Brute force Analysis

CEL

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

ZASOBY

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

Practice Scenario

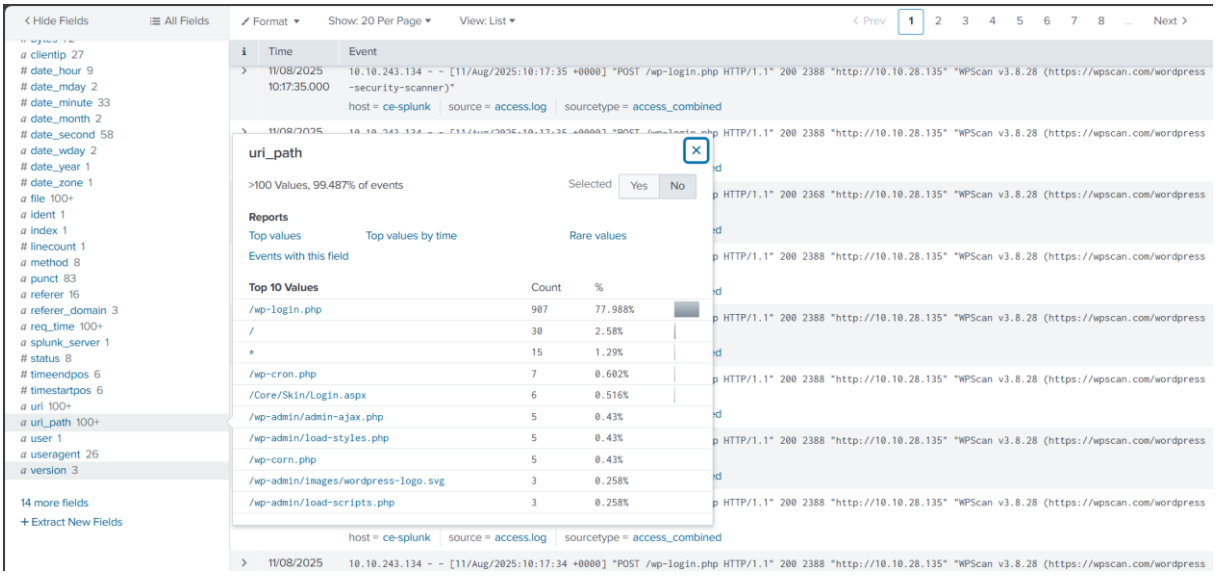
You are an SOC Level 1 Analyst on shift and have received an alert indicating a spike in activity on the organisation's web server.
Your task is to dive into the logs and determine exactly what happened.

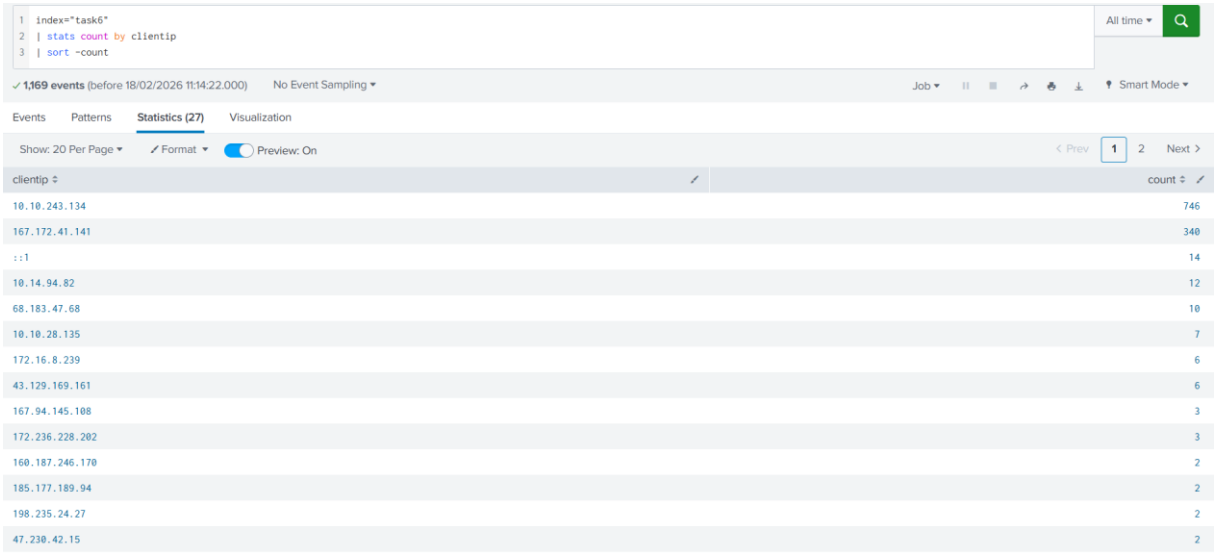
The logs for this task are located in the Splunk index task6. Use the following query: `index=task6`

