Digital Forensic Incident Report

Case ID: 4403b7fe

Generated: 2026-01-30 17:57:33 UTC

1. Executive Summary

Integrated incident narrative (consolidating Batches 1–4) Executive overview Across a very short window on 2026-01-30 around 17:53:44 UTC, multiple external IPs generated access attempts that were denied, with numerous WAF detections and protocol-related alerts. The detections include SQL injection, Local File Inclusion (LFI), and protocol abuse, observed from several sources. In all provided records, there is no confirmation of successful access or data exfiltration. A burst of ACCESS_DENIED events was observed from at least one IP within a tightly scoped timeframe, and a small number of network communications were noted without accompanying payload detail. Consolidated timeline of detections and denials (UTC 2026-01-30) - 17:53:44.930565+00:00 - ACCESS_DENIED: 178.16.55.142 (appears twice) - WAF_CORRELATION: 198.244.240.20 (appears twice) - 17:53:44.933079+00:00 - WAF_CORRELATION: 198.244.240.20 (appears twice) - SQL_INJECTION: 198.244.240.20 - Network communication observed - PROTOCOL_ABUSE: 204.76.203.212 - WAF_CORRELATION: 45.195.7.235 (appears twice) - PROTOCOL_ABUSE: 45.195.7.235 - Network communication observed - ACCESS_DENIED: 109.234.161.199 - ACCESS_DENIED: 77.55.253.213 - ACCESS_DENIED: 103.191.208.118 - ACCESS_DENIED: 198.54.126.38 - ACCESS_DENIED: 212.154.119.3 - ACCESS_DENIED: 185.73.130.137 - ACCESS_DENIED: 212.154.119.3 (duplicate) - ACCESS_DENIED: 162.55.240.80 - ACCESS_DENIED: 143.95.111.157 - ACCESS_DENIED: 178.128.239.177 - ACCESS_DENIED: 103.2.225.70 - 17:53:44.940593+00:00 - LFI (Local File Inclusion): 164.92.103.174 (appears three times) - 17:53:44.944144 / 17:53:44.950649 (Batch 2 timeframe) - LFI: 164.92.103.174 (twice in this batch) - PROTOCOL_ABUSE: multiple sources (eight total across various IPs) - WAF_CORRELATION: multiple sources (notably 164.92.103.174 and 216.244.66.199) - ACCESS_DENIED: multiple instances from various IPs - 17:53:44.960255 / 17:53:44.970331 (Batch 4 timeframe) - SOURCE: 195.178.110.108 - ACCESS_DENIED: 25 occurrences across three timestamps - Context: 5 at 17:53:44.960255, 14 at 17:53:44.965267, 6 at 17:53:44.970331 - Observed pattern: bursts of denied attempts from a single external IP within about 10 milliseconds per timestamp group - 17:53:44.933079–17:53:44.960255 (Additional cross-batch notes) - 216.244.66.199: WAF_CORRELATION (multiple), PROTOCOL_ABUSE (multiple), and at least one ACCESS_DENIED (from Batch 2/3 observations) - 79.124.40.174: WAF_CORRELATION (two detections), RCE (three detections), PROTOCOL_ABUSE (one) - 204.76.203.212: PROTOCOL_ABUSE (one) - 43.166.1.243: PROTOCOL_ABUSE (two) - Other ACCESS_DENIED sources include 167.99.116.143, 185.73.130.137, 43.155.73.192, 217.216.36.182, 103.143.231.246, 39.109.116.19 Observations and pattern notes (conservative) - A cluster of access-denied events occurred from multiple external IPs within a single

