Digital Forensic Incident Report

Case ID: 65a23c52

Engine: DFIR-AI Hybrid (Deterministic + Semantic)

Generated: 2026-01-06 10:20:05.740233+00:00 UTC

CONFIDENTIAL – FOR AUTHORIZED USE ONLY

1. Executive Summary

The incident involves multiple web security events and network communications from various IP addresses. Notab

2. Incident Metrics Overview

- Total forensic artifacts analyzed: 100
- Unique artifact types: 2
- Waf Correlation events observed: 14
- Sql Injection events observed: 4
- Access Denied events observed: 39
- Protocol Abuse events observed: 9
- Lfi events observed: 24

3. Attack Vector Analysis

- Waf Correlation — 14 correlated events indicating automated probing or exploitation attempts.
- Sql Injection — 4 correlated events indicating automated probing or exploitation attempts.
- Access Denied — 39 correlated events indicating automated probing or exploitation attempts.
- Protocol Abuse — 9 correlated events indicating automated probing or exploitation attempts.
- Lfi — 24 correlated events indicating automated probing or exploitation attempts.

4. Source IP Behavioral Analysis

Source IP: 91.107.124.38

- Total events: 3
- WAF_CORRELATION detected from 91.107.124.38 (2 occurrences)
- SQL_INJECTION detected from 91.107.124.38 (1 occurrences)

Source IP: 157.20.32.130

- Total events: 24
- ACCESS_DENIED detected from 157.20.32.130 (3 occurrences)
- Network communication observed (9 occurrences)
- LFI detected from 157.20.32.130 (12 occurrences)

Source IP: 222.252.11.23

- Total events: 3
- ACCESS_DENIED detected from 222.252.11.23 (3 occurrences)

Source IP: 118.70.190.36

- Total events: 2
- ACCESS_DENIED detected from 118.70.190.36 (2 occurrences)

Source IP: 222.252.11.133

- Total events: 1
- ACCESS_DENIED detected from 222.252.11.133 (1 occurrences)

Source IP: 160.191.139.216

- Total events: 6
- ACCESS_DENIED detected from 160.191.139.216 (6 occurrences)

Source IP: 81.88.49.27

- Total events: 6
- ACCESS_DENIED detected from 81.88.49.27 (6 occurrences)

Source IP: 173.199.123.6

- Total events: 3
- WAF_CORRELATION detected from 173.199.123.6 (2 occurrences)
- SQL_INJECTION detected from 173.199.123.6 (1 occurrences)

Source IP: 204.76.203.18
- Total events: 1
- PROTOCOL_ABUSE detected from 204.76.203.18 (1 occurrences)

Source IP: 154.82.150.126
- Total events: 1
- PROTOCOL_ABUSE detected from 154.82.150.126 (1 occurrences)

Source IP: 154.82.171.11
- Total events: 1
- PROTOCOL_ABUSE detected from 154.82.171.11 (1 occurrences)

Source IP: 156.239.204.135
- Total events: 1
- PROTOCOL_ABUSE detected from 156.239.204.135 (1 occurrences)

Source IP: 154.82.169.248
- Total events: 1
- PROTOCOL_ABUSE detected from 154.82.169.248 (1 occurrences)

Source IP: 156.239.206.170
- Total events: 1
- PROTOCOL_ABUSE detected from 156.239.206.170 (1 occurrences)

Source IP: 51.38.109.223
- Total events: 3
- LFI detected from 51.38.109.223 (3 occurrences)

Source IP: 41.90.64.136
- Total events: 3
- WAF_CORRELATION detected from 41.90.64.136 (2 occurrences)
- PROTOCOL_ABUSE detected from 41.90.64.136 (1 occurrences)

Source IP: 66.240.223.230
- Total events: 6
- ACCESS_DENIED detected from 66.240.223.230 (6 occurrences)

Source IP: 174.142.31.70
- Total events: 6
- ACCESS_DENIED detected from 174.142.31.70 (6 occurrences)

