Digital Forensic Incident Report

Case ID: b82d83eb

Generated: 2026-01-24 12:56:11 UTC

1. Executive Summary

During a six-second window around 12:55:21 UTC on 2026-01-24, multiple security-related events were observed from several IP addresses. The events comprise protocol abuse signals, web application firewall (WAF) correlation signals, a SQL injection event, and repeated access-denied responses. No indication of successful access, compromise, or data exfiltration is present in this batch. Per-IP event summary: - 79.124.40.174 - PROTOCOL_ABUSE: 2 events (12:55:21.718420 and 12:55:21.720419) - 198.244.240.150 - WAF_CORRELATION: 2 events (12:55:21.719417 x2) - SQL_INJECTION: 1 event (12:55:21.719417) - 92.205.212.128 - ACCESS_DENIED: 2 events (12:55:21.720419 and 12:55:21.723419) - 216.244.66.199 - WAF_CORRELATION: 2 events (12:55:21.721419 x2) - PROTOCOL_ABUSE: 1 event (12:55:21.722418) - 208.167.225.162 - ACCESS_DENIED: 5 events (12:55:21.723419 x2, 12:55:21.724417 x3) Overall observations: - Multiple IPs generated PROTOCOL_ABUSE and WAF_CORRELATION signals within the same second, indicating concurrent signals across different sources. - A SQL_INJECTION event was detected from a single IP (198.244.240.150). - ACCESS_DENIED events occurred repeatedly from three IPs (92.205.212.128 and 208.167.225.162), with 208.167.225.162 contributing the majority of the denial events (five total). - There is no explicit statement of successful access, compromise, or data exfiltration in this batch; the data indicate detection and blocking of potential threats, with one SQL injection finding. No attribution or compromise is inferred from the provided data. If you would like, I can provide a per-event timeline or exportable counts for further analysis.

2. Chronological Event Timeline

Timestamp (UTC)	Observed Event
2026-01-24 12:55:21.718420+00:00	PROTOCOL_ABUSE detected from 79.124.40.174
2026-01-24 12:55:21.719417+00:00	WAF_CORRELATION detected from 198.244.240.150
2026-01-24 12:55:21.719417+00:00	WAF_CORRELATION detected from 198.244.240.150
2026-01-24 12:55:21.719417+00:00	SQL_INJECTION detected from 198.244.240.150
2026-01-24 12:55:21.720419+00:00	PROTOCOL_ABUSE detected from 79.124.40.174
2026-01-24 12:55:21.720419+00:00	ACCESS_DENIED detected from 92.205.212.128
2026-01-24 12:55:21.721419+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-24 12:55:21.721419+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-24 12:55:21.722418+00:00	PROTOCOL_ABUSE detected from 216.244.66.199
2026-01-24 12:55:21.723419+00:00	ACCESS_DENIED detected from 92.205.212.128
2026-01-24 12:55:21.723419+00:00	ACCESS_DENIED detected from 92.205.212.128
2026-01-24 12:55:21.723419+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-24 12:55:21.723419+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-24 12:55:21.724417+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-24 12:55:21.724417+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-24 12:55:21.724417+00:00	ACCESS_DENIED detected from 208.167.225.162

3. MITRE ATT&CK; Technique Mapping

Artifact ID	Technique ID	Technique Description
b82d83eb	T1048	Exfiltration Over Alternative Protocol
335a44a4	T1046	Network Service Discovery
166a1da2	T1046	Network Service Discovery
7f2947d7	T1190	Exploit Public-Facing Application
e376b631	T1048	Exfiltration Over Alternative Protocol
fb5810d8	T1110	Brute Force / Credential Access
378389ab	T1046	Network Service Discovery
34d5d5cc	T1046	Network Service Discovery
ff617509	T1048	Exfiltration Over Alternative Protocol
9db53e14	T1110	Brute Force / Credential Access
99177613	T1110	Brute Force / Credential Access
07d679bd	T1110	Brute Force / Credential Access
c72b59f2	T1110	Brute Force / Credential Access
89e66a1e	T1110	Brute Force / Credential Access
db36c58a	T1110	Brute Force / Credential Access
3e299f69	T1110	Brute Force / Credential Access

4. Source IP Concentration Analysis

Source IP	Event Count
208.167.225.162	5
198.244.240.150	3
92.205.212.128	3
216.244.66.199	3
79.124.40.174	2

5. Case Intelligence Summary

Attack Channel	Observed
Web	Yes
Authentication	No
Network	No
Endpoint	No
Cloud	No