

# Brute force Analysis

## CEL

Celem analizy była identyfikacja i ocena podejrzanej incydentu bezpieczeństwa na serwerze internetowym na podstawie logów.

## ZASOBY

- Logi serwera www dostępne na platformie **Splunk**

### Practice Scenario

You are an SOC Level 1 Analyst on shift and have received an alert indicating a spike in activity on the organisation's web server.  
Your task is to dive into the logs and determine exactly what happened.

The logs for this task are located in the Splunk index task6. Use the following query: `index=task6`

Podczas analizy zidentyfikowano **dwa niezależne incydenty brute force**, różniące się czasem wystąpienia, źródłem oraz charakterystyką ruchu. Zdarzenia nie były ze sobą bezpośrednio powiązane i zostały przeanalizowane jako osobne przypadki w ramach tego samego typu ataku.

## OPIS ANALIZY

Największa liczba zarejestrowanych zdarzeń dotyczyła zapytań kierowanych do endpointu **/wp-login.php**.

The screenshot shows a Splunk search interface with the following details:

- Fields List:** Shows various log fields such as clientip, date\_hour, date\_minute, date\_month, date\_second, date\_usec, date\_zone, file, id, index, method, punct, referer, referer\_domain, req\_time, status, timeendpos, timestartpos, uri, user, useragent, version, and host.
- Search Results:** Two distinct events are listed, both originating from IP 10.10.243.134 on 11/08/2025 at 10:17:35 UTC, targeting the /wp-login.php endpoint.
  - The first event is labeled "-security-scanner" and is associated with host=ce-splunk, source=access.log, and sourcetype=access\_combined.
  - The second event is labeled "WPScan v3.8.28 (https://wpscan.com/wordpress)" and is also associated with host=ce-splunk, source=access.log, and sourcetype=access\_combined.
- Reports:** A summary table titled "Top 10 Values" shows the most frequent paths:

Path	Count	%
/wp-login.php	987	77.98%
/	38	2.58%
*	15	1.29%
/wp-cron.php	7	0.602%
/Core/Skin/Login.aspx	6	0.516%
/wp-admin/admin-ajax.php	5	0.43%
/wp-admin/load-styles.php	5	0.43%
/wp-admin.php	5	0.43%
/wp-admin/images/wordpress-logo.svg	3	0.258%
/wp-admin/load-scripts.php	3	0.258%

```

1 index="task6"
2 | stats count by clientip
3 | sort -count

```

1,169 events (before 18/02/2026 11:14:22.000) No Event Sampling ▾ Job ▾ II III ▾ Smart Mode ▾

Events Patterns Statistics (27) Visualization

Show: 20 Per Page ▾ Format ▾ Preview: On

clientip	count
10.10.243.134	746
167.172.41.141	340
::1	14
10.14.94.82	12
68.183.47.68	10
10.10.28.135	7
172.16.8.239	6
43.129.169.161	6
167.94.145.108	3
172.236.228.202	3
160.187.246.170	2
185.177.189.94	2
198.235.24.27	2
47.230.42.15	2

W pierwszym kroku przeanalizowano liczbę zapytań do wskazanego URI w podziale na adresy IP. Dwie wartości — **746 oraz 340 zapytań** — znaczco odbiegały od przyjętego baseline'u, co mogło wskazywać na:

- Rekonesans aplikacji,
- lub atak typu brute-force.