Source IP: 45.227.162.235
- Total events: 3
- WAF_CORRELATION detected from 45.227.162.235 (2 occurrences)
- SQL_INJECTION detected from 45.227.162.235 (1 occurrences)

Source IP: 194.195.245.44
- Total events: 6
- ACCESS_DENIED detected from 194.195.245.44 (6 occurrences)

Source IP: 47.128.114.191
- Total events: 1
- Network communication observed (1 occurrences)

Source IP: 34.78.138.227
- Total events: 1
- PROTOCOL_ABUSE detected from 34.78.138.227 (1 occurrences)

Source IP: 34.82.67.239
- Total events: 3
- WAF_CORRELATION detected from 34.82.67.239 (2 occurrences)
- PROTOCOL_ABUSE detected from 34.82.67.239 (1 occurrences)

Source IP: 54.37.118.70
- Total events: 3
- WAF_CORRELATION detected from 54.37.118.70 (2 occurrences)
- SQL_INJECTION detected from 54.37.118.70 (1 occurrences)

Source IP: 93.123.109.135
- Total events: 11
- WAF_CORRELATION detected from 93.123.109.135 (2 occurrences)
- LFI detected from 93.123.109.135 (9 occurrences)

5. Chronological Event Timeline

2026-01-06 10:19:42.305672+00:00 — WAF_CORRELATION detected from 91.107.124.38
2026-01-06 10:19:42.306003+00:00 — WAF_CORRELATION detected from 91.107.124.38
2026-01-06 10:19:42.306037+00:00 — SQL_INJECTION detected from 91.107.124.38
2026-01-06 10:19:42.306239+00:00 — ACCESS_DENIED detected from 157.20.32.130
2026-01-06 10:19:42.306343+00:00 — ACCESS_DENIED detected from 157.20.32.130
2026-01-06 10:19:42.306760+00:00 — Network communication observed
2026-01-06 10:19:42.306873+00:00 — ACCESS_DENIED detected from 157.20.32.130
2026-01-06 10:19:42.306939+00:00 — Network communication observed
2026-01-06 10:19:42.306997+00:00 — Network communication observed
2026-01-06 10:19:42.307096+00:00 — Network communication observed
2026-01-06 10:19:42.307152+00:00 — Network communication observed
2026-01-06 10:19:42.307231+00:00 — Network communication observed
2026-01-06 10:19:42.307288+00:00 — Network communication observed
2026-01-06 10:19:42.307400+00:00 — Network communication observed
2026-01-06 10:19:42.307495+00:00 — Network communication observed
2026-01-06 10:19:42.307604+00:00 — ACCESS_DENIED detected from 222.252.11.23
2026-01-06 10:19:42.307701+00:00 — ACCESS_DENIED detected from 118.70.190.36
2026-01-06 10:19:42.307798+00:00 — ACCESS_DENIED detected from 222.252.11.23
2026-01-06 10:19:42.307901+00:00 — ACCESS_DENIED detected from 118.70.190.36
2026-01-06 10:19:42.308016+00:00 — ACCESS_DENIED detected from 222.252.11.23
2026-01-06 10:19:42.308116+00:00 — ACCESS_DENIED detected from 222.252.11.133
2026-01-06 10:19:42.308233+00:00 — ACCESS_DENIED detected from 160.191.139.216
2026-01-06 10:19:42.308328+00:00 — ACCESS_DENIED detected from 160.191.139.216
2026-01-06 10:19:42.308419+00:00 — ACCESS_DENIED detected from 160.191.139.216
2026-01-06 10:19:42.308510+00:00 — ACCESS_DENIED detected from 160.191.139.216
2026-01-06 10:19:42.308602+00:00 — ACCESS_DENIED detected from 160.191.139.216
2026-01-06 10:19:42.308692+00:00 — ACCESS_DENIED detected from 160.191.139.216
2026-01-06 10:19:42.308781+00:00 — ACCESS_DENIED detected from 81.88.49.27
2026-01-06 10:19:42.308871+00:00 — ACCESS_DENIED detected from 81.88.49.27
2026-01-06 10:19:42.308960+00:00 — ACCESS_DENIED detected from 81.88.49.27
2026-01-06 10:19:42.309050+00:00 — ACCESS_DENIED detected from 81.88.49.27
2026-01-06 10:19:42.309174+00:00 — ACCESS_DENIED detected from 81.88.49.27
2026-01-06 10:19:42.309281+00:00 — ACCESS_DENIED detected from 81.88.49.27
2026-01-06 10:19:42.309496+00:00 — WAF_CORRELATION detected from 173.199.123.6
2026-01-06 10:19:42.309712+00:00 — WAF_CORRELATION detected from 173.199.123.6
2026-01-06 10:19:42.309736+00:00 — SQL_INJECTION detected from 173.199.123.6
2026-01-06 10:19:42.309925+00:00 — PROTOCOL_ABUSE detected from 204.76.203.18
2026-01-06 10:19:42.310152+00:00 — PROTOCOL_ABUSE detected from 154.82.150.126
2026-01-06 10:19:42.310416+00:00 — PROTOCOL_ABUSE detected from 154.82.171.11
2026-01-06 10:19:42.310631+00:00 — PROTOCOL_ABUSE detected from 156.239.204.135

