

Benchmark M6 – Daniele Rufo

Come richiesto dall'esercizio ecco le query.

Per lo svolgimento è stato necessario creare nuovi campi per modificare il parsing ed allinearli alle esigenze di ogni richiesta. Purtroppo il parsing dei nuovi campi (username – sourceIP – port) non risulta perfetto anzi tralascia qualche risultato, lo legge nel modo sbagliato ecc. Li ho creati usando l'interfaccia grafica di Splunk poichè non sapevo usare le “regular expressions” manualmente, nonostante ciò deve esserci qualcosa che mi sfugge perché il risultato è imperfetto. Con i miei strumenti sono riuscito ad arrivare fino a qui, avrei bisogno di più tempo e di uno studio vero del software (quindi tempo) per poter andare oltre.

Negli screenshot si può vedere la query nella barra di ricerca:

1

splunk>enterprise

App

Administrator

Messaggi

Impostazioni

Attività

Guida

Trova

RicercaAnalyticsSet di datiReportAllarmiDashboard

Nuova ricerca

Salva comeCrea vista tabellaChiudi

source=tutorialdata.zip:* FailedPassword=* | table _time sourceIP username port userID

Sempre

✓ 36.143 eventi (prima di 03/11/24 14:35:22,000) Nessun campionamento degli eventi

Processo

Modalità dettagliata

Eventi (36.143)PatternStatistiche (36.143)Visualizzazione

100 per paginaFormatoAnteprima

< Prec12345678...Avanti >

_time	sourceIP	username	port	userID
2024-11-01 16:38:23	194.8.74.23	user appserver	port 3351	
2024-11-01 16:38:23		from 194	port 3768	
2024-11-01 16:38:23	194.8.74.23	user testuser	port 3626	
2024-11-01 16:38:23		from 194	port 4604	
2024-11-01 16:38:23	194.8.74.23	user mongodb	port 2472	
2024-11-01 16:38:23		from 194	port 1552	

2

[illegible]

3

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `source="tutorialdata.zip:*" FailedPassword="*" "from 86.212.199.60" | table _time username port`. The results show 158 events. A tooltip is visible over the search bar area, stating: "Abilita il campionamento degli eventi per eseguire la ricerca e restituire un insieme casuale di eventi." The results table has columns: `_time`, `username`, and `port`.

_time	username	port
2024-11-01 16:38:23	user agushto	port 3692
2024-11-01 16:38:23	user tomcat	port 1464
2024-11-01 16:38:23	user desktop	port 3518
2024-11-01 16:38:23	user yp	port 2856
2024-11-01 16:38:23	from 86	port 1054
2024-11-01 16:38:23	from 86	port 2630

Inizialmente questa query prevedeva la selezione del campo “sourceIP” con cui selezionavo i risultati per l’IP di nostro interesse. Tuttavia, per il problema di creazione campi menzionato sopra, mi sono accorto che il parsing era incompleto quindi, osservando prima l’errore, ho sostituito il campo con un filtro inserito come stringa “from 86.212.199.60” ed infatti gli eventi trovati salgono da 112 a 158.

4

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `source="tutorialdata.zip:*" FailedPassword="*" | stats count as numEvents by sourceIP | where numEvents > 5`. The results show 36,143 events. The results table has columns: `sourceIP` and `numEvents`.

sourceIP	numEvents
196.28.38.71	42
195.69.252.22	49
74.208.173.14	58
192.188.106.240	62
89.167.143.32	63
95.163.78.227	63
111.161.27.20	66

Ho provato diverse metodologie cercando una soluzione il più semplice possibile e adeguata alle mie conoscenze. Mi sono aiutato rinominando “numEvents” il numero di tentativi indicizzandoli per indirizzo IP e poi ho preso questo output e l’ho sottoposto alla condizione “numEvents>5” per il ritorno esclusivo dei dati richiesti.

5

The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with 'splunk>enterprise' and various menu items like 'App', 'Administrator', 'Messaggi', 'Impostazioni', 'Attività', 'Guida', and 'Trova'. Below this is a sub-navigation bar with 'Ricerca', 'Analytics', 'Set di dati', 'Report', 'Allarmi', and 'Dashboard'. The main content area is titled 'Nuova ricerca' and contains a search bar with the query 'source="tutorialdata.zip:*" | search status=500 | table method clientip'. Below the search bar, it shows '733 eventi (prima di 03/11/24 15:47:18,000)' and a 'Processo' button. The results are displayed in a table view with columns 'method' and 'clientip'. The table shows several rows of data, including GET and POST methods with corresponding client IP addresses.

method	clientip
GET	198.35.1.75
GET	198.35.1.75
POST	125.89.78.6
POST	194.146.236.22
POST	121.254.179.199
GET	76.89.103.115

Ho aggiunto una visualizzazione tabellare che riporta metodo della richiesta http e client IP per avere una visione più completa poiché credo siano info utili per “Internal Server Error”

Grazie

Daniele Rufo