

## M6W24D4

### Analisi del malware e Splunk

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.

---

Non riuscendo ad avviarsi su Windows 10 Pro, ho scritto su Prompt dei comandi: net start splunkd per far avviare il servizio dopo che era uscito di non riuscire a stabilire la connessione sulla porta 8000.

Query1 (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): `source="tutorialdata.zip:*" host="Splunk" | rex "Failed password for (invalid user )?(?w+) from (?d{1,3}(?:.d{1,3}){3}) port d+" | eval reason=if(match(_raw, "invalid user"), "Invalid user", "Valid user - wrong password") | table _time, src_ip, username, reason | sort - _time)` come da immagine sottostante, permette di poter vedere e filtrare gli eventi di mancata corretta immissione password in ordine di indirizzo ip, nome utente, motivo del fallimento e a che ora si è verificato l'evento.

Analizziamo la query:

**source="tutorialdata.zip:\*"**: Cerca i dati all'interno di un archivio ZIP chiamato tutorialdata.zip.

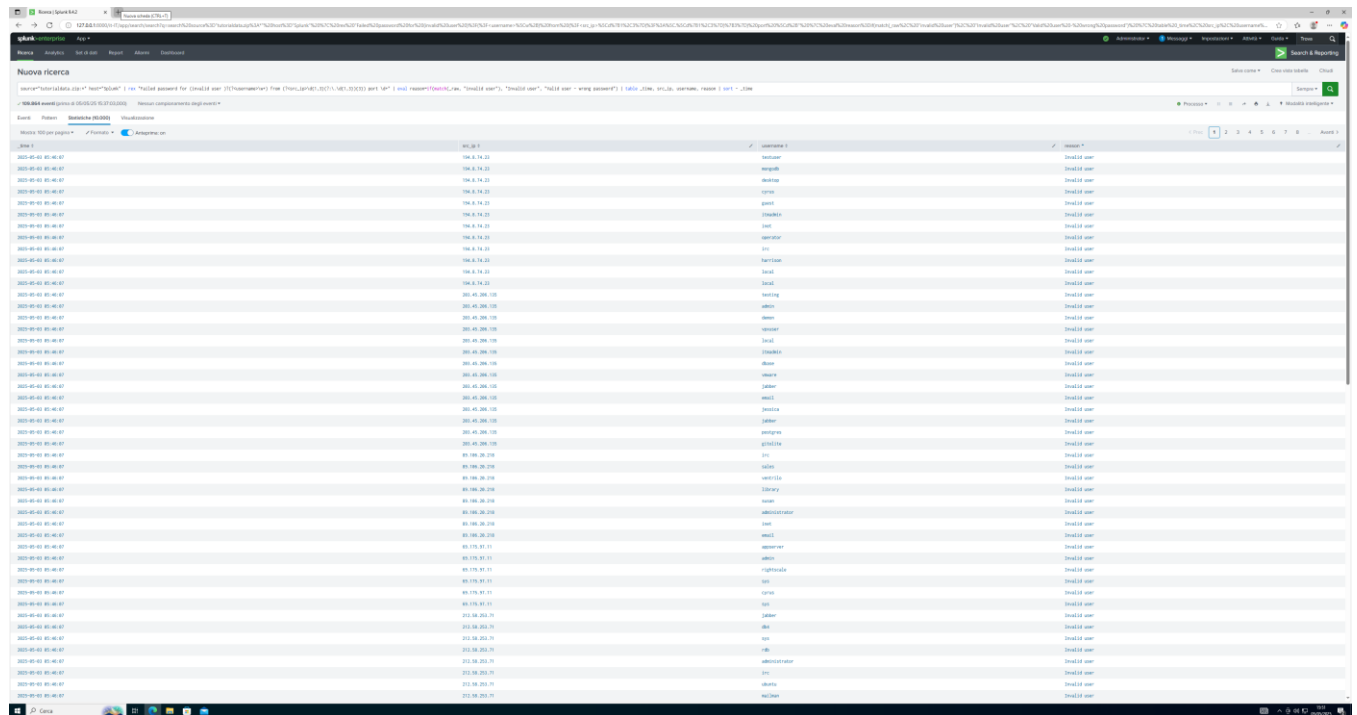
**host="Splunk"**: Filtra solo i log provenienti dall'host denominato Splunk.

