

W24D4

- Scarico da internet “tutorialdata.zip”
- Lo importo su splunk da impostazioni > aggiungi dati > seguo la procedura, ma creo un indice e spacchetto l’import
- Prima query (“Failed password”)

```
source="tutorialdata.zip:*" index="tutorial_data" "Failed password"

| rex field=_raw "Failed password for (invalid user )?(?<user>\S+) from"

| table _time host user _raw
```

Nuova ricerca

source="tutorialdata.zip:*" index="tutorial_data" "Failed password"
| rex field=_raw "Failed password for (invalid user)?(?<user>\S+) from"
| table _time host user _raw

33.253 eventi (prima di 04/11/24 02:37:50.000) Nessun campionamento degli eventi

Processo

Eventi Pattern Statistiche (33.253) Visualizzazione

100 per pagina Formato Anteprima

_time	host	user	_raw
2024-10-27 16:38:07	127.0.0.1	testing	Fri Oct 27 2024 16:38:07 www1 sshd[1004]: Failed password for invalid user testing from 124.169.192.241 port 2328 ssh2
2024-10-27 16:38:07	127.0.0.1	amavis	Fri Oct 27 2024 16:38:07 www1 sshd[1005]: Failed password for invalid user amavis from 110.159.286.78 port 2612 ssh2
2024-10-27 16:38:07	127.0.0.1	noone	Fri Oct 27 2024 16:38:07 www1 sshd[1006]: Failed password for invalid user noone from 208.65.153.253 port 3352 ssh2
2024-10-27 16:38:07	127.0.0.1	sysadmin	Fri Oct 27 2024 16:38:07 www1 sshd[1008]: Failed password for invalid user sysadmin from 203.172.197.2 port 1448 ssh2
2024-10-27 16:38:07	127.0.0.1	vpuser	Fri Oct 27 2024 16:38:07 www1 sshd[1010]: Failed password for invalid user vpuser from 221.207.229.6 port 4887 ssh2
2024-10-27 16:38:07	127.0.0.1	vpuser	Fri Oct 27 2024 16:38:07 www1 sshd[1011]: Failed password for invalid user vpuser from 99.61.68.238 port 4313 ssh2
2024-10-27 16:38:07	127.0.0.1	ftp	Fri Oct 27 2024 16:38:07 www1 sshd[1012]: Failed password for ftp from 87.194.216.51 port 3740 ssh2
2024-10-27 16:38:07	127.0.0.1	dba	Fri Oct 27 2024 16:38:07 www1 sshd[1017]: Failed password for invalid user dba from 195.216.243.24 port 2925 ssh2
2024-10-27 16:38:07	127.0.0.1	mailman	Fri Oct 27 2024 16:38:07 www1 sshd[1019]: Failed password for invalid user mailman from 176.212.8.44 port 4433 ssh2
2024-10-27 16:38:07	127.0.0.1	services	Fri Oct 27 2024 16:38:07 www1 sshd[1027]: Failed password for invalid user services from 117.21.246.164 port 4194 ssh2
2024-10-27 16:38:07	127.0.0.1	gopher	Fri Oct 27 2024 16:38:07 www1 sshd[1028]: Failed password for gopher from 175.44.1.122 port 1164 ssh2
2024-10-27 16:38:07	127.0.0.1	postgres	Fri Oct 27 2024 16:38:07 www1 sshd[1030]: Failed password for invalid user postgres from 91.217.178.210 port 3926 ssh2
2024-10-27 16:38:07	127.0.0.1	nobody	Fri Oct 27 2024 16:38:07 www1 sshd[1031]: Failed password for nobody from 99.61.68.238 port 1117 ssh2
2024-10-27 16:38:07	127.0.0.1	mail	Fri Oct 27 2024 16:38:07 www1 sshd[1038]: Failed password for mail from 123.196.113.11 port 3134 ssh2
2024-10-27 16:38:07	127.0.0.1	mailman	Fri Oct 27 2024 16:38:07 www1 sshd[1041]: Failed password for invalid user mailman from 95.130.178.231 port 3689 ssh2
2024-10-27 16:38:07	127.0.0.1	sys	Fri Oct 27 2024 16:38:07 www1 sshd[1044]: Failed password for invalid user sys from 92.1.170.135 port 4884 ssh2
2024-10-27 16:38:07	127.0.0.1	susan	Fri Oct 27 2024 16:38:07 www1 sshd[1045]: Failed password for invalid user susan from 175.44.1.172 port 4891 ssh2

- Seconda query (prendere id utente dove accetto psw a djohnson)
- ```
source="tutorialdata.zip:*" index="tutorial_data" "Accepted password for djohnson"

| rex field=_raw "sshd\[(?<user_id>\d+)\]"

| table _time user_id
```

