

# 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

Format	Show: 20 Per Page	View: List
i	Time	Event
>	1/4/26 6:53:56.000 PM	Thu Jan 04 2026 18:53:56 mailsv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 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[1039]: Failed password for root from 194.8.74.23 port 3768 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[5258]: Failed password for invalid user testuser from 194.8.74.23 port 3626 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[1165]: Failed password for apache from 194.8.74.23 port 4604 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[3760]: Failed password for invalid user mongodb from 194.8.74.23 port 2472 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[4998]: Failed password for mail from 194.8.74.23 port 1552 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[1930]: Failed password for games from 194.8.74.23 port 3007 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[5801]: Failed password for invalid user desktop from 194.8.74.23 port 2285 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[3759]: Failed password for nagios from 194.8.74.23 port 3769 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[5979]: Failed password for invalid user cyrus from 194.8.74.23 port 3417 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[4994]: Failed password for invalid user guest from 194.8.74.23 port 2294 ssh2 host = kali   source = tutorialdata.zip./mailsv/secure.log   sourcetype = secure-2

## 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

i	Time	Event
>	1/4/26 6:53:56.000 PM	Thu Jan 04 2026 18:53:56 mailsv1 sshd[5728]: Failed password for invalid user agushto from 86.212.199.60 port 3692 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[4843]: Failed password for invalid user tomcat from 86.212.199.60 port 1464 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[5718]: Failed password for invalid user desktop from 86.212.199.60 port 3518 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[1008]: Failed password for invalid user yp from 86.212.199.60 port 2856 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[5878]: Failed password for mail from 86.212.199.60 port 1054 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[2649]: Failed password for apache from 86.212.199.60 port 2630 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[2079]: Failed password for invalid user services from 86.212.199.60 port 4740 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[2205]: Failed password for invalid user irc from 86.212.199.60 port 1203 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[3680]: Failed password for invalid user mysql from 86.212.199.60 port 4802 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[1679]: Failed password for invalid user pmuser from 86.212.199.60 port 1775 ssh2 host = kali   source = tutorialdata.zip:/mailsv/secure.log   sourcetype = secure-2
>	1/4/26	Thu Jan 04 2026 18:53:56 mailsv1 sshd[3243]: Failed password for invalid user ventrilo from 86.212.199.60 port 1465 ssh2

## 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 (?<sourceip>\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

source="tutorialdata.zip:*"   search status=500		
733 events (before 1/5/26 4:08:46.000 PM) No Event Sampling		
Events (733) Patterns Statistics Visualization		
Timeline format Zoom Out Zoom to Selection Deselect		
Format Show: 20 Per Page View: List		
Hide Fields All Fields	i	Time Event
SELECTED FIELDS a host 1 a source 3 a sourcetype 1	>	1/4/26 6:18:59.000 PM 198.35.1.75 - - [04/Jan/2026:18:18:59] "GET /cart.do?action=addtocart&itemId=EST-13&JSESSIONID=SD10SL2FF4ADF53099 HTTP/1.1" 500 2324 "http://a/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 645 host = kali   source = tutorialdata.zip:/www1/access.log   sourcetype = access_combined_wcookie
INTERESTING FIELDS a action 5 # bytes 100+ a categoryid 1 a clientip 100+ # date_hour 24	>	1/4/26 6:18:55.000 PM 198.35.1.75 - - [04/Jan/2026:18:18:55] "GET /product.screen?productId=SF-BVS-G01&JSESSIONID=SD10SL2FF4ADF53099 HTTP/1.1" 500 2809 "http://a/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 370 host = kali   source = tutorialdata.zip:/www1/access.log   sourcetype = access_combined_wcookie
	>	1/4/26 5:42:03.000 PM 125.89.78.6 - - [04/Jan/2026:17:42:03] "POST /cart.do?action=changequantity&itemId=EST-16&JSESSIONID=SD10SL8FF3ADF52952 HTTP/1.1" 500 1168 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 230 host = kali   source = tutorialdata.zip:/www2/access.log   sourcetype = access_combined_wcookie