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**.





```
index="task6"
| stats count by clientip
| sort -count
```

All time

✓ 1,169 events (before 18/02/2026 11:14:22.000) No Event Sampling

Job Smart Mode

Events Patterns Statistics (27) Visualization

Show: 20 Per Page Format Preview: On

< Prev 1 2 Next >

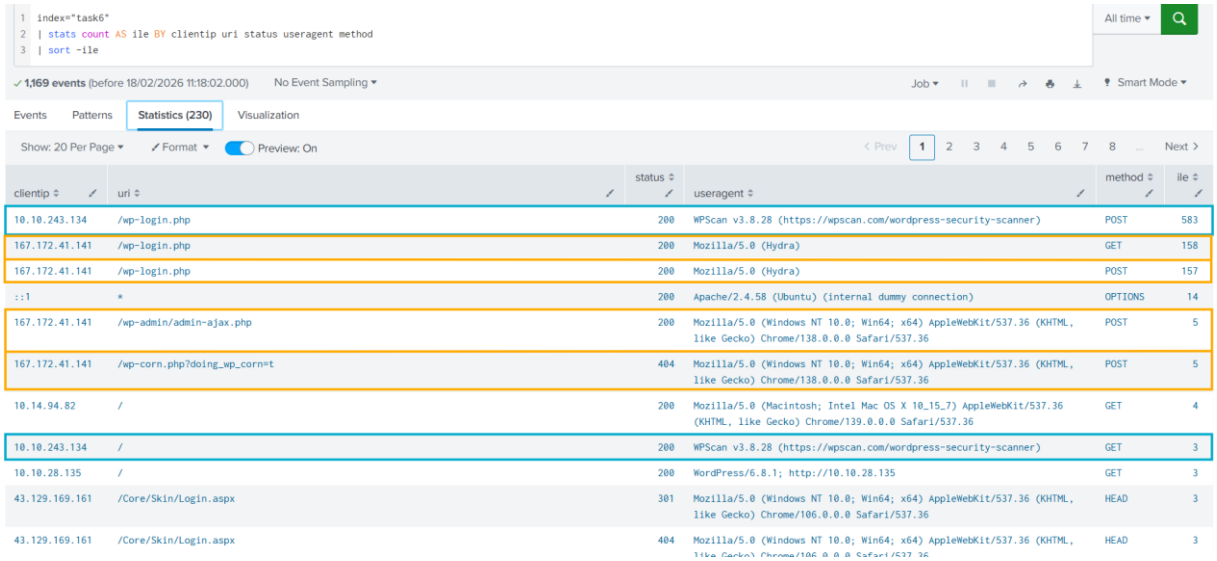
clientip	count
10.10.243.134	746
167.172.41.141	340
::1	14
10.14.94.82	12
68.183.47.68	10
10.10.28.135	7
172.16.8.239	6
43.129.169.161	6
167.94.145.108	3
172.236.228.202	3
160.187.246.170	2
185.177.189.94	2
198.235.24.27	2
47.230.42.15	2

W pierwszym kroku przeanalizowano liczbę zapytań do wskazanego URI w podziale na adresy IP. Dwie wartości — **746 oraz 340 zapytań** — znacząco 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).



