Digital Forensic Incident Report

Case ID: a67fa80a

Generated: 2026-01-06 12:56:00.138868+00:00 UTC

1. Executive Summary

Incident summary - A broad collection of external-origin web security events was observed, spanning multiple IPs and ports. The events include PROTOCOL_ABUSE, WAF_CORRELATION, SQL_INJECTION, XSS, LFI, RCE, and ACCESS_DENIED indicators, as well as several WordPress_ATTACK detections. Representative artifacts illustrating these categories are listed below. - PROTOCOL_ABUSE - a67fa80a-52bc-40ab-a8a2-4c33ac2e1e2d: PROTOCOL_ABUSE from 204.76.203.18 to port 58922 - eb871500-c4f5-4a54-bdcd-3a12947b1f1b: PROTOCOL_ABUSE from 216.244.66.199 to port 53802 - 6477b629-27ea-4d35-a624-3b1884584ffd: PROTOCOL_ABUSE from 198.235.24.117 to port 64918 - c0df0b17-89ed-496a-955a-981c071accc0: PROTOCOL_ABUSE from 216.244.66.199 to port 46508 - ede7eef5-ee04-4f6f-9d4a-cd86199eec56: PROTOCOL_ABUSE from 216.244.66.199 to port 51264 - WAF_CORRELATION - c61ec2b4-b484-48be-854c-2ea70f8929ba: WAF_CORRELATION from 176.31.139.11 to port 39570 - bb045ab7-42be-4e7f-ad13-ddcb16b76cd8: WAF_CORRELATION from 176.31.139.11 to port 39570 - c5e37135-a3ac-4bb3-9a9c-f382ec55f2ff: WAF_CORRELATION from 216.244.66.199 to port 53802 - bd271c99-59bf-46b4-97b4-096a825a08f5: WAF_CORRELATION from 216.244.66.199 to port 53802 - dbe1fc9b-227b-40c0-83e4-fae3999fd149: WAF_CORRELATION from 216.244.66.199 to port 51264 - SQL_INJECTION - 7a48004a-50a7-4670-88aa-ad3dec49ff04: SQL_INJECTION from 176.31.139.11 to port 39570 - e91daab1-2374-460e-ac60-407848ba4eed: SQL_INJECTION from 5.39.109.162 to port 49526 - 28fbba69-3fd1-4fc7-8395-1abb7e8ce33f: SQL_INJECTION from 92.222.108.125 to port 36424 - ba30a2eb-6733-4bc9-8f36-682708a23edf: SQL_INJECTION from 92.222.108.106 to port 37670 - c453e71c-b503-4587-aeb5-8ce33d9bcc10: SQL_INJECTION from 103.152.164.82 to port 42748 - XSS - 897b9933-219d-4fe2-b79d-ab474ad68463: XSS from 105.160.12.14 to port 3302 - bbd93353-f539-426c-b30b-fe7b2c64f014: XSS from 105.160.12.14 to port 3300 - 4d7e0b1d-8770-4b55-b95a-6f90f5be207a: XSS from 105.160.12.14 to port 3301 - LFI - 1700e73c-d084-482a-970a-728ff4e67795: LFI from 51.38.109.223 to port 58308 - 63248d01-6ab9-4db2-aff8-d72fffe065e9: LFI from 51.38.109.223 to port 58308 - ae2b8da3-27c4-4149-9e4d-6a95b674030e: LFI from 185.241.208.170 to port 55322 - RCE - 3e8da282-fbf3-4efa-9010-5ef19a0b8045: RCE from 193.142.147.209 to port 28618 - 8d471e2c-1934-4865-b2bd-421cc3370abd: RCE from 193.142.147.209 to port 28618 - 721e47df-8d2a-43c9-ad0f-8f988f5b4b03: RCE from 193.142.147.209 to port 28618 - f5333acc-e42c-409a-9cdd-60c5f5053198: RCE from 193.142.147.209 to port 28618 - ccc3a3a8-8a87-413b-82a4-6ce3922fa939: RCE from 193.142.147.209 to port 28618 - ACCESS_DENIED (blocked attempts) - 195.201.242.21 shows multiple ACCESS_DENIED entries (e.g.,