2026-01-06 10:19:42.310853+00:00 — PROTOCOL_ABUSE detected from 154.82.169.248
2026-01-06 10:19:42.311082+00:00 — PROTOCOL_ABUSE detected from 156.239.206.170
2026-01-06 10:19:42.311240+00:00 — LFI detected from 51.38.109.223
2026-01-06 10:19:42.311403+00:00 — LFI detected from 51.38.109.223
2026-01-06 10:19:42.311505+00:00 — LFI detected from 51.38.109.223
2026-01-06 10:19:42.311706+00:00 — WAF_CORRELATION detected from 41.90.64.136
2026-01-06 10:19:42.311904+00:00 — WAF_CORRELATION detected from 41.90.64.136
2026-01-06 10:19:42.312114+00:00 — PROTOCOL_ABUSE detected from 41.90.64.136
2026-01-06 10:19:42.312242+00:00 — ACCESS_DENIED detected from 66.240.223.230
2026-01-06 10:19:42.312327+00:00 — ACCESS_DENIED detected from 66.240.223.230
2026-01-06 10:19:42.312414+00:00 — ACCESS_DENIED detected from 66.240.223.230
2026-01-06 10:19:42.312499+00:00 — ACCESS_DENIED detected from 66.240.223.230
2026-01-06 10:19:42.312581+00:00 — ACCESS_DENIED detected from 66.240.223.230
2026-01-06 10:19:42.312712+00:00 — ACCESS_DENIED detected from 66.240.223.230
2026-01-06 10:19:42.312867+00:00 — LFI detected from 157.20.32.130
2026-01-06 10:19:42.312992+00:00 — LFI detected from 157.20.32.130
2026-01-06 10:19:42.313090+00:00 — LFI detected from 157.20.32.130
2026-01-06 10:19:42.313223+00:00 — LFI detected from 157.20.32.130
2026-01-06 10:19:42.313341+00:00 — LFI detected from 157.20.32.130
2026-01-06 10:19:42.313450+00:00 — LFI detected from 157.20.32.130
2026-01-06 10:19:42.313537+00:00 — ACCESS_DENIED detected from 174.142.31.70
2026-01-06 10:19:42.313633+00:00 — ACCESS_DENIED detected from 174.142.31.70
2026-01-06 10:19:42.313719+00:00 — ACCESS_DENIED detected from 174.142.31.70
2026-01-06 10:19:42.313913+00:00 — WAF_CORRELATION detected from 45.227.162.235
2026-01-06 10:19:42.313996+00:00 — ACCESS_DENIED detected from 174.142.31.70
2026-01-06 10:19:42.314209+00:00 — WAF_CORRELATION detected from 45.227.162.235
2026-01-06 10:19:42.314250+00:00 — SQL_INJECTION detected from 45.227.162.235
2026-01-06 10:19:42.314335+00:00 — ACCESS_DENIED detected from 174.142.31.70
2026-01-06 10:19:42.314419+00:00 — ACCESS_DENIED detected from 174.142.31.70
2026-01-06 10:19:42.314520+00:00 — LFI detected from 157.20.32.130
2026-01-06 10:19:42.314623+00:00 — LFI detected from 157.20.32.130
2026-01-06 10:19:42.314720+00:00 — LFI detected from 157.20.32.130