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

All time

✓ 1,169 events (before 18/02/2026 11:18:02.000) No Event Sampling

Job Smart Mode

Events Patterns Statistics (230) Visualization

Show: 20 Per Page Format Preview: On

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

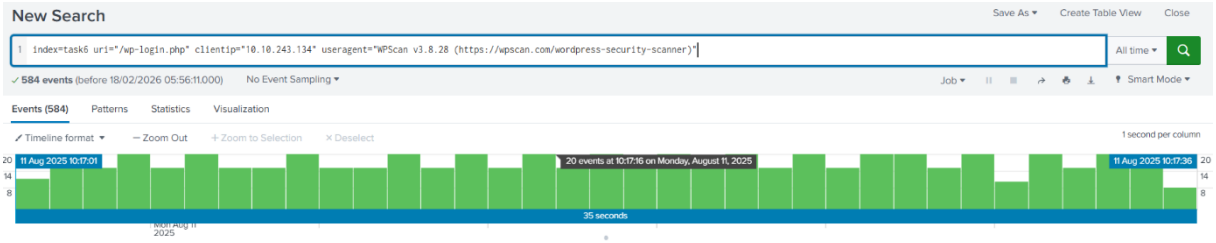
clientip	uri	status	useragent	method	ile
10.10.243.134	/wp-login.php	200	WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)	POST	583
167.172.41.141	/wp-login.php	200	Mozilla/5.0 (Hydra)	GET	158
167.172.41.141	/wp-login.php	200	Mozilla/5.0 (Hydra)	POST	157
::1	*	200	Apache/2.4.58 (Ubuntu) (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-corn.php?doing_wp_corn=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,	HEAD	3

WNIOSKI Z ANALIZY

1. Adres IP: 10.10.243.134

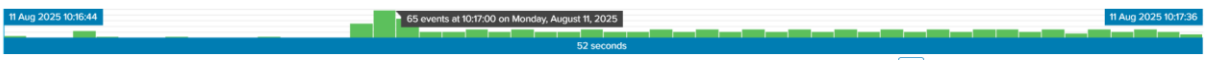
- Największa liczba zapytań (583) dotyczyła endpointu **/wp-login.php**
- Metoda: **POST**
- User-Agent: **WPScan** (narzędzie do skanowania WordPressa)

