**Incident Response Report**

**Company Name :** TechNova Solutions

**Incident ID :** IR-2024-017

**Date :** October 15, 2024

**Report Prepared By :** Chanukya Keerthi, Cybersecurity Analyst Intern

**Tools Used :** Splunk, Kibana, Wireshark

**1. Executive Summary**

**Incident Overview :**

On October 14, 2024, TechNova Solutions experienced a \*\*multi-vector cyberattack” involving a “DDoS attack” targeting its public-facing web servers and \*\*unauthorized access attempts\*\* to its customer database. The incident disrupted services for 2 hours and exposed vulnerabilities in network defenses.

**Key Findings :**

-**DDoS Attack :** Traffic spike from 15,000+ IPs (primarily **`185.220.101.0/24`, `45.129.56.0/24**`).

-**Unauthorized Database Access :** Brute-force login attempts from IP **`103.10.24.55` (Vietnam)** and SQL injection attempts from **`192.168.5.203` (internal IP).**

-**Impact :** Service downtime (**2 hours**), partial database exposure (**50 customer records**).

**2. Methodology**

**2.1 Tools & Techniques**

**1. Splunk :**

- Analyzed firewall logs for traffic spikes and brute-force attempts.

- Queried `failed\_login\_attempts` and `sql\_errors` in database logs.

**2. Kibana :**

- Visualized traffic patterns during the DDoS attack.

- Created dashboards for geolocation mapping of malicious IPs.

**3. Wireshark :**

- Captured network packets during the DDoS attack to identify SYN flood patterns.

- Traced SQL injection payloads targeting the database server.

**3. Incident Timeline**

**|**   **Timestamp (UTC) | Event |**

**|-----------------------------------|---------------------------------------------------------------------------------------------|**

**|** 2024-10-14 08:15 AM  **|** DDoS attack begins (SYN flood from `185.220.101.34`,`45.129.56.72`).**|**

**|** 2024-10-14 08:30 AM **|** Web servers (`192.168.1.10`, `192.168.1.11`) overwhelmed; 90%

packet loss**. |**

**|** 2024-10-14 09:00 AM  **|** Unauthorized login attempts detected on database server (`10.0.2.5`).**|**

**|** 2024-10-14 09:15 AM  **|** SQL injection payloads observed from internal IP `192.168.5.203`. **|**

**|** 2024-10-14 10:00 AM **|** Incident contained; services restored**. |**

**4. Root Cause Analysis**

**4.1 DDoS Attack**

**- \*\*Source\*\*:** Botnet IPs (`185.220.101.0/24`, `45.129.56.0/24`) generating SYN flood traffic.

**- \*\*Triggers\*\*:**

- Lack of rate-limiting on web servers.

- Absence of a Web Application Firewall (WAF).

**4.2 Unauthorized Database Access**

**Brute-Force Attempts :** 1,200+ login tries from `103.10.24.55` targeting `admin@technova.com`.

**SQL Injection :** Payload `' OR 1=1;--` from `192.168.5.203` (compromised internal workstation).

**Triggers :**

- Weak password policy (no MFA).

- Unpatched SQL database (CVE-2024-1234).

**5. Impact Assessment**

**| Category | Details |**

**|----------------------------|-----------------------------------------------------------------------------------------|**

**|**  Financial **|** $25,000 revenue loss due to downtime**. |**

**|** Reputational **|** Customer trust impacted (50 records exposed). **|**

**|**  Operational **|** 2 hours of service disruption**. |**

---

**6. Mitigation Steps**

**6.1 Immediate Actions**

**1. DDoS Mitigation:**

- Deployed AWS Shield to filter malicious traffic.

- Blocked IP ranges `185.220.101.0/24` and `45.129.56.0/24` at the firewall.

**2. Database Security :**

- Reset all user passwords and enforced MFA.

- Patched SQL database (CVE-2024-1234).

**6.2 Long-Term Fixes**

- Configured WAF (Cloudflare) to block SQLi and brute-force attempts.

- Segmented internal network to isolate database servers.

**7. Recommendations**

**1. Prevent DDoS :**

- Implement traffic scrubbing via a DDoS protection service (e.g., Cloudflare, Akamai).

- Enable SYN cookies on web servers.

**2. Secure Database :**

- Conduct quarterly penetration testing.

- Encrypt sensitive customer data at rest.

**3. Monitoring :**

- Create Splunk alerts for:

- >500 requests/sec from a single IP.

- Failed login attempts exceeding 10/minute.

- Use Kibana to visualize real-time traffic geolocation.

**8. Lessons Learned**

**Proactive Monitoring :** Early detection of traffic spikes could have reduced downtime.

**Internal Threats :** The SQL injection originated from an internal IP, highlighting insider risks.

**Password Policies :** MFA would have prevented brute-force success.

**Appendix**

**A. Indicators of Compromise (IoCs)**

**Malicious IPs :**

- DDoS: `185.220.101.34`, `45.129.56.72`, `185.220.101.89`.

- Brute-Force: `103.10.24.55`.

**SQL Injection Payload :** `' OR 1=1;--`.

**B. Tools Used**

**| Tool | Purpose |**

**|----------------|---------------------------------------------------------------------|**

**|** Splunk **|** Log analysis for failed logins and SQL errors. **|**

**|** Kibana **|** Geolocation mapping of attack sources. **|**

**|** Wireshark **|** Packet capture to identify SYN flood patterns. **|**

**Report End**

**\*Confidential – For Internal Use Only\***

---