

SOC Tier 2 Investigation Report

Log Source: access_combined

Platform: Splunk Enterprise (Kali Linux VM)

Index: main

Analyst: SOC Tier 2

Date: August 1, 2025

Objective

Perform deep-dive analysis of HTTP access logs from access_combined sourcetype to identify patterns of malicious activity and anomalous web behavior. The goal is to develop detection hypotheses, confirm benign behavior, and isolate suspicious patterns.

Initial Recon & Data Validation

- Verified that data is being indexed in main and not web.
 - Confirmed sourcetype=access_combined has log records present.
 - Validated fields such as clientip, uri, status, method, referer, useragent, and JSESSIONID are parsed correctly.
 - Ensured time range was set to “All Time” during exploratory phases to avoid missing older logs.
-

Phase 1: Unique Page Requests by Client IP

Objective: Identify IPs making high numbers of unique page requests — possible indicators of scanning.

Search Example:

```
index=main sourcetype=access_combined
| stats dc(uri_path) as unique_pages by clientip
| where unique_pages > 10
| sort -unique_pages
```

Findings:

- Maximum unique_pages was **10**.
- No client had more than 10, indicating low variation and possible normal browsing.
- Sample IPs were examined manually. User behavior appeared legitimate (e.g., normal referers, consistent user agents).

Conclusion: This activity was **normal web behavior**, likely non-malicious.

The image displays two screenshots of the Splunk search interface, showing the results of a search for web traffic data.

Top Screenshot: The search query is `index="main" sourcetype="access_combined"`. The results show 116,455 events. The timeline view is selected, showing a horizontal bar chart. The event list is displayed below, showing two events from 8/20/24 at 1:59:59.000 PM and 1:59:58.000 PM. The first event is a GET request to `/viewCart` from `169.124.122.208` with a user agent of `Mozilla/4.0 (compatible; MSIE 6.1; Windows XP)`. The second event is a GET request to `/viewCart` from `37.41.142.232` with a user agent of `Mozilla/5.0 (Windows NT 6.0; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0`.

Bottom Screenshot: The search query is `index="main" sourcetype="access_combined" | head 5 | table _time clientip method uri_path status bytes referer useragent`. The results show 5 events. The statistics view is selected, showing a table of the top 5 events. The table has columns for `_time`, `clientip`, `method`, `uri_path`, `status`, `bytes`, `referer`, and `useragent`.

_time	clientip	method	uri_path	status	bytes	referer	useragent
2024-08-20 13:59:59	169.124.122.208	GET	/viewCart	200	2037	https://www3.samplesite.ca/addItem	Mozilla/4.0 (compatible; MSIE 6.1; Windows XP)
2024-08-20 13:59:58	37.41.142.232	GET	/viewCart	200	761	https://www2.samplesite.ca/removeItem	Mozilla/5.0 (Windows NT 6.0; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0
2024-08-20 13:59:57	134.41.203.158	GET	/viewCart	200	523	https://www1.samplesite.ca/	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_0) AppleWebKit/537.36 (KHTML, like Gecko)

Search | Splunk 10.0.0 x Search | Splunk 10.0.0 x VirusTotal - API Key - kali x MalShare

127.0.0.1:8000/en-US/app/search/search?q=search index%3Dmain sourcetype%3Daccess_

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

Save As Create Table View Close

```
index=main sourcetype=access_combined
| stats count dc(uri) as unique_pages by clientip
```

Time range: All time

✓ 116,455 events (before 8/1/25 8:08:24.000 AM) No Event Sampling

Job

Events Patterns **Statistics (14,302)** Visualization

Show: 100 Per Page Format Preview: On

clientip	count	unique_pages
0.101.30.157	6	4
0.101.54.9	10	8
0.106.41.7	1	1
0.111.7.77	12	9

Search | Splunk 10.0.0 x Search | Splunk 10.0.0 x VirusTotal - API Key - kali x MalShare

127.0.0.1:8000/en-US/app/search/search?q=search index%3Dmain sourcetype%3Daccess_

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

Save As Create Table View Close

```
index=main sourcetype=access_combined
| stats count dc(uri) as unique_pages by clientip
| where unique_pages >= 10
| sort - unique_pages
```

Time range: All time

✓ 116,455 events (before 8/1/25 8:12:13.000 AM) No Event Sampling

Job

Events Patterns **Statistics (1,022)** Visualization

Show: 100 Per Page Format Preview: On

clientip	count	unique_pages
0.171.209.73	12	10
0.27.146.208	12	10
0.55.95.96	12	10
0.61.225.141	12	10
1.184.181.190	12	10
1.231.157.132	12	10