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

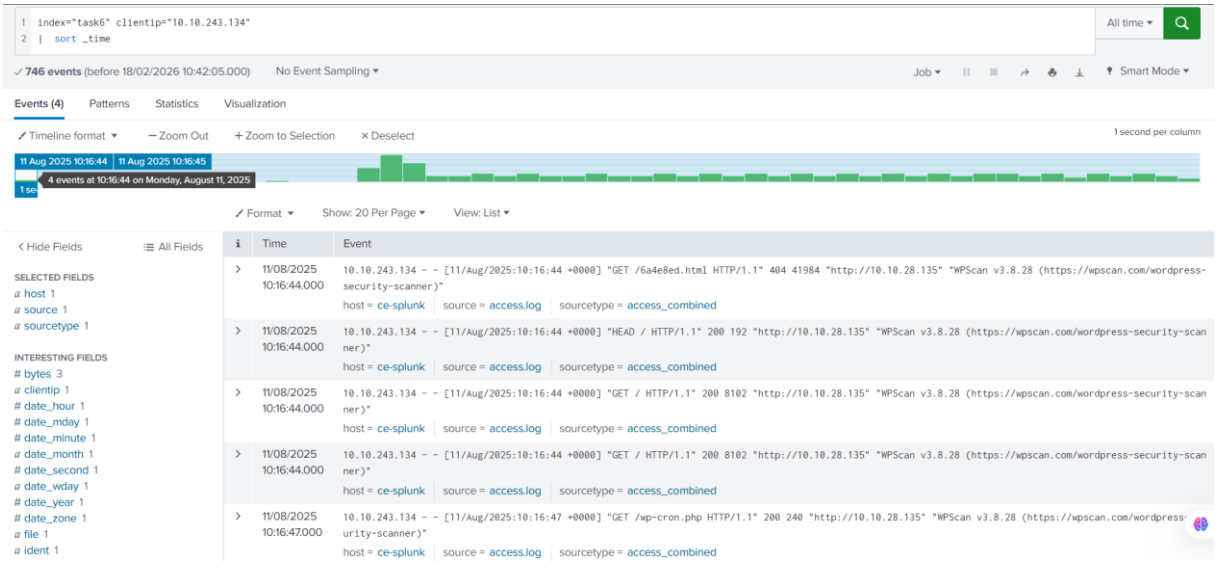


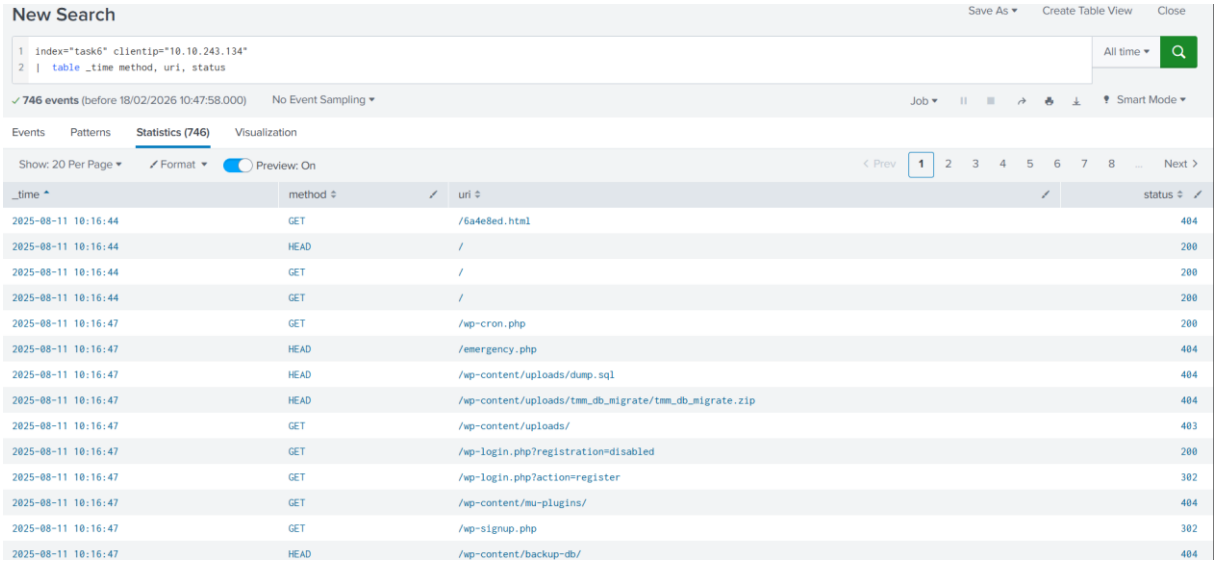
Czas trwania incydentu:
11 sierpnia 2025 r., **10:17:01 - 10:17:36** (ok. 35 sekund)

Timeline żądań:

