



Esercizio
Progetto

Progetto

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. Tentativi di accesso falliti ("Failed password")

Nuova ricerca

Salva come

Crea vista tabella

Chiudi

```
source="tutorialdata.zip:*" host="DESKTOP-RDDPLBO" "Failed password"
| rex "Failed password for (?<user>\\w+) from (?<src_ip>[\\d\\.]+) port (?<src_port>\\d+)"
| table _time user src_ip src_port
| rename _time as Timestamp, user as "Username", src_ip as "Source IP", src_port as "Port Number"
```

✓ 133.012 eventi (prima di 03/11/24 14:03:14,000)

Nessun campionamento degli eventi

Processo

II

→

🗑️

⬇️

⚡ Modalità veloce

Eventi

Pattern

Statistiche (133.012)

Visualizzazione

20 per pagina

Formato

Anteprima

< Prec

1

2

3

4

5

6

7

8

...

Avanti >

Timestamp	Username	Source IP	Port Number
1730172981			
1730172981			
1730172981			
1730172981	root	123.38.168.208	2295
1730172981			
1730172981	root	128.241.220.82	3117
1730172981			
1730172981			
1730172981	prince	128.241.220.82	2481
1730172981	root	128.241.220.82	1070
1730172981			

source="tutorialdata.zip:*" host="DESKTOP-RDDPLBO" "Failed password"
| rex "Failed password for (?<user>\\w+) from (?<src_ip>[\\d\\.]+) port (?<src_port>\\d+)"
| table _time user src_ip src_port
| rename _time as Timestamp, user as "Username", src_ip as "Source IP", src_port as "Port Number"

Questa query cerca nell' indice per "Failed password" e restituisce il timestamp, l'indirizzo IP di origine, il nome utente e la porta.

2. Sessioni SSH aperte con successo per l'utente "djohnson"

```
source="tutorialdata.zip:*" host="DESKTOP-RDDPLBO" "Accepted password"
| rex "Accepted password for (?<user>\\w+)"
| search user="djohnson"
| table _time user
| rename _time as Timestamp, user as "User ID"
```

✓ 3.820 eventi (prima di 03/11/24 13:51:54,000)

Nessun campionamento degli eventi

Processo

Eventi

Pattern

Statistiche (3.820)

Visualizzazione

10 per pagina

Formato

Anteprima

< Prec

1

Timestamp	User ID
1730345780	djohnson
1730345780	djohnson
1730345780	djohnson
1730345780	djohnson
1730345780	djohnson
1730345780	djohnson
1730259380	djohnson
1730259380	djohnson
1730259380	djohnson
1730259380	djohnson
1730259380	djohnson

source="tutorialdata.zip:*" host="DESKTOP-RDDPLBO" "Accepted password"
| rex "Accepted password for (?<user>\\w+)"
| search user="djohnson"
| table _time user
| rename _time as Timestamp, user as "User ID"

Filtra le sessioni SSH accettate per l'utente specificato e restituisce il timestamp e l'ID utente.

3. Tentativi di accesso falliti dall'indirizzo IP "86.212.199.60"

```
source="tutorialdata.zip:*" host="DESKTOP-RDDPLBO" "Failed password"
| rex "Failed password for (?<user>\\w+) from (?<src_ip>[\\d\\.]+) port (?<src_port>\\d+)"
| search src_ip="86.212.199.60"
| table _time user src_ip src_port
| rename _time as Timestamp, src_ip as "Source IP", user as "Username", src_port as "Port Number"
```

✓ 184 eventi (prima di 03/11/24 13:51:14,000)

Nessun campionamento degli eventi

Processo

Modalità veloce

Eventi

Pattern

Statistiche (184)

Visualizzazione

10 per pagina

Formato

Anteprima

< Prec

1

2

3

4

5

6

7

8

...

Avanti >

Timestamp	Username	Source IP	Port Number
1730259381	sync	86.212.199.60	1695
1730172981	ncsd	86.212.199.60	4022
1730172981	games	86.212.199.60	1763
1730172981	root	86.212.199.60	3683
1730172981	mail	86.212.199.60	2696
1730172981	ftp	86.212.199.60	3216
1730172981	prince	86.212.199.60	1975
1730172981	mail	86.212.199.60	3805
1730172983	edgy	86.212.199.60	1097
1730172982	ftp	86.212.199.60	2043

source="tutorialdata.zip:*" host="DESKTOP-RDDPLBO" "Failed password"
| rex "Failed password for (?<user>\\w+) from (?<src_ip>[\\d\\.]+) port (?<src_port>\\d+)"
| search src_ip="86.212.199.60"
| table _time user src_ip src_port
| rename _time as Timestamp, src_ip as "Source IP", user as "Username", src_port as "Port Number"

Questa query cerca tutti i tentativi di accesso falliti provenienti da un IP specifico e mostra il timestamp, il nome utente e il numero di porta.