2026-01-06 10:19:42.314823+00:00 — LFI detected from 157.20.32.130
2026-01-06 10:19:42.314923+00:00 — LFI detected from 157.20.32.130
2026-01-06 10:19:42.315018+00:00 — LFI detected from 157.20.32.130
2026-01-06 10:19:42.315112+00:00 — ACCESS_DENIED detected from 194.195.245.44
2026-01-06 10:19:42.315225+00:00 — ACCESS_DENIED detected from 194.195.245.44
2026-01-06 10:19:42.315323+00:00 — ACCESS_DENIED detected from 194.195.245.44
2026-01-06 10:19:42.315416+00:00 — ACCESS_DENIED detected from 194.195.245.44
2026-01-06 10:19:42.315503+00:00 — ACCESS_DENIED detected from 194.195.245.44
2026-01-06 10:19:42.315669+00:00 — Network communication observed
2026-01-06 10:19:42.315756+00:00 — ACCESS_DENIED detected from 194.195.245.44
2026-01-06 10:19:42.315917+00:00 — PROTOCOL_ABUSE detected from 34.78.138.227
2026-01-06 10:19:42.316113+00:00 — WAF_CORRELATION detected from 34.82.67.239
2026-01-06 10:19:42.316351+00:00 — WAF_CORRELATION detected from 34.82.67.239
2026-01-06 10:19:42.316587+00:00 — PROTOCOL_ABUSE detected from 34.82.67.239
2026-01-06 10:19:42.316768+00:00 — WAF_CORRELATION detected from 54.37.118.70
2026-01-06 10:19:42.316966+00:00 — WAF_CORRELATION detected from 54.37.118.70
2026-01-06 10:19:42.317003+00:00 — SQL_INJECTION detected from 54.37.118.70
2026-01-06 10:19:42.317208+00:00 — WAF_CORRELATION detected from 93.123.109.135
2026-01-06 10:19:42.317302+00:00 — LFI detected from 93.123.109.135
2026-01-06 10:19:42.317407+00:00 — LFI detected from 93.123.109.135
2026-01-06 10:19:42.317543+00:00 — LFI detected from 93.123.109.135
2026-01-06 10:19:42.317639+00:00 — LFI detected from 93.123.109.135
2026-01-06 10:19:42.317732+00:00 — LFI detected from 93.123.109.135
2026-01-06 10:19:42.317835+00:00 — LFI detected from 93.123.109.135

2026-01-06 10:19:42.317941+00:00 — LFI detected from 93.123.109.135
2026-01-06 10:19:42.318139+00:00 — WAF_CORRELATION detected from 93.123.109.135
2026-01-06 10:19:42.318250+00:00 — LFI detected from 93.123.109.135
2026-01-06 10:19:42.318351+00:00 — LFI detected from 93.123.109.135

6. Hash & Payload Analysis

No file hashes (MD5, SHA1, SHA256) were observed. All artifacts represent network-layer or application-layer e

7. Confidence & Limitations

- Scoring derived from deterministic rules combined with semantic similarity.
- Analysis limited to provided server access logs.
- No endpoint telemetry, memory, or file system artifacts were available.