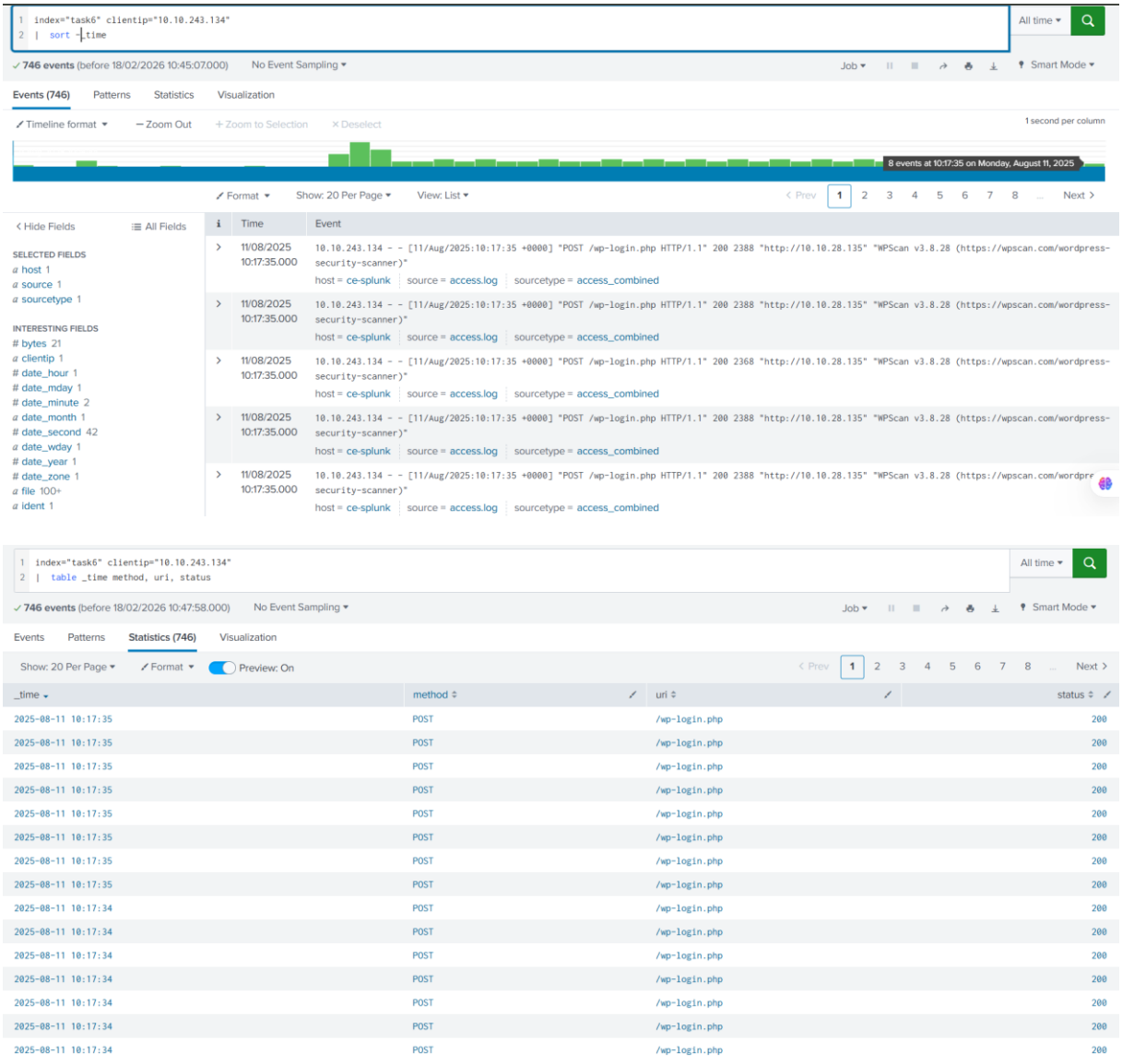


Pierwsze zapytania już były wykonywane poprzez User-agent WPScan – brak wcześniejszego rekonesansu.





Ostatnie także, jednak tu występuje metoda POST



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

_time	method	uri	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.

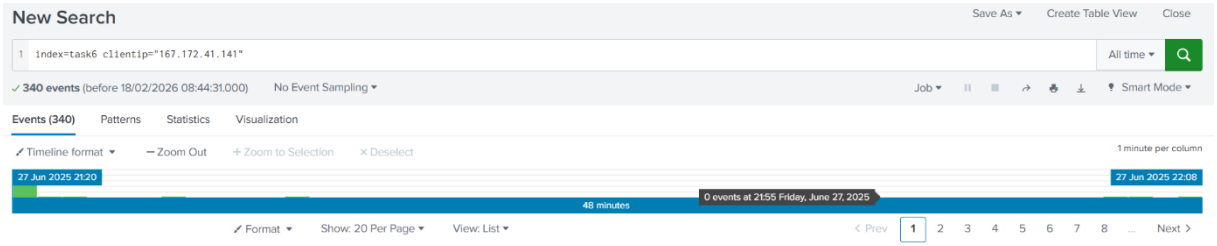
2. Adres IP: 167.172.41.141

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

Zaobserwowane metody:

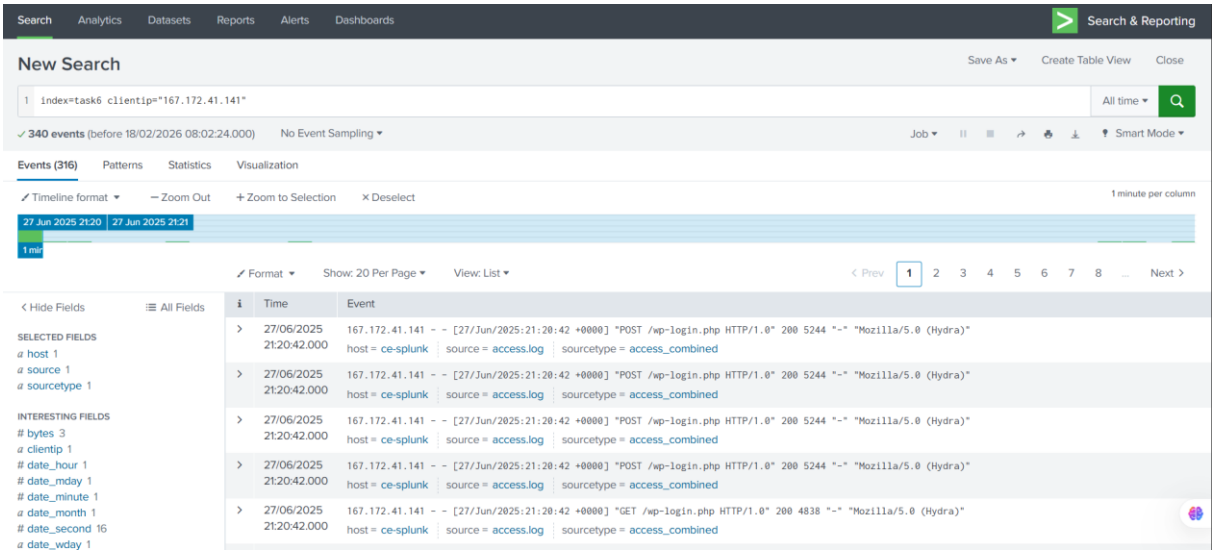
- **GET** – 158 razy
- **POST** – 157 razy

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).

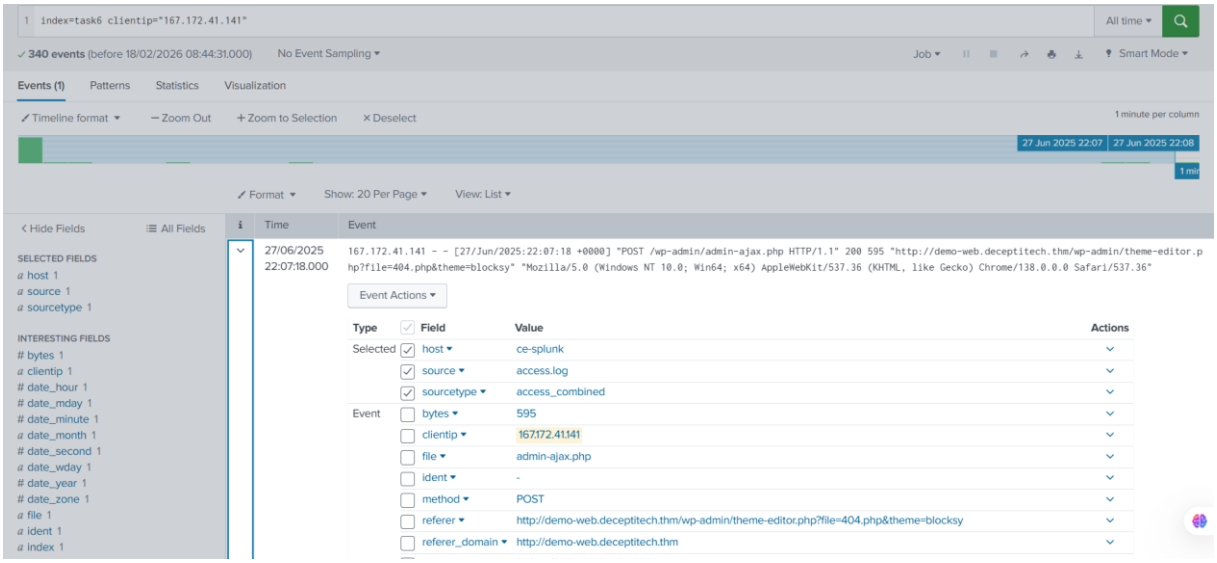
Pierwsze zarejestrowane zdarzenia były już realizowane przy użyciu narzędzia Hydra, bez widocznej wcześniejszej fazy rekonesansu manualnego.



```
index=task6 clientip="167.172.41.141"
```