4. Indirizzi IP con più di 5 tentativi di accesso falliti

```
source="tutorialdata.zip:*" host="DESKTOP-RDDPLBO" "Failed password"
| rex "from (?<src_ip>[\\d\\.]+)"
| stats count as attempts by src_ip
| where attempts > 5
| table src_ip, attempts
| rename src_ip as "Source IP", attempts as "Number of Attempts"
| sort - attempts
```

✓ 166.265 eventi (prima di 03/11/24 14:29:24,000)

Nessun campionamento degli eventi

Processo

Modalità veloce

Eventi

Pattern

Statistiche (165)

Visualizzazione

20 per pagina

Formato

Anteprima

< Prec

1

2

3

4

5

6

7

8

...

Avanti >

Source IP	Number of Attempts
10.1.10.172	80
10.2.10.163	235
10.3.10.46	605
107.3.146.207	1410
108.65.113.83	1245
109.169.32.135	2575
110.138.30.229	815
110.159.208.78	625
111.161.27.20	430
112.111.162.4	600

```
source="tutorialdata.zip:*" host="DESKTOP-RDDPLBO" "Failed password"
| rex "from (?<src_ip>[\\d\\.]+)"
| stats count as attempts by src_ip
| where attempts > 5
| table src_ip, attempts
| rename src_ip as "Source IP", attempts as "Number of Attempts"
| sort - attempts
```

Conta i tentativi di accesso falliti per ogni indirizzo IP e filtra per quelli con più di 5 tentativi.

5. Errori interni del server (Internal Server Error)

Nuova ricerca

Salva come

Crea vista

```
source="tutorialdata.zip:*" host="DESKTOP-RDDPLBO" status=500
| table _time, host, source, user, uri
| rename _time as Timestamp, host as "Host", source as "Source", user as "User", uri as "URI"
```

✓ 2.932 eventi (prima di 03/11/24 13:38:10,000)

Nessun campionamento degli eventi

Processo

Eventi

Pattern

Statistiche (2.932)

Visualizzazione

10 per pagina

Formato

Anteprima

< Prec

1

2

3

4

5

6

7

Timestamp	Host	Source	User	URI
1730284057	DESKTOP-RDDPLBO	tutorialdata.zip:.\\www1\\access.log	-	/oldlink?itemId=EST-12&JSESSIONID=SD0SL7FF1ADFF44202
1730279801	DESKTOP-RDDPLBO	tutorialdata.zip:.\\www1\\access.log	-	/oldlink?itemId=EST-21&JSESSIONID=SD2SL1FF9ADFF43931
1730277267	DESKTOP-RDDPLBO	tutorialdata.zip:.\\www1\\access.log	-	/oldlink?itemId=EST-14&JSESSIONID=SD1SL10FF1ADFF43736
1730271320	DESKTOP-RDDPLBO	tutorialdata.zip:.\\www1\\access.log	-	/oldlink?itemId=EST-12&JSESSIONID=SD9SL2FF4ADFF43292
1730266097	DESKTOP-RDDPLBO	tutorialdata.zip:.\\www1\\access.log	-	/oldlink?itemId=EST-11&JSESSIONID=SD9SL8FF2ADFF42953
1730265991	DESKTOP-RDDPLBO	tutorialdata.zip:.\\www1\\access.log	-	/cart.do?action=view&itemId=EST-18&JSESSIONID=SD9SL0FF1ADFF42940
1730263449	DESKTOP-RDDPLBO	tutorialdata.zip:.\\www1\\access.log	-	/oldlink?itemId=EST-18&JSESSIONID=SD7SL10FF8ADFF42753
1730259968	DESKTOP-RDDPLBO	tutorialdata.zip:.\\www1\\access.log	-	/product.screen?productId=SF-BVS-001&JSESSIONID=SD6SL9FF10ADFF42533
1730251619	DESKTOP-RDDPLBO	tutorialdata.zip:.\\www1\\access.log	-	/product.screen?productId=SF-BVS-001&JSESSIONID=SD10SL8FF8ADFF41755
1730248551	DESKTOP-RDDPLBO	tutorialdata.zip:.\\www1\\access.log	-	/cart.do?action=purchase&itemId=EST-19&JSESSIONID=SD3SL3FF4ADFF41568

```
source="tutorialdata.zip:*" host="DESKTOP-RDDPLBO" status=500
| table _time, host, source, user, uri
| rename _time as Timestamp, host as "Host", source as "Source", user as "User", uri
as "URI"
```

Cerca gli errori interni del server e restituisce il timestamp

Conclusioni sui log analizzati :

Analizzando i log, è possibile ottenere informazioni preziose sulla sicurezza e l'affidabilità del sistema. I tentativi di accesso falliti possono indicare attività di forza bruta o attacchi mirati, specialmente se provengono da indirizzi IP con molteplici tentativi. Sessioni SSH aperte con successo per utenti specifici possono evidenziare comportamenti normali o anomali. Inoltre, l'analisi degli "Internal Server Error" può rivelare problemi ricorrenti con l'infrastruttura o il codice, suggerendo la necessità di miglioramenti o ottimizzazioni. Utilizzando strumenti di intelligenza artificiale, è possibile automatizzare il monitoraggio di questi log per identificare modelli e anomalie in tempo reale, migliorando così la reattività agli attacchi e la stabilità del sistema.

P.S:

Grazie di tutto Prof :) <3