second, consistent with automated or broad-scope probing activity. - WAF ALERTS/DETECTS are present from multiple sources, including: - 198.244.240.20: WAF_CORRELATION and SQL_INJECTION - 45.195.7.235: WAF_CORRELATION and PROTOCOL_ABUSE - 164.92.103.174: LFI and WAF_CORRELATION (across multiple entries) - 216.244.66.199: WAF_CORRELATION and PROTOCOL_ABUSE (and at least one ACCESS_DENIED) - 79.124.40.174: WAF_CORRELATION and RCE detections - 204.76.203.212: PROTOCOL_ABUSE - 43.166.1.243: PROTOCOL_ABUSE - A single IP (164.92.103.174) shows multiple LFI detections and multiple WAF_CORRELATION events within the same short window. - A notable burst of ACCESS_DENIED activity is observed from 195.178.110.108 in a tightly spaced sequence, suggesting a high-rate denial event with no accompanying success indicators in these records. - Across batches, there are mentions of two separate network-communication observations, but payload details and endpoints are not provided. Assessment (conservative and non-speculative) - The records reflect detections and access-denied events, with multiple WAF and protocol-abuse alerts, and several LFI detections. There is no documented evidence within these records of a successful breach or data exfiltration. - No attribution or actor inference is made; the narrative is limited to the observed event types, sources, and timing. Recommended follow-up (brief, non-presumptive) - Correlate these detections with authentication logs, firewall/WAF rule logs, and related server/application logs to identify any subsequent activity beyond these detections. - Check the entering IPs against threat-intelligence lists and verify whether any addresses are known to be associated with legitimate traffic. - Inspect the 164.92.103.174 activity for LFI patterns and confirm there were no successful exploit attempts. - Validate that WAF rules for SQLi, LFI, and protocol abuse are current and tuned to balance security with legitimate traffic. - Review the high-volume ACCESS_DENIED activity from 195.178.110.108 in the surrounding time window with authentication and firewall logs to determine targeted resources and any rate-limiting or anomaly-detection triggers. If you would like, I can present this as a compact incident-brief with a per-IP timeline or consolidate it into a succinct executive summary for reporting.

2. Chronological Event Timeline

Timestamp (UTC)	Observed Event
2026-01-30 17:53:44.930565+00:00	ACCESS_DENIED detected from 178.16.55.142
2026-01-30 17:53:44.930565+00:00	ACCESS_DENIED detected from 178.16.55.142
2026-01-30 17:53:44.930565+00:00	WAF_CORRELATION detected from 198.244.240.20
2026-01-30 17:53:44.933079+00:00	WAF_CORRELATION detected from 198.244.240.20
2026-01-30 17:53:44.933079+00:00	SQL_INJECTION detected from 198.244.240.20
2026-01-30 17:53:44.933079+00:00	Network communication observed
2026-01-30 17:53:44.933079+00:00	PROTOCOL_ABUSE detected from 204.76.203.212
2026-01-30 17:53:44.933079+00:00	WAF_CORRELATION detected from 45.195.7.235
2026-01-30 17:53:44.933079+00:00	WAF_CORRELATION detected from 45.195.7.235
2026-01-30 17:53:44.933079+00:00	PROTOCOL_ABUSE detected from 45.195.7.235
2026-01-30 17:53:44.933079+00:00	Network communication observed
2026-01-30 17:53:44.933079+00:00	ACCESS_DENIED detected from 109.234.161.199
2026-01-30 17:53:44.933079+00:00	ACCESS_DENIED detected from 77.55.253.213
2026-01-30 17:53:44.933079+00:00	ACCESS_DENIED detected from 103.191.208.118
2026-01-30 17:53:44.933079+00:00	ACCESS_DENIED detected from 198.54.126.38
2026-01-30 17:53:44.933079+00:00	ACCESS_DENIED detected from 212.154.119.3
2026-01-30 17:53:44.933079+00:00	ACCESS_DENIED detected from 185.73.130.137
2026-01-30 17:53:44.933079+00:00	ACCESS_DENIED detected from 212.154.119.3
2026-01-30 17:53:44.933079+00:00	ACCESS_DENIED detected from 162.55.240.80
2026-01-30 17:53:44.933079+00:00	ACCESS_DENIED detected from 143.95.111.157
2026-01-30 17:53:44.933079+00:00	ACCESS_DENIED detected from 178.128.239.177
2026-01-30 17:53:44.933079+00:00	ACCESS_DENIED detected from 103.2.225.70
2026-01-30 17:53:44.940593+00:00	LFI detected from 164.92.103.174
2026-01-30 17:53:44.940593+00:00	LFI detected from 164.92.103.174
2026-01-30 17:53:44.940593+00:00	LFI detected from 164.92.103.174
2026-01-30 17:53:44.940593+00:00	LFI detected from 164.92.103.174
2026-01-30 17:53:44.940593+00:00	WAF_CORRELATION detected from 164.92.103.174
2026-01-30 17:53:44.940593+00:00	WAF_CORRELATION detected from 164.92.103.174
2026-01-30 17:53:44.940593+00:00	LFI detected from 164.92.103.174
2026-01-30 17:53:44.940593+00:00	PROTOCOL_ABUSE detected from 164.92.103.174
2026-01-30 17:53:44.944144+00:00	PROTOCOL_ABUSE detected from 43.166.1.243
2026-01-30 17:53:44.944144+00:00	PROTOCOL_ABUSE detected from 43.166.1.243
2026-01-30 17:53:44.944144+00:00	ACCESS_DENIED detected from 167.99.116.143
2026-01-30 17:53:44.944144+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-30 17:53:44.944144+00:00	ACCESS_DENIED detected from 185.73.130.137

