Investigation Report: MiddleMayhem — Blue Team Labs Online

Objective: Analyze the attack chain, identify exploitation indicators, and trace lateral movement activities.

Scenario

The security team at MiddleMayhem Inc. has detected unusual network traffic to their admin portal, but no security breaches have been confirmed. Your SOC team has been provided with SIEM logs from the incident. Analyze the attack pattern to determine how attackers bypassed authentication, gained remote code execution, and moved laterally through the network.

1. Summary

During the analysis of the *MiddleMayhem* investigation hosted on Blue Team Labs Online, an external attacker successfully exploited a web application via a known vulnerability (CVE-2025-29927), uploaded a reverse shell script, and attempted lateral movement within the internal network. Through thorough inspection of SIEM logs using Splunk Search Engine, we identified the exploited vector, post-exploitation behavior, and the final user account compromised during lateral movement.

2. Attack Timeline and Technical Findings

Initial Reconnaissance

- **Attacker IP:** 218.92.0.204
- The attacker scanned the web application hosted at 172.217.164.174:8080 using a large number of HTTP requests (totaling **9930 unique URIs**), including HEAD, GET, and POST methods.
- This behavior suggests automated enumeration likely driven by a scanning tool or vulnerability scanner.

Exploitation (CVE-2025-29927)

- The attacker exploited a vulnerability in the application via a crafted HTTP header:
  Header used: X-Middleware-Subrequest

- The malicious payload was delivered via a POST request to /api/upload.
- This exploit led to the successful upload of a shell script (shell.sh), which attempted to establish a reverse shell connection.

Reverse Shell Callback

- **Reverse shell target:** 113.89.232.157:31337
- The callback originated from the web server (172.217.164.174) towards the attacker's listener.
- Two connection attempts were recorded, the second of which indicated a successful session establishment.

Discovery and Lateral Movement

- Following post-exploitation activity, SSH brute-force attempts were launched from the web server.
- **Targeted internal host:** 192.168.1.8
- Repeated TCP connection attempts were logged on **port 22 (SSH)**.
- This activity was later confirmed as **SSH brute force**, which succeeded in establishing lateral access.

Successful Compromise

- Logs from sshd on 192.168.1.8 revealed that the attacker gained access using the following account:
  Username: dbserv
- This is confirmed by the authentication message:
  "session opened for user dbserv(uid=100)"
  indicating a successful login following the brute-force attack.

3. Answers to Investigation Prompts

Question	Answer
Access the Website in the browser, present it in the bookmark, and identify the JavaScript framework and version used.	Next.js, 15.0.0
Using Splunk, Find the attacker's IP address	218.92.0.204

Question	**Answer**
Analyze the SIEM logs to determine how many unique URIs were accessed by the attacker.	9930
Explore the site and identify two specific locations that could reveal internal structures or potential access points not meant for public eyes. Provide the two relative URLs.	/admin, /admin/file-upload
Based on the Framework and Version, what recent CVE could be used to bypass authorization?	CVE-2025-29927
Find the relevant HTTP header in the SIEM logs that indicates CVE exploitation. Provide the header name.	X-Middleware-Subrequest
What interesting URI did the attacker access after exploiting the CVE?	/api/upload
The attacker tried uploading a reverse shell. Find out the IP and port to which the target would connect once the connection is established.	113.89.232.157:31337
After compromising the WebApp server, the attacker attempted lateral movement. Identify the technique used, as recorded in the SIEM logs.	SSH brute force
Identify the user account that achieved successful lateral movement to another server.	dbserv

4. Conclusion

The *MiddleMayhem* attack demonstrates a complete exploitation chain: from external reconnaissance and vulnerability exploitation to reverse shell deployment and lateral movement. The attacker successfully found a vulnerability knowing the framework and version of the website, leveraged a vulnerable HTTP header to upload a shell script, obtained remote execution, and used brute-force techniques to pivot deeper into the internal network. Timely detection of the X-Middleware-Subrequest header and brute-force SSH behavior would have been critical in preventing further compromise.