Search | Splunk 10.0.0 x Search | Splunk 10.0.0 x VirusTotal - API Key - kali x MalShare

127.0.0.1:8000/en-US/app/search/search?q=search index%3Dmain sourcetype%3Daccess_combined cli

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

splunk>enterprise Apps Administrator 4 Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

Save As Create Table View Close

```
index=main sourcetype=access_combined clientip="0.171.209.73"
| stats count by uri, status, method, useragent
| sort - count
```

Time range: All time

12 events (before 8/1/25 8:17:05.000 AM) No Event Sampling

Job II Smart Mode

Events Patterns **Statistics (10)** Visualization

Show: 100 Per Page Format Preview: On

uri	status	method	useragent	count
/viewCart	200	GET	Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1667.0 Safari/537.36	3
/addItem?item=1000014&qty=1	200	POST	Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1667.0 Safari/537.36	1
/addItem?item=1000016&qty=1	200	POST	Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1667.0 Safari/537.36	1

Search | Splunk 10.0.0 x Search | Splunk 10.0.0 x VirusTotal - API Key - kali x MalShare

127.0.0.1:8000/en-US/app/search/search?q=search index%3Dmain sourcetype%3Daccess_combined%0

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

splunk>enterprise Apps Administrator 4 Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

Save As Create Table View Close

```
index=main sourcetype=access_combined
| search uri IN ("/admin", "/.env", "/phpmyadmin", "/config", "/wp-login.php", "/login", "/.git", "/shell", "/cmd", "/debug")
| table _time clientip method uri status useragent
```

Time range: All time

2,221 events (before 8/1/25 9:23:00.000 AM) No Event Sampling

Job II Smart Mode

Events Patterns **Statistics (2,221)** Visualization

Show: 100 Per Page Format Preview: On

< Prev 1 2 3 4 5 6 7 8 ... Next >

_time	clientip	method	uri	status	useragent
2024-08-20 08:07:08	41.215.21.100	GET	/phpMyAdmin	404	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1664.3 Safari/537.36
2024-08-20 08:04:16	228.164.238.156	GET	/admin	403	Mozilla/4.0 (compatible; MSIE 6.1; Windows XP)
2024-08-20 08:04:16	130.132.72.167	GET	/admin	403	Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1667.0 Safari/537.36
2024-08-20 08:03:25	102.49.10.153	GET	/admin	403	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_0) AppleWebKit/537.36 (KHTML, like Gecko)

Search | Splunk 10.0.0 x Search | Splunk 10.0.0 x VirusTotal - API Key - kali x MalShare

127.0.0.1:8000/en-US/app/search/search?q=search index%3Dmain sourcetype%3Daccess_combined%0

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

splunk>enterprise Apps Administrator 4 Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

Save As Create Table View Close

```
index=main sourcetype=access_combined
| search uri IN ("/admin", "/.env", "/phpmyadmin", "/config", "/wp-login.php", "/login", "/.git", "/shell", "/cmd", "/debug")
| stats count by clientip
| sort - count
```

Time range: All time

2,221 events (before 8/1/25 9:31:19.000 AM) No Event Sampling Job

Events Patterns **Statistics (2,221)** Visualization

Show: 100 Per Page Format Preview: On

clientip	count
0.106.41.7	1
0.138.44.134	1
0.165.214.112	1
0.188.139.210	1
0.197.177.210	1

Search | Splunk 10.0.0 x Search | Splunk 10.0.0 x VirusTotal - API Key - kali x MalShare

127.0.0.1:8000/en-US/app/search/search?q=search index%3Dmain sourcetype%3Daccess_combined%0

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

splunk>enterprise Apps Administrator 4 Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

Save As Create Table View Close

```
index=main sourcetype=access_combined
| search uri IN ("/admin", "/.env", "/phpmyadmin", "/config", "/wp-login.php", "/login", "/.git", "/shell", "/cmd", "/debug")
| top useragent
```

Time range: All time

2,221 events (before 8/1/25 9:32:18.000 AM) No Event Sampling Job

Events Patterns **Statistics (10)** Visualization

Show: 100 Per Page Format Preview: On

useragent	count	percent
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1664.3 Safari/537.36	214	9.635299
Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/5.0)	126	5.673120
Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1667.0 Safari/537.36	123	5.538046
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.6; rv:25.0) Gecko/20100101 Firefox/25.0	121	5.447396
Opera/9.80 (Windows NT 5.1; U; zh-sg) Presto/2.9.181 Version/12.00	120	5.402372
Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:25.0) Gecko/20100101 Firefox/25.0	119	5.352047