Timestamp (UTC)	Observed Event
2026-01-30 17:53:44.944144+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-30 17:53:44.944144+00:00	PROTOCOL_ABUSE detected from 216.244.66.199
2026-01-30 17:53:44.944144+00:00	ACCESS_DENIED detected from 43.155.73.192
2026-01-30 17:53:44.944144+00:00	ACCESS_DENIED detected from 217.216.36.182
2026-01-30 17:53:44.944144+00:00	ACCESS_DENIED detected from 103.143.231.246
2026-01-30 17:53:44.944144+00:00	ACCESS_DENIED detected from 39.109.116.19
2026-01-30 17:53:44.944144+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-30 17:53:44.944144+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-30 17:53:44.944144+00:00	PROTOCOL_ABUSE detected from 216.244.66.199
2026-01-30 17:53:44.944144+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-30 17:53:44.950649+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-30 17:53:44.950649+00:00	PROTOCOL_ABUSE detected from 216.244.66.199
2026-01-30 17:53:44.950649+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-30 17:53:44.950649+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-30 17:53:44.950649+00:00	PROTOCOL_ABUSE detected from 216.244.66.199
2026-01-30 17:53:44.950649+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-30 17:53:44.950649+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-30 17:53:44.950649+00:00	PROTOCOL_ABUSE detected from 216.244.66.199
2026-01-30 17:53:44.955198+00:00	PROTOCOL_ABUSE detected from 204.76.203.212
2026-01-30 17:53:44.955198+00:00	Network communication observed
2026-01-30 17:53:44.955198+00:00	Network communication observed
2026-01-30 17:53:44.955198+00:00	Network communication observed
2026-01-30 17:53:44.955198+00:00	Network communication observed
2026-01-30 17:53:44.955198+00:00	WAF_CORRELATION detected from 79.124.40.174
2026-01-30 17:53:44.955198+00:00	WAF_CORRELATION detected from 79.124.40.174
2026-01-30 17:53:44.955198+00:00	RCE detected from 79.124.40.174
2026-01-30 17:53:44.955198+00:00	RCE detected from 79.124.40.174
2026-01-30 17:53:44.955198+00:00	RCE detected from 79.124.40.174
2026-01-30 17:53:44.955198+00:00	PROTOCOL_ABUSE detected from 79.124.40.174
2026-01-30 17:53:44.955198+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.955198+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.960255+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.960255+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.960255+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.960255+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.960255+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.960255+00:00	ACCESS_DENIED detected from 195.178.110.108

Timestamp (UTC)	Observed Event
2026-01-30 17:53:44.960255+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.960255+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.960255+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.960255+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.960255+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.960255+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.960255+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.960255+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.965267+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.965267+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.965267+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.965267+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.965267+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.965267+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.965267+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.965267+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.965267+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.965267+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.965267+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.965267+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.965267+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.965267+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.970331+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.970331+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.970331+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.970331+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.970331+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-30 17:53:44.970331+00:00	ACCESS_DENIED detected from 195.178.110.108

3. MITRE ATT&CK; Technique Mapping

Artifact ID	Technique ID	Technique Description
4403b7fe	T1110	Brute Force / Credential Access
cd7fba0c	T1110	Brute Force / Credential Access
594243ac	T1046	Network Service Discovery
91a95dd5	T1046	Network Service Discovery
51c03cad	T1190	Exploit Public-Facing Application
726550a1	T1048	Exfiltration Over Alternative Protocol
3c968a81	T1046	Network Service Discovery
15d8a4e9	T1046	Network Service Discovery
b6e14f89	T1048	Exfiltration Over Alternative Protocol
9fedd8c1	T1110	Brute Force / Credential Access
6735ebd3	T1110	Brute Force / Credential Access
d857f940	T1110	Brute Force / Credential Access
43627ca8	T1110	Brute Force / Credential Access
b8586fcb	T1110	Brute Force / Credential Access
ac37b037	T1110	Brute Force / Credential Access
651eeafa	T1110	Brute Force / Credential Access
5a98fda7	T1110	Brute Force / Credential Access
d663a71f	T1110	Brute Force / Credential Access
eaeef828	T1110	Brute Force / Credential Access
900dda6c	T1110	Brute Force / Credential Access
9f7cf464	T1005	Data from Local System
0aa26e08	T1005	Data from Local System
caae4a74	T1005	Data from Local System
93c37c92	T1005	Data from Local System
d831c544	T1046	Network Service Discovery
3e2d5e86	T1046	Network Service Discovery
128b67ac	T1005	Data from Local System
260b94d3	T1048	Exfiltration Over Alternative Protocol
08878e17	T1048	Exfiltration Over Alternative Protocol
91891b87	T1048	Exfiltration Over Alternative Protocol
5c39a19e	T1110	Brute Force / Credential Access
939c8ccc	T1046	Network Service Discovery
8963c180	T1110	Brute Force / Credential Access
3b810f92	T1046	Network Service Discovery
550b84f2	T1048	Exfiltration Over Alternative Protocol