✓ 340 events (before 18/02/2026 08:02:24.000)

```
27/06/2025 21:20:42.000  167.172.41.141 - - [27/Jun/2025:21:20:42 +0000] "POST /wp-login.php HTTP/1.0" 200 5244 "-" "Mozilla/5.0 (Hydra)"
                         host = ce-splunk   source = access.log   sourcetype = access_combined
27/06/2025 21:20:42.000  167.172.41.141 - - [27/Jun/2025:21:20:42 +0000] "POST /wp-login.php HTTP/1.0" 200 5244 "-" "Mozilla/5.0 (Hydra)"
                         host = ce-splunk   source = access.log   sourcetype = access_combined
27/06/2025 21:20:42.000  167.172.41.141 - - [27/Jun/2025:21:20:42 +0000] "POST /wp-login.php HTTP/1.0" 200 5244 "-" "Mozilla/5.0 (Hydra)"
                         host = ce-splunk   source = access.log   sourcetype = access_combined
27/06/2025 21:20:42.000  167.172.41.141 - - [27/Jun/2025:21:20:42 +0000] "POST /wp-login.php HTTP/1.0" 200 5244 "-" "Mozilla/5.0 (Hydra)"
                         host = ce-splunk   source = access.log   sourcetype = access_combined
27/06/2025 21:20:42.000  167.172.41.141 - - [27/Jun/2025:21:20:42 +0000] "GET /wp-login.php HTTP/1.0" 200 4838 "-" "Mozilla/5.0 (Hydra)"
                         host = ce-splunk   source = access.log   sourcetype = access_combined
```



```
index=task6 clientip="167.172.41.141"
```

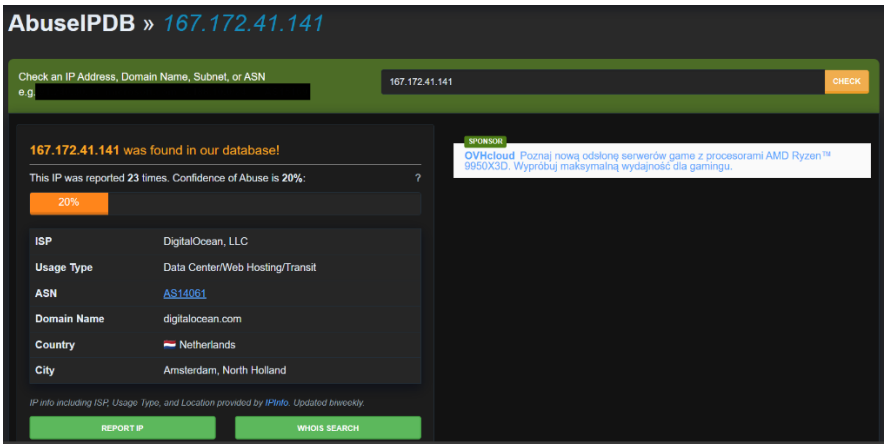
✓ 340 events (before 18/02/2026 08:44:31.000)

```
27/06/2025 22:07:18.000  167.172.41.141 - - [27/Jun/2025:22:07:18 +0000] "POST /wp-admin/admin-ajax.php HTTP/1.1" 200 595 "http://demo-web.deceptitech.thm/wp-admin/theme-editor.p
                         hp?file=404.php&theme=blocksy" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36"
```

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.



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

W SKRÓCIE:

- **Klasyfikacja:** 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.

ŻRÓDŁO: https://tryhackme.com/room/loganalysiswithsiem