W celu potwierdzenia charakteru zdarzenia przeanalizowano:

- kody odpowiedzi serwera,
- metody zapytań,
- nagłówki User-Agent (pogrupowane i zliczone).

```

1 index="task6"
2 | stats count AS ile BY clientip uri status useragent method
3 | sort -ile

```

1,169 events (before 18/02/2026 11:18:02.000) No Event Sampling ▾ Job ▾ II III ▾ Smart Mode ▾

Events Patterns Statistics (230) Visualization

Show: 20 Per Page ▾ Format ▾ Preview: On

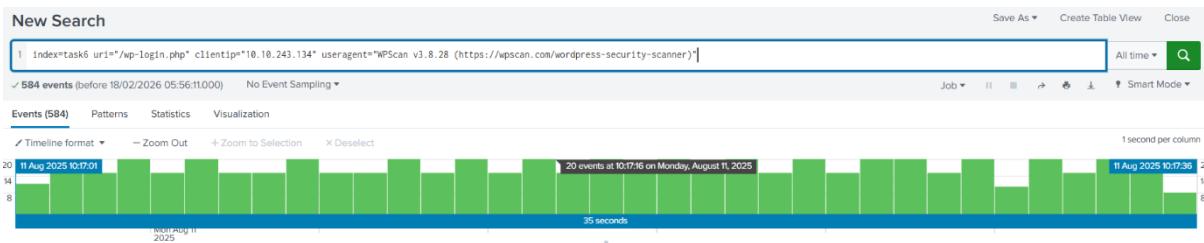
clientip	uri	status	useragent	method	ile
10.10.243.134	/wp-login.php	200	WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)	POST	583
167.172.41.141	/wp-login.php	200	Mozilla/5.0 (Hydra)	GET	158
167.172.41.141	/wp-login.php	200	Mozilla/5.0 (Hydra)	POST	157
::1	*	200	Apache/2.4.58 (Ubuntu) (internal dummy connection)	OPTIONS	14
167.172.41.141	/wp-admin/admin-ajax.php	200	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36	POST	5
167.172.41.141	/wp-cron.php?doing_wp_cron=t	404	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36	POST	5
10.14.94.82	/	200	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36	GET	4
10.10.243.134	/	200	WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)	GET	3
10.10.28.135	/	200	WordPress/6.8.1; http://10.10.28.135	GET	3
43.129.169.161	/Core/Skin/Login.aspx	301	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36	HEAD	3
43.129.169.161	/Core/Skin/Login.aspx	404	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36	HEAD	3

## WNIOSKI Z ANALIZY

### 1. Adres IP: 10.10.243.134

- Największa liczba zapytań (583) dotyczyła endpointu **/wp-login.php**
- Metoda: **POST**
- User-Agent: **WPScan** (narzędzie do skanowania WordPressa)

Charakter ruchu oraz wykorzystanie dedykowanego narzędzia bezpieczeństwa **silnie wskazują na zautomatyzowany atak typu brute-force.**



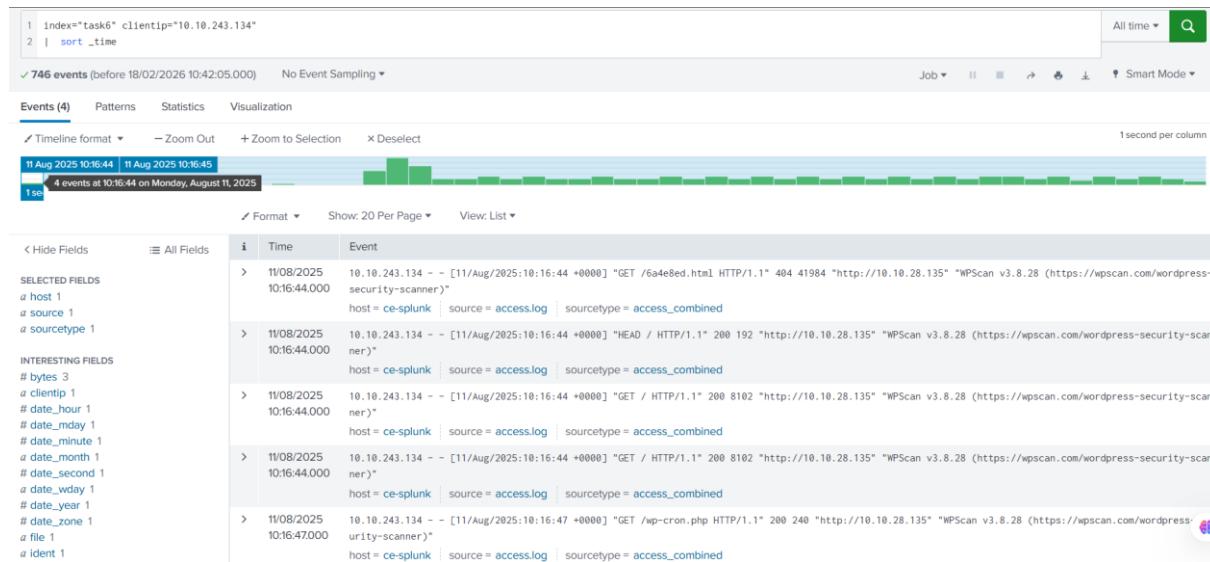
#### Czas trwania incydentu:

