Incident Report: Suspicious activity in Web Server

Incident ID: IR-2025-004

Attack Type: Bruteforce - TryHackme

Date: Dec 21, 2025

Analyst: BALA KOTESWARA REDDY REDDYMALLI

Severity: High

Status: Closed - True Positive

1. Executive Summary

A Brute force attack against the WordPress admin login page was detected. The attacker performed the Bruteforce by using Hydra from an external IP 167.172.41.141 and has successfully compromised the account.

2. Scenario Context

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.

Environment	Details
Target System	Web Server

3. Incident Timeline

Time	Event Description
27/06/2025 21:20:27	Attacker started the Bruteforce attack against /wp-login.php
27/06/2025 21:20:42	BruteForce Attack successful and wordpress admin account compromised. 302 Login Redirection Detected.

4. Investigation Methodology

My Approach:

1. Begin by analyzing common indicators such as User Agents, HTTP Methods, and URI Paths ("low-hanging fruit").
2. Generate count statistics for the web traffic, grouping the data by HTTP method and URI path to identify anomalies
3. Trace the suspicious web requests by grouping them based on the client IP that generated a high count of requests to specific URI paths(Obtained in previous step).
4. Conduct a detailed investigation associated with suspicious user agents.
5. Determine if the attack was successful by examining web server status codes(302 Redirection)
6. Extracted IOCs for threat hunting

5. Technical Analysis

Detection queries(SPL):

Displays all user agents involved:

```
index="task6"
| dedup useragent
| table useragent
```

Count statistics of web traffic, grouping by http method and uri_path:

```
index=task6 status=200
| stats count by method,uri_path
| sort -count
```

Count statistics of web requests grouping them based on client ip for specific uri_path:

```
index=task6 method=POST uri_path="/wp-login.php"
| stats values(referer_domain) as referer_domain values(status) as status values(useragent) as UserAgent values(uri_path) as uri_path values(method) as method count by clientip
| table referer_domain clientip UserAgent uri_path count method status
```

Detailed Investigation of events by individual suspicious user agents:

```
index=task6 method=POST uri_path="/wp-login.php" useragent=*Hydra*

index=task6 method=POST uri_path="/wp-login.php" useragent=*Hydra*
| stats values(bytes) as bytes values(clientip) as clientip values(status) as status count by useragent
| table useragent clientip status bytes count

index=task6 method=POST uri_path="/wp-login.php" useragent=*WPscan*

index=task6 method=POST uri_path="/wp-login.php" useragent=*WPscan*
| stats values(bytes) as bytes values(clientip) as clientip values(status) as status count by useragent
| table useragent clientip status bytes count
```

Determining if attack was successful:
index=task6 method=POST uri_path="/wp-login.php" status!=200

Key Findings:

- Multiple suspicious User agents found(Hydra,WPscan,curl,python scripts)
- Higher number of Post request are found to be sent to uri path named “/wp-login.php”
- Bruteforce Attack observed against wordpress admin login using Hydra.
- The Bruteforce attack is successfully completed.(Based on 302 Redirection)