**rex "Failed password for (invalid user )?(?w+) from (?d{1,3}(?:.d{1,3}){3}) port d+":** Utilizza la funzione rex per estrarre informazioni dai messaggi di log ed estrae il username e l'IP di origine (src\_ip).

**eval reason=if(match(\_raw, "invalid user"), "Invalid user", "Valid user - wrong password")**: Crea un campo chiamato reason che identifica il motivo del fallimento, se la riga contiene "invalid user", allora il motivo sarà "Invalid user" altrimenti, sarà "Valid user - wrong password".

**table \_time, src\_ip, username, reason:** Visualizza i dati in una tabella con le colonne

**Sort - \_time:** Ordina i risultati in ordine decrescente per data, mostrando prima i tentativi più recenti.



_time	src_ip	username	reason
2023-01-01 00:00:00	192.168.1.1	root	Invalid user
2023-01-01 00:00:01	192.168.1.1	admin	Invalid user
2023-01-01 00:00:02	192.168.1.1	user	Invalid user
2023-01-01 00:00:03	192.168.1.1	root	Invalid user
2023-01-01 00:00:04	192.168.1.1	admin	Invalid user
2023-01-01 00:00:05	192.168.1.1	user	Invalid user
2023-01-01 00:00:06	192.168.1.1	root	Invalid user
2023-01-01 00:00:07	192.168.1.1	admin	Invalid user
2023-01-01 00:00:08	192.168.1.1	user	Invalid user
2023-01-01 00:00:09	192.168.1.1	root	Invalid user
2023-01-01 00:00:10	192.168.1.1	admin	Invalid user
2023-01-01 00:00:11	192.168.1.1	user	Invalid user
2023-01-01 00:00:12	192.168.1.1	root	Invalid user
2023-01-01 00:00:13	192.168.1.1	admin	Invalid user
2023-01-01 00:00:14	192.168.1.1	user	Invalid user
2023-01-01 00:00:15	192.168.1.1	root	Invalid user
2023-01-01 00:00:16	192.168.1.1	admin	Invalid user
2023-01-01 00:00:17	192.168.1.1	user	Invalid user
2023-01-01 00:00:18	192.168.1.1	root	Invalid user
2023-01-01 00:00:19	192.168.1.1	admin	Invalid user
2023-01-01 00:00:20	192.168.1.1	user	Invalid user
2023-01-01 00:00:21	192.168.1.1	root	Invalid user
2023-01-01 00:00:22	192.168.1.1	admin	Invalid user
2023-01-01 00:00:23	192.168.1.1	user	Invalid user
2023-01-01 00:00:24	192.168.1.1	root	Invalid user
2023-01-01 00:00:25	192.168.1.1	admin	Invalid user
2023-01-01 00:00:26	192.168.1.1	user	Invalid user
2023-01-01 00:00:27	192.168.1.1	root	Invalid user
2023-01-01 00:00:28	192.168.1.1	admin	Invalid user
2023-01-01 00:00:29	192.168.1.1	user	Invalid user
2023-01-01 00:00:30	192.168.1.1	root	Invalid user
2023-01-01 00:00:31	192.168.1.1	admin	Invalid user
2023-01-01 00:00:32	192.168.1.1	user	Invalid user
2023-01-01 00:00:33	192.168.1.1	root	Invalid user
2023-01-01 00:00:34	192.168.1.1	admin	Invalid user
2023-01-01 00:00:35	192.168.1.1	user	Invalid user
2023-01-01 00:00:36	192.168.1.1	root	Invalid user
2023-01-01 00:00:37	192.168.1.1	admin	Invalid user
2023-01-01 00:00:38	192.168.1.1	user	Invalid user
2023-01-01 00:00:39	192.168.1.1	root	Invalid user
2023-01-01 00:00:40	192.168.1.1	admin	Invalid user
2023-01-01 00:00:41	192.168.1.1	user	Invalid user
2023-01-01 00:00:42	192.168.1.1	root	Invalid user
2023-01-01 00:00:43	192.168.1.1	admin	Invalid user
2023-01-01 00:00:44	192.168.1.1	user	Invalid user
2023-01-01 00:00:45	192.168.1.1	root	Invalid user
2023-01-01 00:00:46	192.168.1.1	admin	Invalid user
2023-01-01 00:00:47	192.168.1.1	user	Invalid user
2023-01-01 00:00:48	192.168.1.1	root	Invalid user
2023-01-01 00:00:49	192.168.1.1	admin	Invalid user
2023-01-01 00:00:50	192.168.1.1	user	Invalid user
2023-01-01 00:00:51	192.168.1.1	root	Invalid user
2023-01-01 00:00:52	192.168.1.1	admin	Invalid user
2023-01-01 00:00:53	192.168.1.1	user	Invalid user
2023-01-01 00:00:54	192.168.1.1	root	Invalid user
2023-01-01 00:00:55	192.168.1.1	admin	Invalid user
2023-01-01 00:00:56	192.168.1.1	user	Invalid user
2023-01-01 00:00:57	192.168.1.1	root	Invalid user
2023-01-01 00:00:58	192.168.1.1	admin	Invalid user
2023-01-01 00:00:59	192.168.1.1	user	Invalid user
2023-01-01 00:01:00	192.168.1.1	root	Invalid user