Nuova ricerca

source="tutorialdata.zip:\*" index="tutorial\_data" "Accepted password for djohnson"  
| rex field=\_raw "sshd\[(?<user\_id>\d+)\]"  
| table \_time user\_id

955 eventi (prima di 04/11/24 02:41:06.000) Nessun campionamento degli eventi

Processo

Eventi Pattern Statistiche (955) Visualizzazione

100 per pagina Formato Anteprima

| _time               | user_id |
|---------------------|---------|
| 2024-11-02 16:38:07 | 38585   |
| 2024-11-02 16:38:07 | 85131   |
| 2024-11-02 16:38:07 | 18828   |
| 2024-11-02 16:38:07 | 3725    |
| 2024-11-02 16:38:07 | 24113   |
| 2024-11-02 16:38:07 | 52845   |
| 2024-11-02 16:38:07 | 87824   |
| 2024-11-02 16:38:07 | 4312    |
| 2024-11-02 16:38:07 | 44968   |
| 2024-11-02 16:38:07 | 34855   |
| 2024-11-02 16:38:07 | 25970   |
| 2024-11-02 16:38:07 | 65707   |
| 2024-11-02 16:38:07 | 88188   |
| 2024-11-02 16:38:07 | 47122   |
| 2024-11-02 16:38:07 | 78218   |
| 2024-11-02 16:38:07 | 9445    |
| 2024-11-02 16:38:07 | 35434   |

- Terza query.

```
source="tutorialdata.zip:*" index="tutorial_data" "Failed password" "86.212.199.60"
```

```
| rex field=_raw "Failed password for (invalid user)?(?<user>\S+) from \S+ port (?<port>\d+)"
```

```
| table _time user port
```

Nuova ricerca

Salva come Crea vista tabella Chiudi

source="tutorialdata.zip:\*" index="tutorial\_data" "Failed password" "86.212.199.60"  
 | rex field=\_raw "Failed password for (invalid user )?(?<user>\S+) from \S+ port (?<port>\d+)"  
 | table \_time user port

158 eventi (prima di 04/11/24 02:44:35,000) Nessun campionamento degli eventi

Processo

Eventi Pattern Statistiche (158) Visualizzazione

100 per pagina Formato Anteprima

| _time               | user          | port |
|---------------------|---------------|------|
| 2024-11-01 16:38:00 | services      | 1393 |
| 2024-11-01 16:38:00 | sync          | 1695 |
| 2024-11-01 16:38:00 | admin         | 3673 |
| 2024-11-01 16:38:00 | nginx         | 1582 |
| 2024-11-01 16:38:00 | whois         | 1635 |
| 2024-11-01 16:38:00 | mailman       | 4339 |
| 2024-11-01 16:38:00 | mailman       | 1954 |
| 2024-11-01 16:38:00 | rdp           | 2658 |
| 2024-10-31 16:38:00 | ncsd          | 4822 |
| 2024-10-31 16:38:00 | games         | 1763 |
| 2024-10-31 16:38:00 | noone         | 1583 |
| 2024-10-31 16:38:00 | fpass         | 3428 |
| 2024-10-31 16:38:00 | divine        | 1859 |
| 2024-10-31 16:38:00 | root          | 3683 |
| 2024-10-31 16:38:00 | administrator | 1173 |
| 2024-10-31 16:38:00 | administrator | 3473 |
| 2024-10-31 16:38:00 | mail          | 7608 |

- Quarta query

```
source="tutorialdata.zip:*" index="tutorial_data" "Failed password"
```

```
| rex field=_raw "from (?<src_ip>\S+) port"
```

```
| stats count by src_ip
```

```
| where count > 5
```

```
| table src_ip count
```

Nuova ricerca

Salva come Crea vista tabella Chiudi

source="tutorialdata.zip:\*" index="tutorial\_data" "Failed password"  
 | rex field=\_raw "from (?<src\_ip>\S+) port"  
 | stats count by src\_ip  
 | where count > 5  
 | table src\_ip count

33.253 eventi (prima di 04/11/24 02:46:53,000) Nessun campionamento degli eventi

Processo

Eventi Pattern Statistiche (185) Visualizzazione

100 per pagina Formato Anteprima

| src_ip          | count |
|-----------------|-------|
| 10.1.10.172     | 16    |
| 10.2.10.163     | 47    |
| 10.3.10.46      | 121   |
| 107.3.146.207   | 282   |
| 108.65.113.83   | 249   |
| 109.169.32.135  | 515   |
| 110.138.30.729  | 163   |
| 110.159.208.78  | 125   |
| 111.161.27.20   | 86    |
| 112.111.162.4   | 128   |
| 117.21.246.164  | 195   |
| 118.142.68.222  | 92    |
| 12.130.60.4     | 227   |
| 12.130.60.5     | 155   |
| 121.254.179.199 | 183   |