11 sierpnia 2025 r., **10:17:01 - 10:17:36** (ok. 35 sekund)

#### Timeline żądań:



Pierwsze zapytania już były wykonywane poprzez User-agent WPScan – brak wcześniejszego rekonesansu.



New Search		Save As ▾	Create Table View	Close
<pre>1 index="task6" clientip="10.10.243.134" 2   table _time method, uri, status</pre> <p>✓ 746 events (before 18/02/2026 10:47:58.000) No Event Sampling ▾</p>				
Events	Patterns	Statistics (746)	Visualization	
Show: 20 Per Page ▾	✓ Format ▾	<input checked="" type="checkbox"/> Preview: On		◀ Prev 1 2 3 4 5 6 7 8 ... Next ▶
_time ▾	method ▾	uri ▾		status ▾
2025-08-11 10:16:44	GET	/6a4e8ed.html		404
2025-08-11 10:16:44	HEAD	/		200
2025-08-11 10:16:44	GET	/		200
2025-08-11 10:16:44	GET	/		200
2025-08-11 10:16:47	GET	/wp-cron.php		200
2025-08-11 10:16:47	HEAD	/emergency.php		404
2025-08-11 10:16:47	HEAD	/wp-content/uploads/dump.sql		404
2025-08-11 10:16:47	HEAD	/wp-content/uploads/tmm_db_migrate/tmm_db_migrate.zip		404
2025-08-11 10:16:47	GET	/wp-content/uploads/		403
2025-08-11 10:16:47	GET	/wp-login.php?registration=disabled		200
2025-08-11 10:16:47	GET	/wp-login.php?action=register		302
2025-08-11 10:16:47	GET	/wp-content/mu-plugins/		404
2025-08-11 10:16:47	GET	/wp-signup.php		302
2025-08-11 10:16:47	HEAD	/wp-content/backup-db/		404

Ostatnie także, jednak tu występuje metoda POST

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** index="task6" clientip="10.10.243.134" | sort -time
- Event Count:** 746 events (before 18/02/2026 10:45:07.0000)
- Sampling:** No Event Sampling
- Time Range:** All time
- Events (746):** The main pane displays a timeline of green bars representing event times. A specific event at 10:17:35 on Monday, August 11, 2025, is highlighted with a blue box.
- Fields:** The left sidebar lists selected fields: host, source, sourcetype, and interesting fields like date, file, and offset.
- Event List:** Below the timeline, a table lists the 8 selected events for the highlighted timestamp. Each event includes a timestamp, host, source, sourcetype, and a detailed log message.

Dodatkowo zaobserwowano próby dostępu do wielu innych endpointów, w tym liczne zapytania typu **HEAD**, co może świadczyć o rekonesansie aplikacji.

