **Data Exfiltration:** Using the authorized token to call other API endpoints (e.g., /api/users) and extract sensitive database information.

2. Incident Response Plan

Based on the NIST SP 800-61 Incident Handling Guide, the following immediate steps must be taken:

- **Immediate Containment:** Block the attacker's IP address via the WAF. Revoke all active API tokens for the compromised user account and force an immediate password reset.
- **Eradication:** Review system logs to ensure the attacker did not create rogue administrative accounts or plant backdoors.
- **Recovery:** Restore services to normal operations after applying additional security controls. Maintain heightened, intensive monitoring for the next 48 hours.

3. Prevention & Infrastructure Hardening

To secure the Ghaymah infrastructure, the following CISA and NIST standards must be applied:

- **Network Policies:** Enforce strict Rate Limiting at the API Gateway (e.g., a maximum of 5 attempts per IP per 15 minutes). Deploy a WAF equipped with OWASP Core Rule Sets to block automated malicious behavior.

- **Container Security & Micro-segmentation:** Apply the Zero Trust model and Principle of Least Privilege. Isolate the API container from the database container so direct communication is impossible except through highly restricted, internally authenticated channels.
- **Security Awareness Training:** Implement behavior-changing awareness programs compliant with NIST SP 800-50. Train employees to recognize and report phishing attacks to mitigate the initial credential theft risk.

4. SIEM Early Warning Alert Rule

Design an alert rule logic for the SIEM system (e.g., Splunk or ELK) to catch this early:

Condition: Detect more than 5 failed login attempts (HTTP 401 Unauthorized).

Source: From the same IP address OR targeting the same username.

Timeframe: Within a 1-minute window.

Action: Trigger a High-Severity alert to the SOC team and execute an automated temporary block on the offending IP address.