- Quinta query  
index="tutorial\_data" ("error" OR "500")  
| table\_time host\_raw

### Nuova ricerca

index:"tutorial\_data" ("error" OR "500")  
 | table\_time host -raw

**1.208 eventi** (prima di 04/11/24 02:48:52.000)    Nessun campionamento degli eventi ▼

Processo ▾ || = ↻ ⬅ ➡ ⬇ Modaltà intelligente ▼

| Eventi           | Pattern   | Statistiche (1.208) | Visualizzazione |
|------------------|-----------|---------------------|-----------------|
| 100 per pagina ▾ | Formato ▾ | Anteprima ▾         |                 |
| < Precedente     | 1         | 2                   | 3               |
|                  | 4         | 5                   | 6               |
|                  | 7         | 8                   |                 |
| Avanti >         |           |                     |                 |

| _time s             | host s    | raw s                                                                                                                                                                                                                                                                                                                        |
|---------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2024-11-01 11:27:37 | 127.0.0.1 | 142.233.200.21 ~ [81/Nov/2024:11:27:37] "GET /oldlink?itemID=EST-12&SESSIONID=S0SL9FFADFF440B HTTP 1.1" 500 886 "http://www.buttercupgames.com/cart.do?action=changequantity&itemID=EST-12" Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5 816                   |
| 2024-11-01 10:42:35 | 127.0.0.1 | 121.9.245.177 ~ [81/Nov/2024:10:42:35] "POST /cart/error.do?msg=CredNotAccepted&SESSIONID=S0SL9FFADFF440B HTTP 1.1" 200 1394 "http://www.buttercupgames.com/cart.do?action=purchase&itemID=EST-1" Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/1.0; .NET CLR 3.5.30729; .NET4.WC) 862                   |
| 2024-11-01 10:16:41 | 127.0.0.1 | 201.28.109.162 ~ [81/Nov/2024:10:16:41] "GET /oldlink?itemID=EST-21&SESSIONID=S0ZL1YFPAOFF4393 HTTP 1.1" 500 3643 "http://www.buttercupgames.com/cart.do?action=viewItem&itemID=EST-21" Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120808 Firefox/3.6.20 (.NET CLR 3.5.30729; .NET4.WC) 452        |
| 2024-11-01 10:09:18 | 127.0.0.1 | 126.241.229.82 ~ [81/Nov/2024:10:09:18] "GET /category.screen?categoryId=STRATEGY&SESSIONID=S0SL9FFADFF4393 HTTP 1.1" 200 734 "http://www.buttercupgames.com/category.screen?categoryId=STRATEGY" Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5 500             |
| 2024-11-01 09:34:27 | 127.0.0.1 | 76.89.183.115 ~ [81/Nov/2024:09:34:27] "POST /oldlink?itemID=EST-14&SESSIONID=S0SL1WFF1BAOFF43736 HTTP 1.1" 500 297 "http://www.buttercupgames.com/category.screen?categoryId=NALL" Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8.3) 682                                     |
| 2024-11-01 09:03:22 | 127.0.0.1 | 203.92.58.136 ~ [81/Nov/2024:09:03:22] "POST /cart/error.do?msg=CredNotAccepted&SESSIONID=S0BL9FFADFF4388 HTTP 1.1" 200 1932 "http://www.buttercupgames.com/cart.do?action=purchase&itemID=EST-21" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/534.55.3 (KHTML, like Gecko) Version/5.1.5 Safari/534.55.3 544 |
| 2024-11-01 08:38:48 | 127.0.0.1 | 195.216.243.24 ~ [81/Nov/2024:08:38:48] "POST /cart/error.do?msg=ForeError&SESSIONID=S0BL9FFADFF4343 HTTP 1.1" 200 1862 "http://www.buttercupgames.com/cart.do?action=purchase&itemID=EST-21" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5 487      |
| 2024-11-01 07:55:28 | 127.0.0.1 | 182.236.164.11 ~ [81/Nov/2024:07:55:28] "GET /oldlink?itemID=EST-12&SESSIONID=S0SL2PFFADFF43292 HTTP 1.1" 500 3317 "http://www.buttercupgames.com/cart.do?action=viewItem&itemID=EST-12" Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120808 Firefox/3.6.20 (.NET CLR 3.5.30729; .NET4.WC) 145       |
| 2024-11-01 07:07:34 | 127.0.0.1 | 130.251.37.97 ~ [81/Nov/2024:07:07:34] "POST /cart/error.do?msg=nothingInCart&SESSIONID=S0SL9FFADFF4389 HTTP 1.1" 200 3123 "http://www.buttercupgames.com/cart.do?action=purchase&itemID=EST-7" Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8.3) 837                         |
| 2024-11-01 07:00:22 | 127.0.0.1 | 91.285.183.27 ~ [81/Nov/2024:07:00:22] "POST /cart/error.do?msg=ForeError&SESSIONID=S0SL2PFFADFF43874 HTTP 1.1" 200 1675 "http://www.buttercupgames.com/cart.do?action=purchase&itemID=EST-14" Opera/9.60 (Windows NT 5.1; U; en)" 955                                                                                       |

- Conclusioni utilizzando AI.