_time	method	url	status
2025-08-11 10:17:00	GET	/wp-config.php	200
2025-08-11 10:17:00	HEAD	/wp-config.php_____	404
2025-08-11 10:17:00	HEAD	/wp-config.php_	404
2025-08-11 10:17:00	HEAD	/wp-config.php__	404
2025-08-11 10:17:00	HEAD	/wp-config.php	200
2025-08-11 10:16:59	HEAD	/wp-config.orig	404
2025-08-11 10:16:59	HEAD	/wp-config.ORG	404
2025-08-11 10:16:59	HEAD	/wp-config.original	404
2025-08-11 10:16:59	HEAD	/wp-config.old	404
2025-08-11 10:16:59	HEAD	/wp-config.old.old	404
2025-08-11 10:16:59	HEAD	/wp-config.local.php	404
2025-08-11 10:16:59	HEAD	/wp-config.htm	404
2025-08-11 10:16:59	HEAD	/wp-config.html	404
2025-08-11 10:16:59	HEAD	/wp-config.inc	404
2025-08-11 10:16:59	HEAD	/wp-config.good	404
2025-08-11 10:16:59	HEAD	/wp-config.dump	404
2025-08-11 10:16:59	HEAD	/wp-config.conf	404
2025-08-11 10:16:59	HEAD	/wp-config.data	404
2025-08-11 10:16:59	HEAD	/wp-config.bak	404

Analiza sekwencji zdarzeń wykazała, że:

- pierwsze żądania były wykonywane z wykorzystaniem User-Agent WPScan,
  - brak było wcześniejszej fazy manualnego rekonesansu,
  - ostatnie żądania również pochodziły z WPScan i obejmowały metodę POST.
- Dodatkowo zaobserwowano próby dostępu do innych endpointów oraz liczne zapytania typu **HEAD**, co może wskazywać na automatyczne mapowanie zasobów aplikacji.

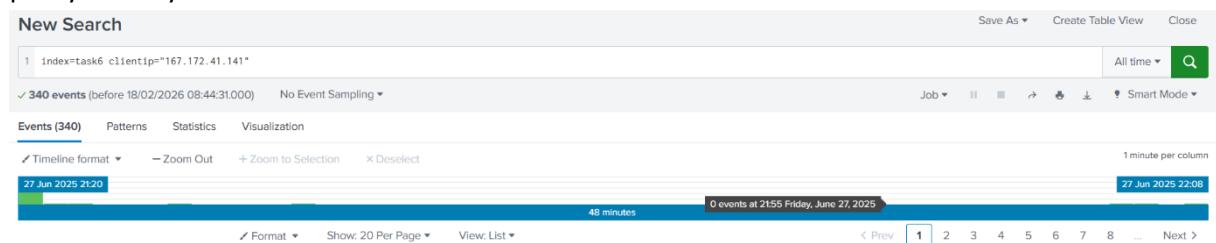
## 2. Adres IP: 167.172.41.141

- Drugi co do liczby wystąpień adres IP
- Endpoint: **/wp-login.php**
- User-Agent: **Hydra** (narzędzie do ataków brute-force)

Zaobserwowane metody:

- **GET** – 158 razy
- **POST** – 157 razy

Taki rozkład metod wskazuje na cykliczne pobieranie strony logowania oraz następujące po nim próby uwierzytelnienia.



Czas trwania komunikacji: **27 czerwca 2025 r., 21:20 - 22:07** (ok. 48 minut).

Pierwsze zarejestrowane zdarzenia były już realizowane przy użyciu narzędzia Hydra, bez widocznej wcześniejszej fazy rekonesansu manualnego.

The image contains two side-by-side screenshots of a Splunk search interface. Both screenshots show search results for the query "index=task6 clientip='167.172.41.141'".

