W24D4 - PROGETTO SPLUNK

SOMMARIO

Oggi si userà Splunk, una piattaforma di software progettata per la raccolta, l'analisi e la visualizzazione dei dati generati da macchine, come log, eventi e dati di monitoraggio in tempo reale. È ampiamente utilizzato per l'analisi dei dati operativi, la gestione della sicurezza, e la risoluzione dei problemi in ambienti complessi. Splunk consente di aggregare, indicizzare e cercare enormi volumi di dati non strutturati in modo rapido ed efficiente.
Il progetto che verrà sviluppato prevede l'uso di Splunk per eseguire analisi sui dati. L'obiettivo sarà quello di esplorare e analizzare i dati raccolti da vari sistemi, applicazioni o dispositivi, utilizzando specifiche query per estrarre informazioni utili, rilevare anomalie e generare report visuali. Il compito includerà l'analisi dei risultati ottenuti e la loro presentazione sotto forma di dashboard o report.

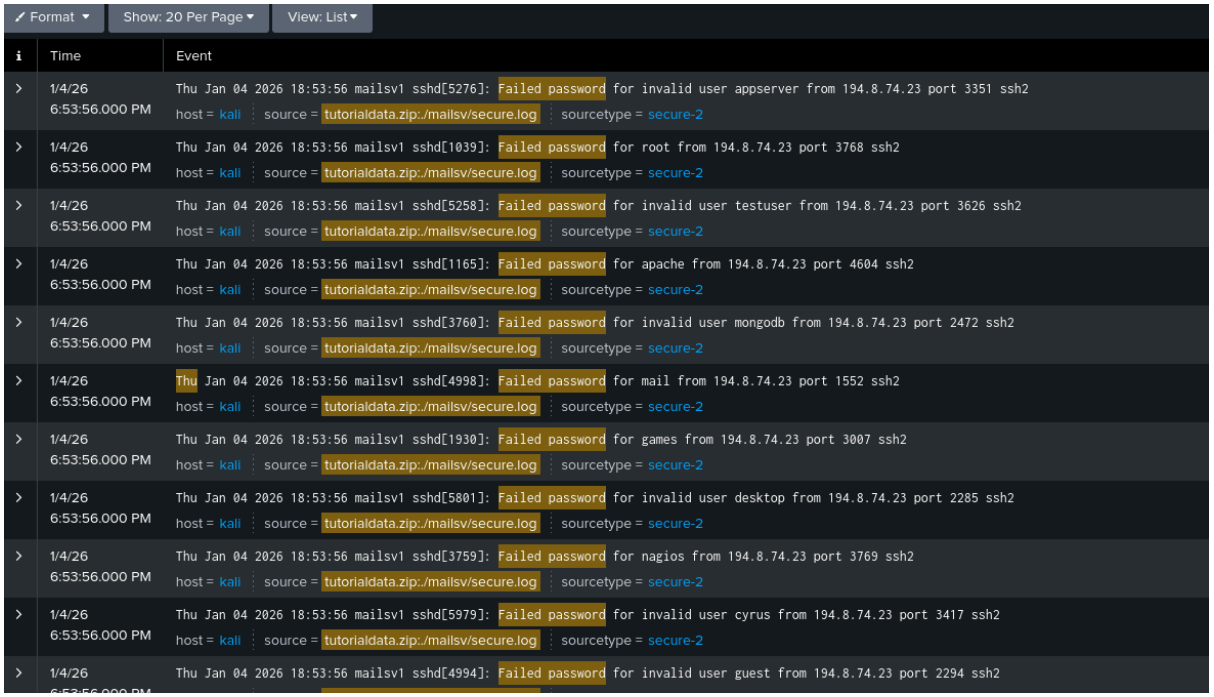
QUERY 1

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.

con la seguente query:

```
source="tutorialdata.zip:*" | search "failed password"
```

ricondurremo a trovare i tentativi di accesso falliti



QUERY 2

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.

con la seguente query:

```
source="tutorialdata.zip:*" | search "ssh2" | search "accepted"
```

siamo riusciti a vedere tutte le sessioni SSH

i	Time	Event
>	1/4/26 6:53:56.000 PM	Thu Jan 04 2026 18:53:56 mailsv1 sshd[74181]: Accepted password for nsharpe from 10.2.10.163 port 4245 ssh2 host = kali source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2
>	1/4/26 6:53:56.000 PM	Thu Jan 04 2026 18:53:56 mailsv1 sshd[54545]: Accepted password for djohnson from 10.3.10.46 port 5143 ssh2 host = kali source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2
>	1/4/26 6:53:56.000 PM	Thu Jan 04 2026 18:53:56 mailsv1 sshd[90328]: Accepted password for djohnson from 10.3.10.46 port 3914 ssh2 host = kali source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2
>	1/4/26 6:53:56.000 PM	Thu Jan 04 2026 18:53:56 mailsv1 sshd[64272]: Accepted password for nsharpe from 10.2.10.163 port 6379 ssh2 host = kali source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2
>	1/4/26 6:53:56.000 PM	Thu Jan 04 2026 18:53:56 mailsv1 sshd[96628]: Accepted password for myuan from 10.1.10.172 port 9590 ssh2 host = kali source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2
>	1/4/26 6:53:56.000 PM	Thu Jan 04 2026 18:53:56 mailsv1 sshd[19779]: Accepted password for nsharpe from 10.2.10.163 port 2836 ssh2 host = kali source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2
>	1/4/26 6:53:56.000 PM	Thu Jan 04 2026 18:53:56 mailsv1 sshd[52473]: Accepted password for djohnson from 10.3.10.46 port 5449 ssh2 host = kali source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2
>	1/4/26 6:53:56.000 PM	Thu Jan 04 2026 18:53:56 mailsv1 sshd[96461]: Accepted password for djohnson from 10.3.10.46 port 3041 ssh2 host = kali source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2
>	1/4/26 6:53:56.000 PM	Thu Jan 04 2026 18:53:56 mailsv1 sshd[15363]: Accepted password for myuan from 10.1.10.172 port 4531 ssh2 host = kali source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2

QUERY 3

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.

con la seguente query:

```
source="tutorialdata.zip:*" | search "failed password" "86.212.199.60"
```

vedremo gli eventi dei tentativi di login falliti provenienti dall'IP 86.212.199.60

QUERY 4

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.

per quanto riguardano gli eventi sono gli stessi della query 1, ma per mostrare l'indirizzo IP e il numero de tentativi, in questo caso più di 5 volte, si procederà così:

source="tutorialdata.zip:*" | search "failed password" –la query base
| rex field =*raw "from (?<source*ip>\d)" – estrazione degli indirizzi IP
| stats count as FAIL by source_ip – si adopera stats una funzione di Splunk per il conteggio dei tentativi e lo metteremo in una variabile, in questo caso FAIL
| where FAIL >5 – condizione richiesta più di 5 tentativi falliti di login
| table source_ip FAIL –riporto i dati in tabella

QUERY 5

Crea una query Splunk per trovare tutti gli Internal Server Error.

la query è la seguente:
source="tutorialdata.zip:*" | search status=500