Artifact ID	Technique ID	Technique Description
59f980b8	T1110	Brute Force / Credential Access
b7181464	T1110	Brute Force / Credential Access
be3dcc2d	T1110	Brute Force / Credential Access
0b73de3a	T1110	Brute Force / Credential Access
63978af8	T1046	Network Service Discovery
be053f8c	T1046	Network Service Discovery
a339f387	T1048	Exfiltration Over Alternative Protocol
38f05a0b	T1046	Network Service Discovery
574ed70b	T1046	Network Service Discovery
8605af59	T1048	Exfiltration Over Alternative Protocol
bb28088d	T1046	Network Service Discovery
bfc400ef	T1046	Network Service Discovery
479e4ed1	T1048	Exfiltration Over Alternative Protocol
0e01cddb	T1046	Network Service Discovery
ed1a7c29	T1046	Network Service Discovery
25e1e62c	T1048	Exfiltration Over Alternative Protocol
9139a8d8	T1048	Exfiltration Over Alternative Protocol
91308ce6	T1046	Network Service Discovery
2faa7875	T1046	Network Service Discovery
39705625	T1048	Exfiltration Over Alternative Protocol
0de47f4d	T1110	Brute Force / Credential Access
5298fa22	T1110	Brute Force / Credential Access
86fbae9d	T1110	Brute Force / Credential Access
bf75e951	T1110	Brute Force / Credential Access
50948ad1	T1110	Brute Force / Credential Access
1b841ae7	T1110	Brute Force / Credential Access
736024ad	T1110	Brute Force / Credential Access
4e487133	T1110	Brute Force / Credential Access
32e71d9f	T1110	Brute Force / Credential Access
e61b2056	T1110	Brute Force / Credential Access
efb8bf56	T1110	Brute Force / Credential Access
66a082df	T1110	Brute Force / Credential Access
eb00be8c	T1110	Brute Force / Credential Access
1a385849	T1110	Brute Force / Credential Access
f5b4cdaf	T1110	Brute Force / Credential Access
1d379081	T1110	Brute Force / Credential Access
13d86122	T1110	Brute Force / Credential Access

Artifact ID	Technique ID	Technique Description
61567ef2	T1110	Brute Force / Credential Access
c513fed8	T1110	Brute Force / Credential Access
4ad2af63	T1110	Brute Force / Credential Access
90cda96b	T1110	Brute Force / Credential Access
4686e532	T1110	Brute Force / Credential Access
7b175146	T1110	Brute Force / Credential Access
9956a451	T1110	Brute Force / Credential Access
deaaafdf	T1110	Brute Force / Credential Access
199065f9	T1110	Brute Force / Credential Access
6a50cee2	T1110	Brute Force / Credential Access
c4a18a26	T1110	Brute Force / Credential Access
ac438801	T1110	Brute Force / Credential Access
d119964c	T1110	Brute Force / Credential Access
17d71b7e	T1110	Brute Force / Credential Access
054de0c5	T1110	Brute Force / Credential Access
fb3cbe3e	T1110	Brute Force / Credential Access
17f32518	T1110	Brute Force / Credential Access
b01c1309	T1110	Brute Force / Credential Access
ce71b989	T1110	Brute Force / Credential Access

4. Source IP Concentration Analysis

Source IP	Event Count
195.178.110.108	36
216.244.66.199	15
164.92.103.174	8
79.124.40.174	6
178.20.210.148	4
198.244.240.20	3
45.195.7.235	3
178.16.55.142	2
204.76.203.212	2
212.154.119.3	2
185.73.130.137	2
43.166.1.243	2
44.233.146.111	1
195.178.110.68	1
109.234.161.199	1
77.55.253.213	1
103.191.208.118	1
198.54.126.38	1
162.55.240.80	1
143.95.111.157	1
178.128.239.177	1
103.2.225.70	1
167.99.116.143	1
43.155.73.192	1
217.216.36.182	1
103.143.231.246	1
39.109.116.19	1

5. Case Intelligence Summary

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