6. Indicators of Compromise (IOCs)

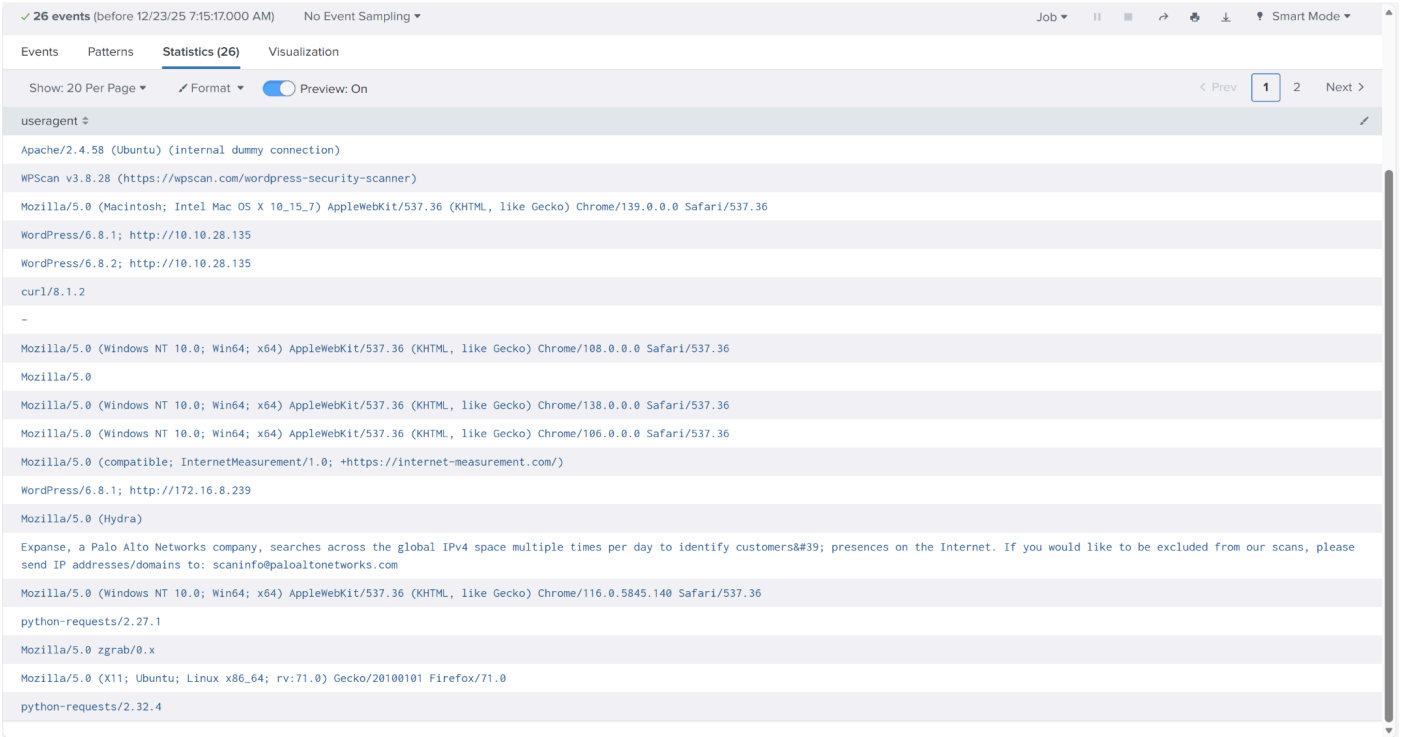
Indicator Type	Value	Context
IP Address	167.172.41.141	Attacker IP
Tool	Hydra	Password Bruteforce
Target URI Path	/wp-login.php	Wordpress admin login page

7. MITRE ATT&CK Mapping

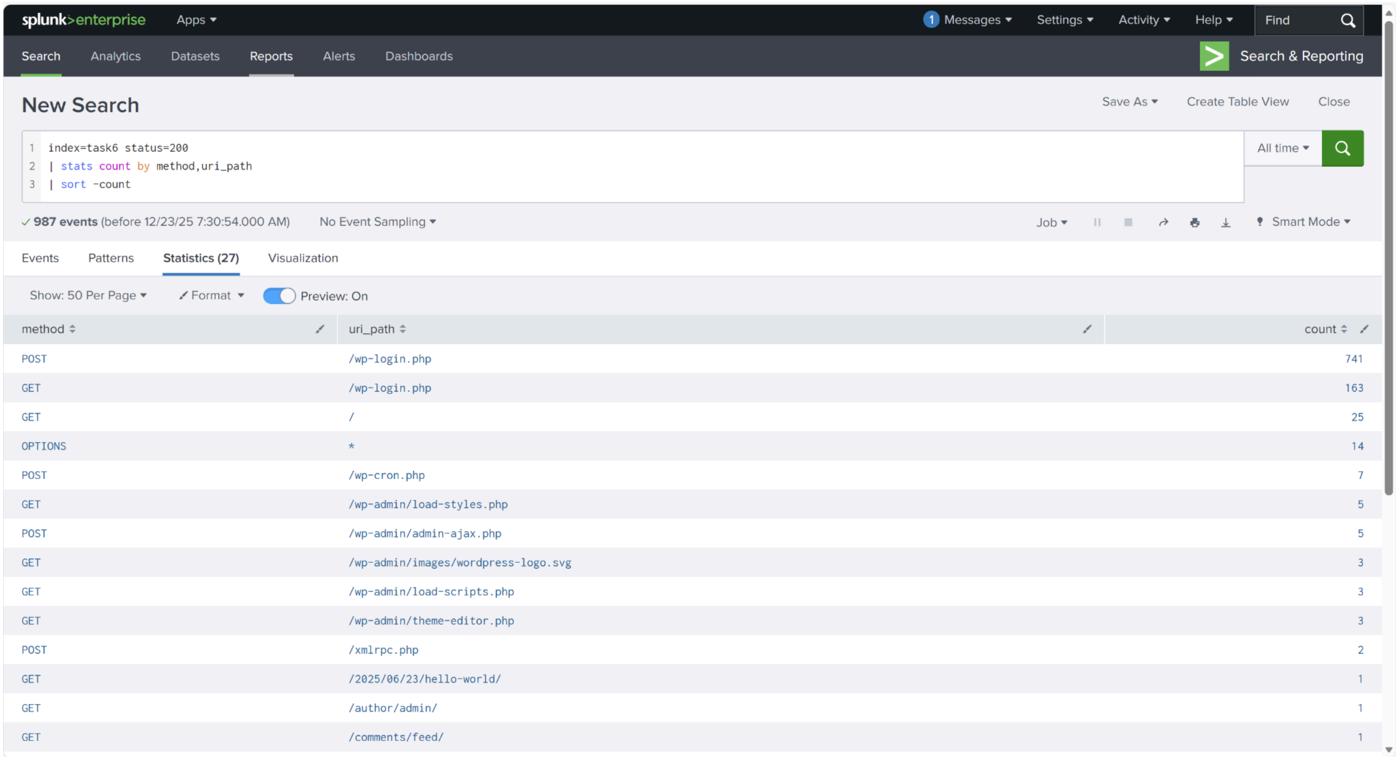
- **T1110 (Bruteforce):** The attacker used Hydra to systematically guess passwords
- **T1588 (Obtain Capabilities):** The attacker utilized Hydra, a known credential cracking tool, for the attack.

