

Progetto Fine M6

Importate su Splunk i dati di esempio “tutorialdata.zip”:

- Crea una query Splunk per identificare tutti i tentativi di accesso falliti "Failed password". La query dovrebbe mostrare il timestamp, l'indirizzo IP di origine, il nome utente e il motivo del fallimento.
- Scrivi una query Splunk per trovare tutte le sessioni SSH aperte con successo. La query dovrebbe filtrare per l'utente “djohnson” e mostrare il timestamp e l'ID utente.
- Scrivi una query Splunk per trovare tutti i tentativi di accesso falliti provenienti dall'indirizzo IP “86.212.199.60”. La query dovrebbe mostrare il timestamp, il nome utente e il numero di porta.
- Crea una query Splunk per identificare gli indirizzi IP che hanno tentato di accedere ("Failed password") al sistema più di 5 volte. La query dovrebbe mostrare l'indirizzo IP e il numero di tentativi.
- Crea una query Splunk per trovare tutti gli Internal Server Error.

Trarre delle conclusioni sui log analizzati utilizzando AI.

1 . Query Splunk per identificare tutti i tentativi di accesso falliti "Failed password". La query dovrebbe mostrare il timestamp, l'indirizzo IP di origine, il nome utente e il motivo del fallimento.

source="tutorialdata.zip:*" host="HOST" "Failed password" |table _time src_ip user reason

splunk>enterpriseApps

AdministratorMessagesSettingsActivityHelpFind

SearchAnalyticsDatasetsReportsAlertsDashboards

New SearchSave AsCreate Table ViewClose

source="tutorialdata.zip:*" host="HOST" "Failed password" |table _time src_ip user reasonAll time

133,012 events (before 04/11/2024 01:28:21.000)No Event SamplingJobFormatPreviewSmart Mode

EventsPatternsStatistics (133,012)Visualization

20 Per PageFormatPreview

12345678Next

_time	src_ip	user	reason
2024-11-01 16:36:51	27.1.11.11	zabbix	invalid user
2024-11-01 16:36:51		root	
2024-11-01 16:36:51	27.1.11.11	whois	invalid user
2024-11-01 16:36:51	27.1.11.11	jabber	invalid user
2024-11-01 16:36:51		games	
2024-11-01 16:36:51	27.1.11.11	db	invalid user
2024-11-01 16:36:51		squid	
2024-11-01 16:36:51	27.1.11.11	itm2user	invalid user
2024-11-01 16:36:51	27.1.11.11	local	invalid user
2024-11-01 16:36:51	27.1.11.11	info	invalid user
2024-11-01 16:36:51	27.1.11.11	appserver	invalid user
2024-11-01 16:36:51	92.46.53.223	system	invalid user
2024-11-01 16:36:51	92.46.53.223	dasusr1	invalid user
2024-11-01 16:36:51	92.46.53.223	operator	invalid user
2024-11-01 16:36:51	92.46.53.223	postgres	invalid user
2024-11-01 16:36:51	92.46.53.223	sys	invalid user

12°C Nuvole sparse

Search

ENG IT01:2804/11/2024

2. Query Splunk per trovare tutte le sessioni SSH aperte con successo. La query dovrebbe filtrare per l'utente "djohnson" e mostrare il timestamp e l'ID utente

source="tutorialdata.zip:*" "Accepted password" user=djohnson | table _time user

Corso Cyber Security & Ethical hacking
 Studente: Adjetey Isabelle

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

New Search

source=tutorialdata.zip:* "Accepted password" user=djohnson | table _time user All time

✓ 60 events (before 04/11/2024 01:56:54.000) Sampling 1 : 100 Job Format Smart Mode

Events Patterns **Statistics (60)** Visualization

100 Per Page ✓ Format Preview

_time ↕	user ↕
2024-10-31 16:36:55	djohnson
2024-10-30 16:36:55	djohnson
2024-10-27 16:36:55	djohnson
2024-10-26 16:36:55	djohnson
2024-10-26 16:36:55	djohnson
2024-10-26 16:36:55	djohnson
2024-10-28 16:36:52	djohnson
2024-10-29 16:36:51	djohnson
2024-10-25 16:36:51	djohnson
2024-11-01 16:36:55	djohnson
2024-10-28 16:36:54	djohnson
2024-10-27 16:36:54	djohnson

