

Tier 3.2

Hướng tiếp cận của nhóm tập trung vào phát hiện các event brute-force có vẻ bất thường trong các response trả về.

Sau khi query các event thực hiện brute-force bằng các qua giao thức POST đến /:

index=* "POST / HTTP/1.1"

✓ 1,105,961 events (12/4/24 12:00:00.000 AM to 1/3/25 9:11:36.000 PM) No Event Sampling ▼

Events (1,105,961) Patterns Statistics Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection x Deselect

List ▼ Format 20 Per Page ▼

< Hide Fields	≡ All Fields	i	Time	Event
SELECTED FIELDS a host 1 a source 1 a sourcetype 1 INTERESTING FIELDS # bytes 5 a clientip 1 # date_hour 7 # date_offset 4		>	12/14/24 9:07:23.000 PM	192.168.184.128 - - [14/Dec/2024:21:07:23 +0700] "POST / HTTP/1.1" 302 757 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 host = appserver source = /var/log/apache2/access.log sourcetype = access_combined
		>	12/14/24 9:07:23.000 PM	192.168.184.128 - - [14/Dec/2024:21:07:23 +0700] "POST / HTTP/1.1" 302 757 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 host = appserver source = /var/log/apache2/access.log sourcetype = access_combined
		>	12/14/24 9:07:23.000 PM	192.168.184.128 - - [14/Dec/2024:21:07:23 +0700] "POST / HTTP/1.1" 302 757 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 host = appserver source = /var/log/apache2/access.log sourcetype = access_combined

Nhận thấy rằng hầu hết các event đều có trường bytes (kích thước response) là 757. Tiến hành lọc trường này:

New Search

index=* "POST / HTTP/1.1" bytes!=757

✓ 45 events (12/4/24 12:00:00.000 AM to 1/3/25 9:21:39.000 PM) No Event Sampling ▼

Events (45) Patterns Statistics Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection x Deselect

List ▼ Format 20 Per Page ▼

< Hide Fields	≡ All Fields	i	Time	Event
SELECTED FIELDS a host 1 a source 1 a sourcetype 1 INTERESTING FIELDS # bytes 4		>	12/14/24 4:57:58.000 PM	192.168.184.128 - - [14/Dec/2024:16:57:58 +0700] "POST / HTTP/1.1" 302 815 "http://citydiamond.shop/ke-gecko.com/" Chrome/104.0.5112.81 Safari/537.36 host = appserver source = /var/log/apache2/access.log sourcetype = access_combined
		>	12/14/24 4:57:58.000 PM	192.168.184.128 - - [14/Dec/2024:16:57:58 +0700] "POST / HTTP/1.1" 302 815 "http://citydiamond.shop/ke-gecko.com/" Chrome/104.0.5112.81 Safari/537.36 host = appserver source = /var/log/apache2/access.log sourcetype = access_combined

Lần này ta lại thấy hàng loạt các event có bytes 815. Lọc các event này:

New Search

Save As Create Table View Close

Last 30 days

Q

5 events (12/4/24 12:00:00.000 AM to 1/3/25 9:23:07.000 PM)

No Event Sampling

Job

Smart Mode

Events (5)

Patterns

Statistics

Visualization

Format Timeline

Zoom Out

Zoom to Selection

Deselect

1 day per column

List

Format

20 Per Page

< Hide Fields

All Fields

SELECTED FIELDS

host 1

source 1

sourcetype 1

INTERESTING FIELDS

bytes 3

clientip 1

date_hour 2

date_mday 1

date_minute 3

date_month 1

date_second 5

date_wday 1

date_year 1

date_zone 1

ident 1

index 1

linecount 1

i	Time	Event
>	12/14/24 4:57:13.000 PM	192.168.184.128 - - [14/Dec/2024:16:57:13 +0700] "POST / HTTP/1.1" 200 530 "http://citydiamond.shop/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.81 Safari/537.36" host = appserver source = /var/log/apache2/access.log sourcetype = access_combined
>	12/14/24 4:57:11.000 PM	192.168.184.128 - - [14/Dec/2024:16:57:11 +0700] "POST / HTTP/1.1" 200 530 "http://citydiamond.shop/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.81 Safari/537.36" host = appserver source = /var/log/apache2/access.log sourcetype = access_combined
>	12/14/24 4:31:02.000 PM	192.168.184.128 - - [14/Dec/2024:16:31:02 +0700] "POST / HTTP/1.1" 302 763 "http://citydiamond.shop/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36" host = appserver source = /var/log/apache2/access.log sourcetype = access_combined
>	12/14/24 3:52:59.000 PM	192.168.184.128 - - [14/Dec/2024:15:52:59 +0700] "POST / HTTP/1.1" 200 530 "http://citydiamond.shop/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.81 Safari/537.36" host = appserver source = /var/log/apache2/access.log sourcetype = access_combined
>	12/14/24 3:52:56.000 PM	192.168.184.128 - - [14/Dec/2024:15:52:56 +0700] "POST / HTTP/1.1" 200 567 "http://citydiamond.shop/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.81 Safari/537.36" host = appserver source = /var/log/apache2/access.log sourcetype = access_combined

Lúc này ta chỉ cần tập trung chỉ yếu vào 5 event trên. Đặc biệt ở event thứ 3 có mã trả về khác với các event còn lại. Ngoài ra để dễ tìm kiếm bên trong file pcap ta nhận thấy chỉ có request này có user-agent Linux.

Sau khi tra cứu chỉ có duy nhất 1 lệnh POST có user-agent có “Linux”:

No.	Time	Source	Destination	Protocol	Length	Value	User-Agent	Info
4948662	3718.145	192.168.184.128	192.168.184.132	HTTP	741	adm.capricorn2	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.81 Safari/537.36	POST / HTTP/1.1 (application/x-www-form-urlencoded)

Có username và password tiến hành hash bằng MD5:

Recipe

MD5

^

📁

🗑️

^

🚫

⏸️

Input

adm/capricorn2

ABC 14

1

Output

09445bfda055fe89696c0cef183d2d96