Search | Splunk 10.0.0 x Search | Splunk 10.0.0 x VirusTotal - API Key - kali x MalShare

127.0.0.1:8000/en-US/app/search/search?q=search index%3Dmain sourcetype%3Daccess_combined

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

splunk>enterprise Apps Administrator 4 Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

Save As Create Table View Close

index=main sourcetype=access_combined | search uri IN ("/admin", "/.env", "/phpmyadmin", "/config", "/wp-login.php", "/login", "/.git", "/shell", "/cmd", "/debug") useragent="Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1664.3 Safari/537.36" Time range: All time

214 events (before 8/1/25 9:32:41.000 AM) No Event Sampling Job

Events (214) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect 1 hour per column

Format Show: 20 Per Page View: List

Hide Fields All Fields

	Time	Event
>	8/20/24 1:58:38.000 PM	46.187.87.47 - - [03/Aug/2014:23:58:38 +0000] "GET /admin HTTP/1.1" 403 793 "http://www.yahoo.com" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1664.3 Safari/537.36" "JSESSIONID=729F870D60855DACD2A570B131A08124" 29 host = kali source = /opt/splunk/etc/apps/OpsDataGen/data/access_log sourcetype = access_combined

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

Search | Splunk 10.0.0 x Search | Splunk 10.0.0 x VirusTotal - API Key - kali x MalShare

127.0.0.1:8000/en-US/app/search/search?q=search index%3Dmain sourcetype%3Daccess_combined%0

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

splunk>enterprise Apps Administrator 4 Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

Save As Create Table View Close

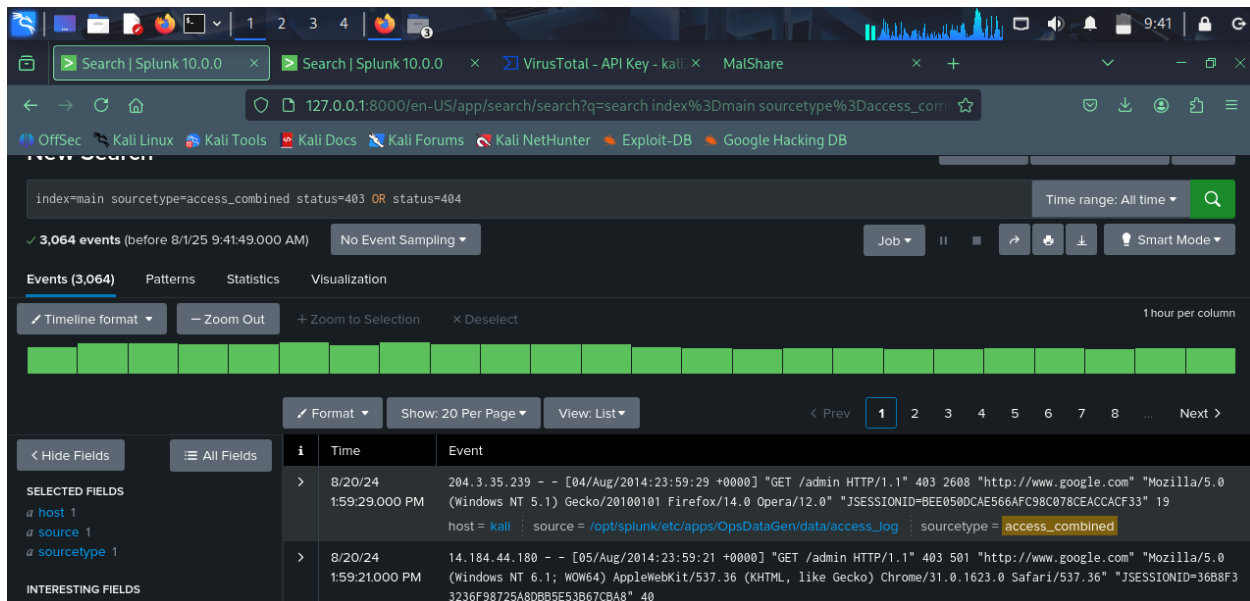
index=main sourcetype=access_combined | search useragent="Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_0)*" | stats count by uri, status | sort - count Time range: All time

11,379 events (before 8/1/25 9:36:50.000 AM) No Event Sampling Job

Events Patterns Statistics (1,440) Visualization

Show: 100 Per Page Format Preview: On

uri	status	count
/viewCart	200	2498
/home	200	1708
/error	200	469
/search?terms=Hoobles&category=3	200	363
/viewItem?item=1000014	200	363
/search?terms=Ripple&category=2	200	336
/viewItem?item=1000015	200	336
/addItem	503	315



Phase 2: Targeted Enumeration Detection

Objective: Identify probing attempts for known admin paths, suspicious tools, and status codes.