3. Query Splunk per trovare tutti i tentativi di accesso falliti provenienti dall'indirizzo IP "86.212.199.60". La query dovrebbe mostrare il timestamp, il nome utente e il numero di porta.

```
source="tutorialdata.zip:*" host="HOST" "Failed password" src_ip=86.212.199.60 | table
_time user port
```

splunk

enterprise

Apps

Administrator

Messages

Settings

Activity

Help

Find

Search

Analytics

Datasets

Reports

Alerts

Dashboards

New Search

Save As

Create Table View

Close

source=tutorialdata.zip:* host=HOST* *Failed password* src_ip=86.212.199.60 | table _time user port

All time

6 events (before 04/11/2024 01:55:16.000)

Sampling 1: 100

Job

Smart Mode

Events

Patterns

Statistics (6)

Visualization

100 Per Page

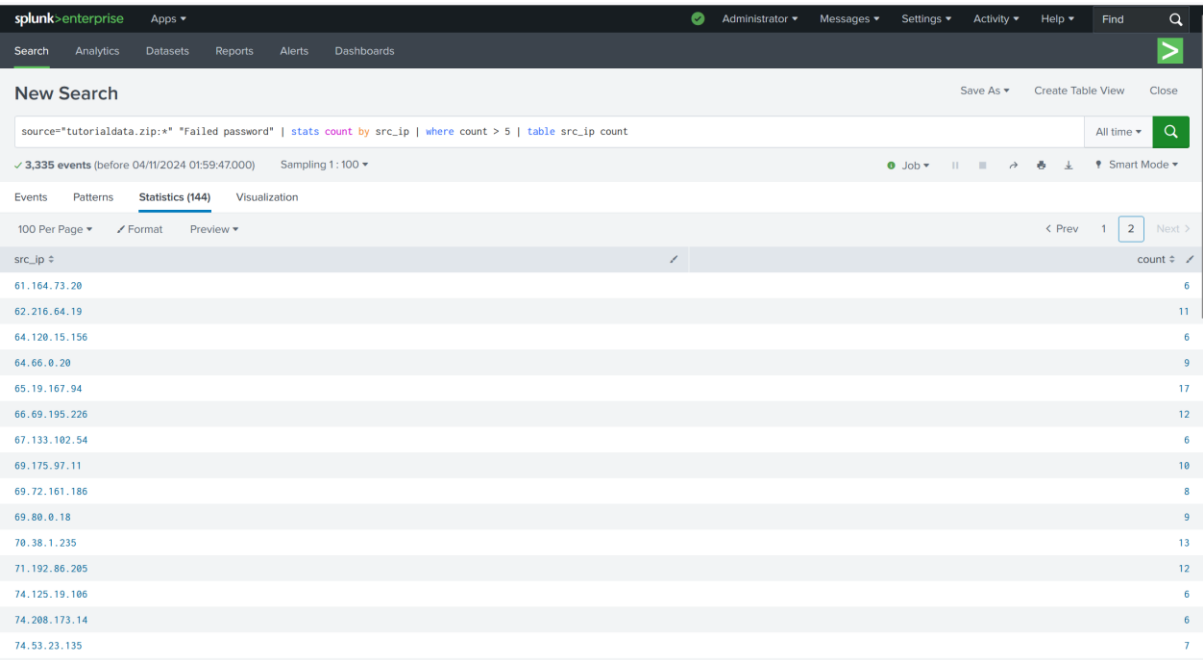
Format

Preview

_time	user	port
2024-10-25 16:36:55	info	4078
2024-10-31 16:36:52	admin	3673
2024-10-29 16:36:55	divine	2857
2024-10-25 16:36:55	desktop	2905
2024-10-30 16:36:54	whois	4566
2024-11-01 16:36:55	agushto	3692