Risposta AI:

Le query che hai eseguito su Splunk forniscono una panoramica utile sui tentativi di accesso al sistema e sugli errori rilevati. Ecco un'analisi dettagliata dei risultati e alcune conclusioni che puoi trarre dai log analizzati:

### 1. Tentativi di Accesso Falliti ("Failed password")

- **Query Analizzata:** La prima query identifica tutti i tentativi di accesso falliti, mostrando il timestamp, l'host, il nome utente (se esiste) e il log grezzo.
- **Conclusione:** I tentativi di accesso falliti possono indicare un potenziale attacco brute-force, soprattutto se provengono da indirizzi IP non autorizzati o se ci sono molteplici tentativi con utenti diversi. È importante monitorare questi eventi per identificare e mitigare possibili rischi per la sicurezza.

## 2. Accessi Riusciti per l'Utente "djohnson"

- **Query Analizzata:** La seconda query cerca gli accessi SSH riusciti per l'utente djohnson e cattura l'ID utente associato.
- **Conclusione:** Gli accessi autorizzati dell'utente djohnson sono importanti per garantire che solo persone autorizzate possano accedere al sistema. Se ci sono molti accessi in momenti sospetti o non ordinari, potrebbe essere necessario eseguire un controllo di sicurezza.

### 3. Tentativi di Accesso Falliti dall'IP "86.212.199.60"

- **Query Analizzata:** La terza query si concentra sui tentativi di accesso falliti provenienti da un indirizzo IP specifico e mostra il timestamp, l'utente (se presente) e il numero di porta.
- **Conclusione:** Un singolo indirizzo IP che tenta ripetutamente di accedere al sistema potrebbe indicare un comportamento sospetto o un attacco mirato. Questo IP dovrebbe essere bloccato o segnalato per prevenire ulteriori tentativi di accesso.

#### 4. Indirizzi IP con più di 5 Tentativi di Accesso Falliti

- **Query Analizzata:** La quarta query identifica gli indirizzi IP che hanno effettuato più di 5 tentativi falliti.
- **Conclusione:** Un numero elevato di tentativi di accesso falliti da un singolo IP potrebbe indicare un attacco brute-force. È consigliabile implementare misure di sicurezza, come il blocco degli IP sospetti o l'uso di un sistema di rilevamento delle intrusioni (IDS).

#### **5. Errori di Server ("error" o "500")**

- **Query Analizzata:** La quinta query cerca eventi che contengono la parola "error" o il codice di stato HTTP "500", mostrando l'host e il log grezzo.
- **Conclusione:** La presenza di errori del server, come "Internal Server Error" (500), indica problemi con il funzionamento del sistema. Questi errori devono essere diagnosticati e risolti per garantire che l'applicazione funzioni correttamente e per evitare tempi di inattività.

---

#### **Conclusioni Generali sui Log Analizzati**

1. **Sicurezza:** I numerosi tentativi di accesso falliti suggeriscono che il sistema è potenzialmente oggetto di attacchi brute-force o di attività non autorizzate. È importante rafforzare le politiche di sicurezza, come l'implementazione di autenticazione a più fattori (MFA) e il monitoraggio continuo degli accessi.
2. **Accessi Riusciti:** Monitorare gli accessi riusciti, in particolare per utenti privilegiati come djohnson, è essenziale per garantire che non vi siano compromissioni. È possibile configurare alert per accessi sospetti o non usuali.
3. **Errori di Sistema:** Gli errori server-side devono essere analizzati e risolti per migliorare la stabilità e la sicurezza del sistema. Potrebbero essere necessari aggiornamenti software o ottimizzazioni della configurazione.

Se desideri ulteriori approfondimenti su come migliorare la sicurezza o le prestazioni del sistema basandoti su questi risultati, fammelo sapere!

#### **CONCLUSIONE (mia, non AI):**

L'analisi dei log rivela numerosi tentativi di accesso falliti, suggerendo, probabilmente, potenziali attacchi brute-force che richiedono misure di sicurezza, come il blocco degli IP sospetti e insoliti e l'uso di sistemi di rilevamento delle intrusioni. Gli accessi riusciti dell'utente "djohnson" devono essere attentamente monitorati per evitare compromissioni. Gli errori di server, come i "500 Internal Server Error", indicano problemi da diagnosticare per migliorare la stabilità del sistema e prevenire interruzioni.

Il monitoraggio continuo è fondamentale per far sì che non si creino problemi di alcun tipo (che non si portino avanti soprattutto).