8. Evidence Screenshots

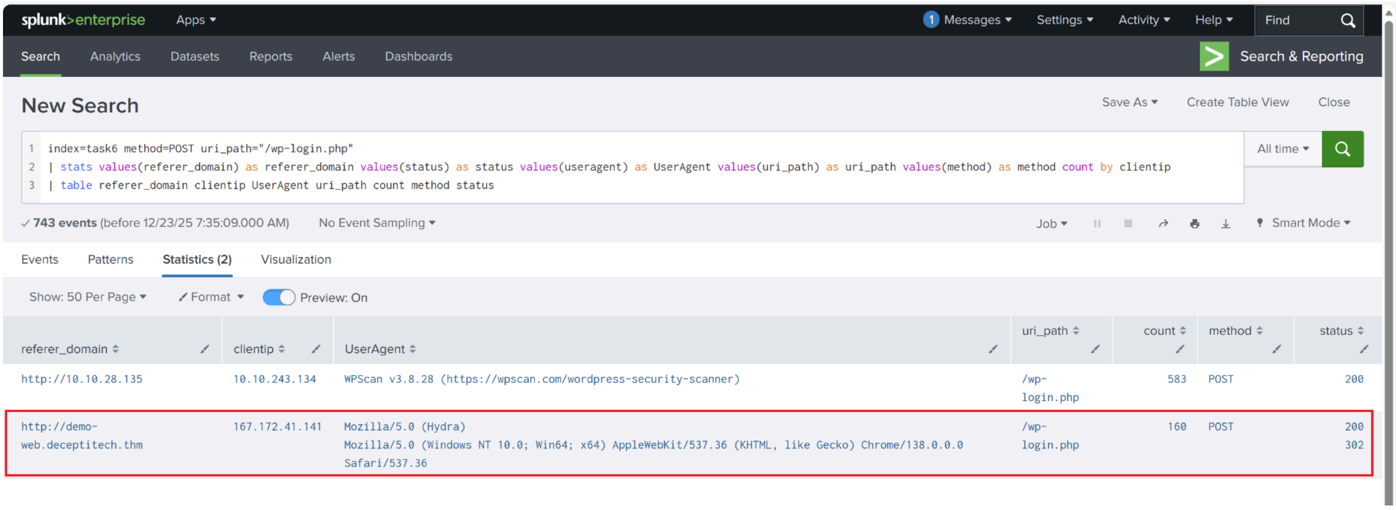
Splunk Query showing list of user agents:



Splunk Query showing Count stats grouping by http method and uripath:

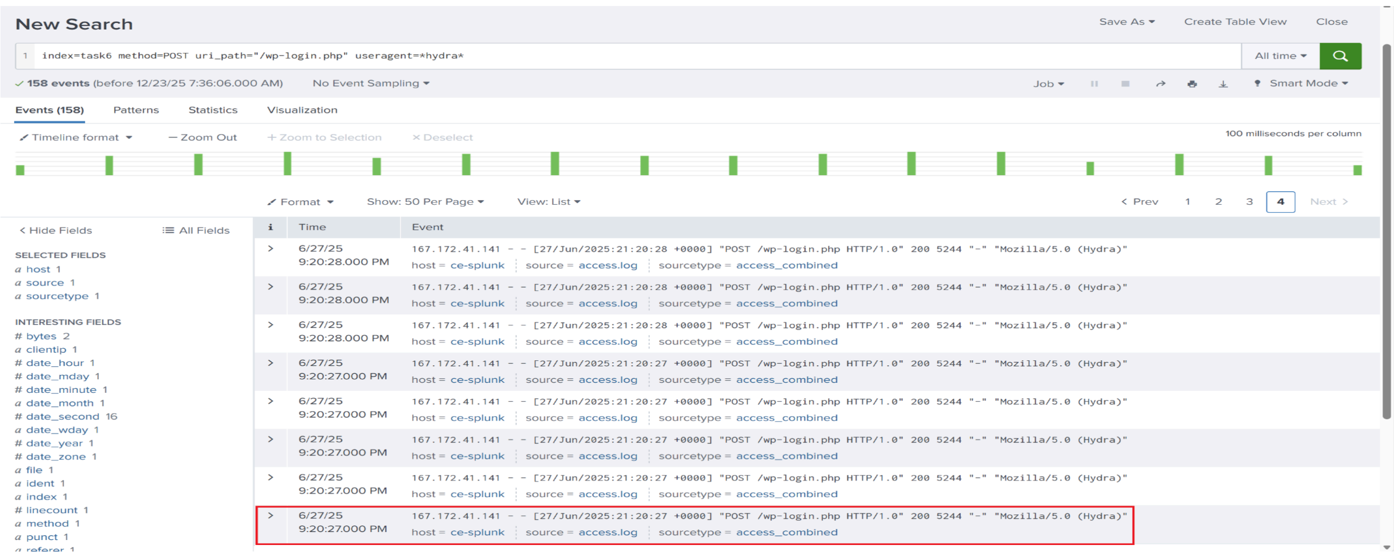


Splunk Query showing Count stats grouping by clientip:

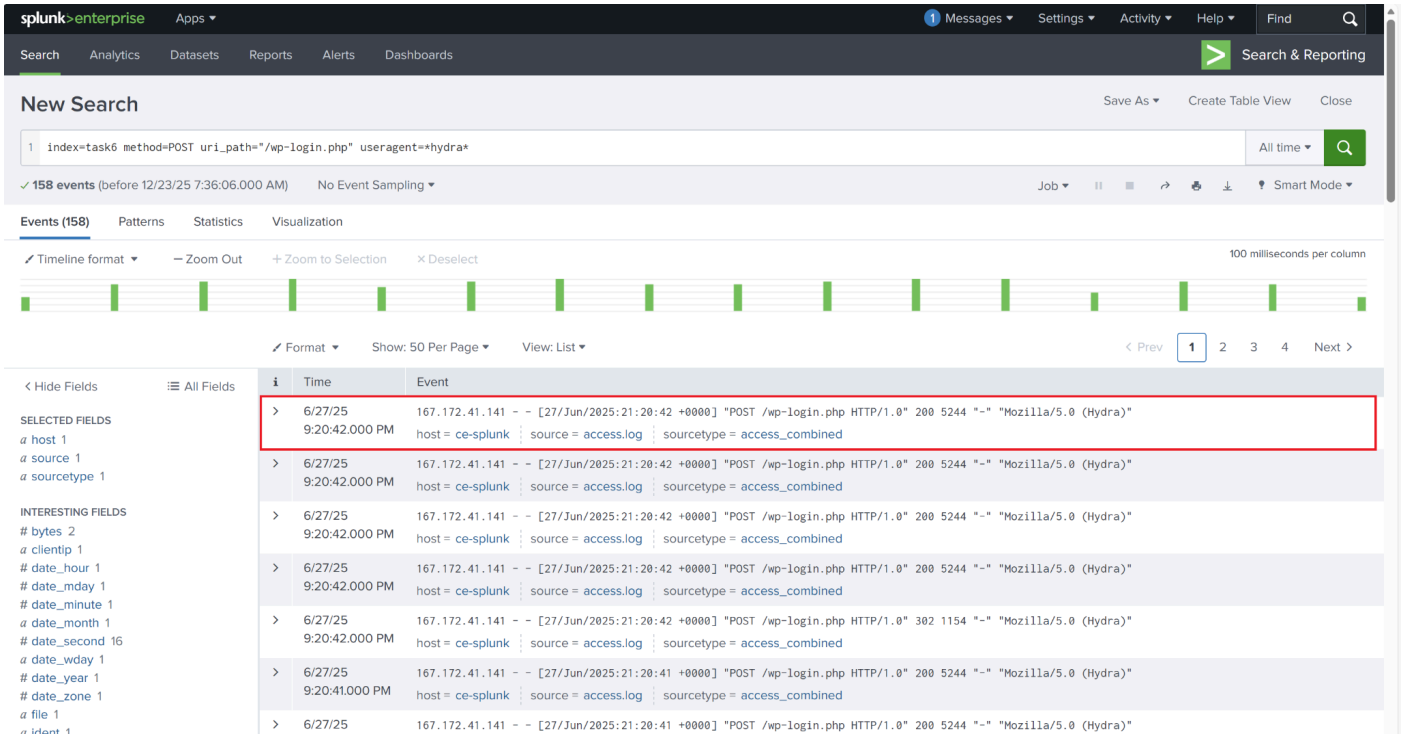


Splunk Query showing Bruteforce Events:

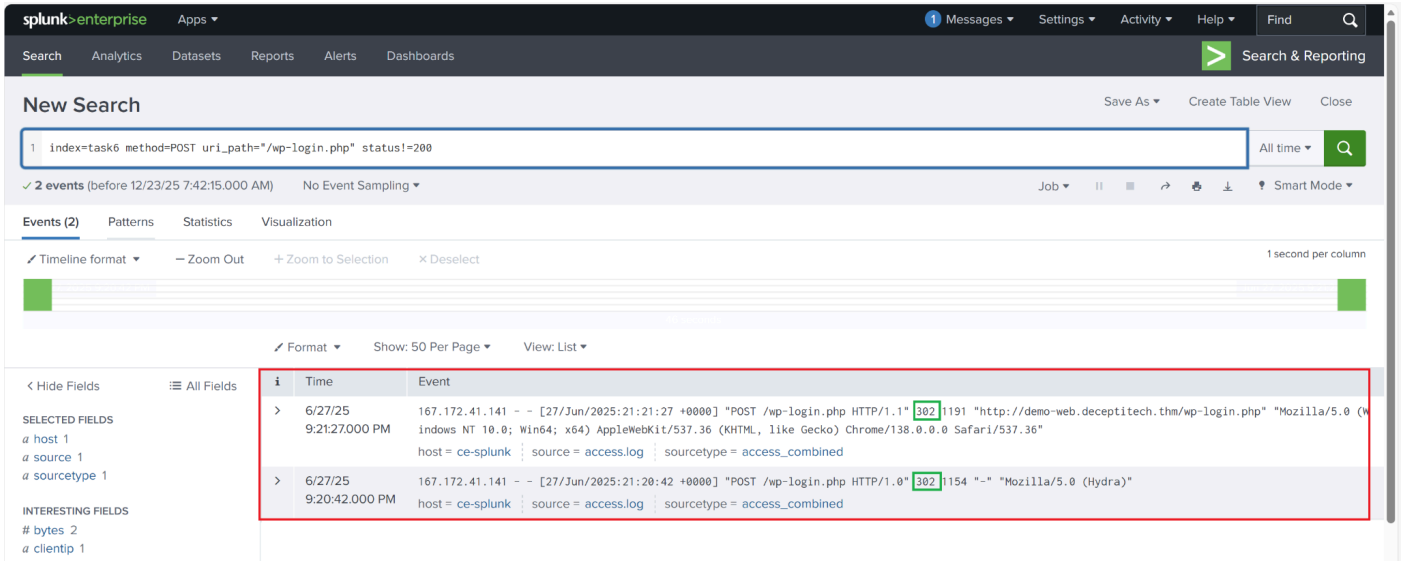
Start Event:



End Event:



Splunk Query determining whether the brute force is successful or not:



8. Recommendations & Remediation

- Isolate Machine from network
- Reset wordpress account credentials
- Block the IP 162.172.41.141 in the firewall.