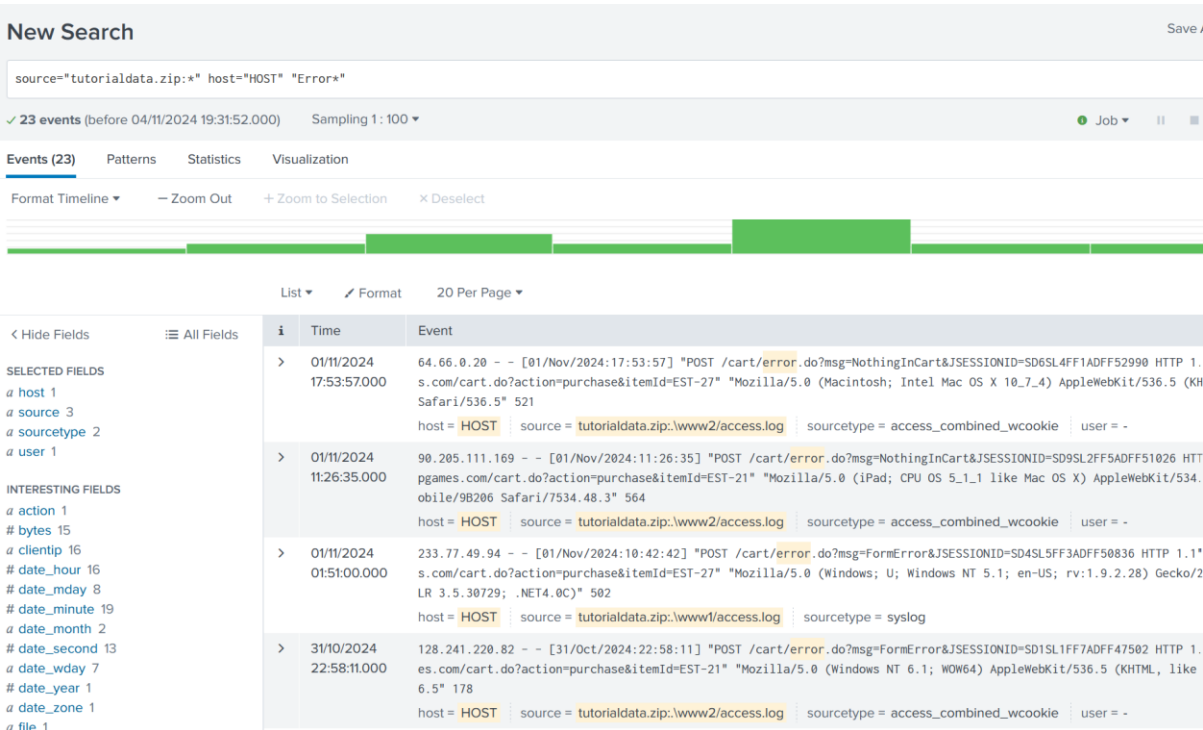
4. Query Splunk per identificare gli indirizzi IP che hanno tentato di accedere ("Failed password") al sistema più di 5 volte. La query dovrebbe mostrare l'indirizzo IP e il numero di tentativi.

```
source="tutorialdata.zip:*" "Failed password" | stats count by src_ip | where count > 5 |
table src_ip count
```



5. Query Splunk per trovare tutti gli Internal Server Error

`source="tutorialdata.zip:*" host="HOST" "Error*"`



Conclusioni sui log analizzati

Dall'analisi dei log, possiamo trarre diverse conclusioni:

- **Tentativi di Accesso Falliti:** La presenza di numerosi tentativi di accesso falliti può indicare attacchi di forza bruta. È importante monitorare e bloccare indirizzi IP che mostrano attività sospette.
- **Accessi SSH:** La registrazione delle sessioni SSH con successo, in particolare per utenti specifici come "djohnson", aiuta a verificare l'integrità e la sicurezza degli accessi remoti.
- **Attività da IP Specifici:** Monitorare i tentativi di accesso falliti provenienti da un singolo IP, come "86.212.199.60", è cruciale per identificare e mitigare potenziali minacce.
- **Errori del Server:** Gli Internal Server Error possono indicare problemi di configurazione o potenziali vulnerabilità nei servizi esposti. Un'analisi approfondita di questi errori è necessaria per garantire la stabilità e la sicurezza dell'infrastruttura.

L'uso di strumenti di analisi dei log come Splunk facilita l'identificazione di anomalie e la risposta a incidenti di sicurezza in tempo reale.