Search:

```
index=main sourcetype=access_combined status=403 OR status=404
| table _time uri status clientip user_agent
```

Result: 3,064 events with URIs like:

- /phpMyAdmin
- /admin
- /help

Observation:

- Most URIs are common brute-force and scan targets.
- Status codes primarily 403 (forbidden) and 404 (not found).
- Methods were mostly GET.

The top screenshot shows a Splunk search interface with the following search query: `index=main sourcetype=access_combined status=403 OR status=404 | table _time uri status clientip user_agent`. The results show 3,064 events. The table below represents the data shown in the screenshot:

_time	uri	status	clientip	user_agent
2024-08-20 08:36:45	/login.php	404	70.73.214.16	
2024-08-20 08:35:44	/admin	403	16.88.198.37	
2024-08-20 08:32:09	/admin	403	123.68.211.213	
2024-08-20 08:29:32	/login.php	404	116.203.39.96	
2024-08-20 08:26:53	/admin	403	123.210.80.179	
2024-08-20 08:22:31	/admin	403	157.116.41.89	
2024-08-20 08:19:39	/q9384f98ghvv	404	200.103.95.228	

The bottom screenshot shows a Splunk search interface with the following search query: `index=main sourcetype=access_combined status=403 OR status=404 clientip=0.82.159.39 | table _time uri status user_agent | sort _time`. The results show 1 event. The table below represents the data shown in the screenshot:

_time	uri	status	user_agent
2024-08-19 14:02:48	/help	404	

Phase 3: Top Aggressors by Count

Search:

```
index=main sourcetype=access_combined status=403 OR status=404
| stats count by clientip
| sort -count
```

Result:

- All IPs had count=1, suggesting scanning by **many unique IPs** — consistent with mass scan behavior (e.g., botnets or Shodan-like tools).

Alternative Pivot:


```
index=main sourcetype=access_combined status=403 OR status=404
| top clientip
```

Outcome:

- Top IPs still had count=1. Activity not concentrated from a single source.

Hypothesis: Distributed scanning (slow, stealthy enumeration).

New Search

```
index=main sourcetype=access_combined status=403 OR status=404
| stats count by clientip
| where count >= 1
| sort -count
```

3,064 events (before 8/1/25 9:56:44.000 AM) No Event Sampling

Events Patterns **Statistics (3,064)** Visualization

Show: 100 Per Page Format Preview: On

clientip	count
0.106.41.7	1
0.138.44.134	1
0.161.169.253	1

New Search

```
index=main sourcetype=access_combined status=403 OR status=404
| stats count by clientip
| where count >= 3
| sort -count
```

3,064 events (before 8/1/25 9:57:35.000 AM) No Event Sampling

Events Patterns **Statistics (0)** Visualization

Show: 100 Per Page Format Preview: On

No results found.

Phase 4: User Agent Analysis

Search:

```
index=main sourcetype=access_combined status=403 OR status=404
| top useragent
```

Result:

- Detected aggressive user agent strings (e.g., legacy browsers, known bot UAs).
- Sample: Firefox 25.0, Chrome 32.0 — unusual in 2025.

Manual Inspection:

- One such UA used over 200 times.
- IP 46.187.87.47 accessed /admin, received 403, used Yahoo as referer.

Conclusion: Behavior indicative of **automated scanner with spoofed headers**.

Final Observation: Lack of Multi-Request Patterns

- All IPs had a single event in statistics (count=1).
- Even high-volume URIs didn't correlate to repeated requests from same IP.

Theory: Noise from wide IP scanning or vulnerability mapping bots.

Recommendations

1. **Whitelist/Ignore** known benign patterns (e.g., Yahoo/Hotmail referers).
2. **Flag** unusual user agents or legacy browsers accessing sensitive paths.
3. **Build detection rules** for high `dc(uri_path)` per IP over short period.
4. **Alert** on sequences like /phpMyAdmin, /admin, /setup, /help by same IP.
5. **Rate-limit** or block high-entropy URI scans.