**Screenshot 1 (Top):**

- Selected Fields:** index=task6, clientip=167.172.41.141, host=ce-splunk, source=access.log, sourcetype=access\_combined.
- Interesting Fields:** #bytes, #clientip, #date\_hour, #date\_mday, #date\_minute, #date\_month, #date\_second, #date\_wday.
- Event List:**
  - 27/06/2025 21:20:42.000: POST /wp-login.php HTTP/1.0. 200 5244 "-" "Mozilla/5.0 (Hydra)"
  - 27/06/2025 21:20:42.000: POST /wp-login.php HTTP/1.0. 200 5244 "-" "Mozilla/5.0 (Hydra)"
  - 27/06/2025 21:20:42.000: POST /wp-login.php HTTP/1.0. 200 5244 "-" "Mozilla/5.0 (Hydra)"
  - 27/06/2025 21:20:42.000: GET /wp-login.php HTTP/1.0. 200 4838 "-" "Mozilla/5.0 (Hydra)"

**Screenshot 2 (Bottom):**

- Selected Fields:** index=task6, clientip=167.172.41.141, host=ce-splunk, source=access.log, sourcetype=access\_combined.
- Interesting Fields:** #bytes, #clientip, #date\_hour, #date\_mday, #date\_minute, #date\_month, #date\_second, #date\_wday, #date\_year, #date\_zone.
- Event Actions:**

Type	Field	Value	Actions
Selected	host	ce-splunk	▼
	source	access.log	▼
	sourcetype	access_combined	▼
Event	bytes	595	▼
	clientip	167.172.41.141	▼
	file	admin-ajax.php	▼
	ident	-	▼
	method	POST	▼
	referer	http://demo-web.deceptitech.thm/wp-admin/theme-editor.php?file=404.php&theme=blocksy	▼
	referer_domain	http://demo-web.deceptitech.thm	▼

Ostatnie zaobserwowane zdarzenia mogą potencjalnie wskazywać na udane uwierzytelnienie, co znacząco podnosi ryzyko kompromitacji kont administracyjnych i wymaga dalszej weryfikacji na poziomie SOC L2.

Sprawdzenie reputacji adresu IP w bazie AbuseIPDB wskazuje na jego wcześniejsze powiązania z aktywnością o charakterze złośliwym, w tym atakami brute-force.

The screenshot shows the AbuseIPDB interface. At the top, it says "AbuseIPDB » 167.172.41.141". Below that is a search bar with placeholder text "Check an IP Address, Domain Name, Subnet, or ASN e.g. 127.0.0.1" and a "CHECK" button. The main content area displays the following information for IP 167.172.41.141:

ISP	DigitalOcean, LLC
Usage Type	Data Center/Web Hosting/Transit
ASN	AS14061
Domain Name	digitalocean.com
Country	Netherlands
City	Amsterdam, North Holland

Below this, there's a note: "This IP was reported 23 times. Confidence of Abuse is 20%". A "REPORT IP" button is at the bottom left, and a "WHOIS SEARCH" button is at the bottom right.

A small advertisement for OVNCLOUD is visible on the right side of the page.

Po przeprowadzonej analizie można stwierdzić, że jest to atak brute-force, wykonany z dwóch źródeł: 10.10.243.134 oraz 167.172.41.141.

## W SKRÓCIE:

- **Klasifikacja:** True Positive
- **Severity:** High
- **Potential Impact:** Critical
- **Decyzja:** Wymagana eskalacja

**KTO:** Niezidentyfikowani atakujący

**KIEDY:** 11.08.2025, 10:17:01–10:17:36

27.06.2025, 21:20:42 – 22:07:18

**SKĄD:** 10.10.243.134, 167.172.41.141

**CZYM:** WPScan, Hydra (narzędzia do brute-force / recon)

Analiza zakończona na etapie triage incydentu SOC L1. Zdarzenie zostało sklasyfikowane jako True Positive o wysokiej krytyczności. Ze względu na charakter ataku oraz ryzyko kompromitacji kont administracyjnych incydent WYMAGA DALSZEJ ANALIZY NA POZIOMIE SOC L2.

Rekomendacje:

- Blokada adresów IP na WAF / firewall,
- reset haseł kont uprzywilejowanych,
- weryfikacja logów uwierzytelnienia aplikacji WordPress,
- monitoring /wp-login.php z progiem alertowym.

ŽRÓDŁO: <https://tryhackme.com/room/loganalysiswithsiem>