13cd35de-9b78-44c3-a3d9-90053c33a387; b587a74b-1112-49d8-b43c-a8cefabc7fea; 0f794aa6-c2e3-430b-924b-04df88894887) - 103.112.62.56 shows several ACCESS_DENIED entries (e.g., e2abcb84-f356-4d0f-a1ab-26b3e3ea4eed) - 77.78.76.152 shows ACCESS_DENIED (dd429246-bfd0-47d1-af9f-38191744931e) - 116.202.132.228 shows multiple ACCESS_DENIED entries (da12fe2e-7717-4a06-ac4a-c7f12dbe26b4; e0f...?; 19d...) - 133.167.43.48 shows ACCESS_DENIED (a191078d-d634-4e9c-88a6-d4881081a33b) - WordPress_ATTACK - 45bdedb6-9f34-4114-a41f-0b8cc2175369: WORDPRESS_ATTACK from 62.164.177.243 - b09d4a19-ef6c-4a22-8f2c-0d5d935e4ca9: WORDPRESS_ATTACK from 62.164.177.243 - 35c3c7b2-9956-424f-afcd-807c72a1b6fb: WORDPRESS_ATTACK from 62.164.177.243 - Representative network activity (sample) - f319f0d8-952e-4cd5-a3c0-954cfc7dd579: Network communication observed to 197.248.93.73:9351 - a057555a-bbdf-4f10-9ae5-e50e2c806184: Network communication observed to 47.128.31.170:53690 - 5e3d4a06-b4d9-494f-92f1-fe1429a82ee7: PROTOCOL_ABUSE observed from 95.214.55.71 to port 37262 - 42a1fe8f-d6df-4bb2-a575-57945f0a3c1c: ACCESS_DENIED from 114.108.165.112 to port 38478 Notes - The artifacts show widespread external probing across many IPs and regions, with repeated high-risk patterns (SQL_INJECTION, XSS, RCE, LFI) and multiple protocol-abuse indicators. - Several attempts were explicitly denied (ACCESS_DENIED) across a range of external sources. - No explicit indication of internal hosts compromised or data exfiltration is present in the provided evidence. - Activity includes both WAF_CORRELATION hits and direct attack-type detections, suggesting automated or mass-action scanning from external actors. If you want, I can produce a filtered list by source country or summarize counts per category using the artifacts above.

2. MITRE ATT&CK; Mapping & Tactic Rollup

Indicator	Technique ID	Technique Name
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
SQL_INJECTION	T1190	Exploit Public-Facing Application
WAF_CORRELATION	T1046	Network Service Discovery
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
SQL_INJECTION	T1190	Exploit Public-Facing Application
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol

Indicator	Technique ID	Technique Name
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
SQL_INJECTION	T1190	Exploit Public-Facing Application
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery

Indicator	Technique ID	Technique Name
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
SQL_INJECTION	T1190	Exploit Public-Facing Application
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol

Indicator	Technique ID	Technique Name
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
ACCESS_DENIED	T1110	Brute Force

Indicator	Technique ID	Technique Name
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force

Indicator	Technique ID	Technique Name
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
SQL_INJECTION	T1190	Exploit Public-Facing Application
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
SQL_INJECTION	T1190	Exploit Public-Facing Application
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
SQL_INJECTION	T1190	Exploit Public-Facing Application
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
LFI	T1005	Data from Local System
LFI	T1005	Data from Local System
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol

Indicator	Technique ID	Technique Name
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol

Indicator	Technique ID	Technique Name
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force

Indicator	Technique ID	Technique Name
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
SQL_INJECTION	T1190	Exploit Public-Facing Application
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery

Indicator	Technique ID	Technique Name
SQL_INJECTION	T1190	Exploit Public-Facing Application
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery

Indicator	Technique ID	Technique Name
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
SQL_INJECTION	T1190	Exploit Public-Facing Application
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery

Indicator	Technique ID	Technique Name
LFI	T1005	Data from Local System
LFI	T1005	Data from Local System
LFI	T1005	Data from Local System
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
LFI	T1005	Data from Local System
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
SQL_INJECTION	T1190	Exploit Public-Facing Application
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
SQL_INJECTION	T1190	Exploit Public-Facing Application
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol

Indicator	Technique ID	Technique Name
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
SQL_INJECTION	T1190	Exploit Public-Facing Application
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
SQL_INJECTION	T1190	Exploit Public-Facing Application
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
SQL_INJECTION	T1190	Exploit Public-Facing Application
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
SQL_INJECTION	T1190	Exploit Public-Facing Application
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
SQL_INJECTION	T1190	Exploit Public-Facing Application

Indicator	Technique ID	Technique Name
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
SQL_INJECTION	T1190	Exploit Public-Facing Application
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
SQL_INJECTION	T1190	Exploit Public-Facing Application
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
SQL_INJECTION	T1190	Exploit Public-Facing Application
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol

Indicator	Technique ID	Technique Name
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
SQL_INJECTION	T1190	Exploit Public-Facing Application
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery

Indicator	Technique ID	Technique Name
SQL_INJECTION	T1190	Exploit Public-Facing Application
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
LFI	T1005	Data from Local System
LFI	T1005	Data from Local System
LFI	T1005	Data from Local System
LFI	T1005	Data from Local System
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force
ACCESS_DENIED	T1110	Brute Force

Indicator	Technique ID	Technique Name
PROTOCOL_ABUSE	T1048	Exfiltration Over Alternative Protocol
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
SQL_INJECTION	T1190	Exploit Public-Facing Application
WAF_CORRELATION	T1046	Network Service Discovery
WAF_CORRELATION	T1046	Network Service Discovery
SQL_INJECTION	T1190	Exploit Public-Facing Application
ACCESS_DENIED	T1110	Brute Force
WAF_CORRELATION	T1046	Network Service Discovery

ATT&CK Tactic	Observed Events
Exfiltration	84
Discovery	158
Initial Access	24
Credential Access	180
Collection	10

3. Severity Heat Visualization

Severity	Count	
HIGH	0	
MEDIUM	0	
LOW	511	

4. Per-IP Geo-Behavioral Profiles

Source IP	Events	Countries	Severity Mix
Unknown	511	Unknown:511	LOW:511