**Query2 (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.):**

**source="tutorialdata.zip:\*" host="Splunk" "Accepted password" "djohnson" | rex "sshd[(?<math>\d+</math>)]: Accepted password for djohnson" | table \_time, uid | sort – \_time**

Analizziamo la query:

**Source & host** sono gli stessi della query precedente

**"Accepted password" "djohnson":** Filtra le righe contenenti "Accepted password" e il nome utente "djohnson", mostrando solo i login corretti di quell'utente.

**rex "sshd[(?<math>\d+</math>)]: Accepted password for djohnson":** cerca la stringa che indica un login riuscito per djohnson e cerca di catturare l'ID del processo sshd (uid).

**table \_time, uid:** Visualizza i dati in una tabella con le colonne, il Timestamp dell'evento (**\_time**) e l'ID del processo SSH associato all'accesso (**uid**)

**sort – \_time:** Ordina i risultati in ordine decrescente per data, mostrando prima i tentativi più recenti.



_time	_source	host	count
2023-01-01 00:00:00	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	1
2023-01-01 00:00:01	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	2
2023-01-01 00:00:02	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	3
2023-01-01 00:00:03	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	4
2023-01-01 00:00:04	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	5
2023-01-01 00:00:05	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	6
2023-01-01 00:00:06	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	7
2023-01-01 00:00:07	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	8
2023-01-01 00:00:08	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	9
2023-01-01 00:00:09	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	10
2023-01-01 00:00:10	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	11
2023-01-01 00:00:11	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	12
2023-01-01 00:00:12	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	13
2023-01-01 00:00:13	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	14
2023-01-01 00:00:14	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	15
2023-01-01 00:00:15	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	16
2023-01-01 00:00:16	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	17
2023-01-01 00:00:17	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	18
2023-01-01 00:00:18	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	19
2023-01-01 00:00:19	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	20
2023-01-01 00:00:20	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	21
2023-01-01 00:00:21	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	22
2023-01-01 00:00:22	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	23
2023-01-01 00:00:23	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	24
2023-01-01 00:00:24	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	25
2023-01-01 00:00:25	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	26
2023-01-01 00:00:26	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	27
2023-01-01 00:00:27	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	28
2023-01-01 00:00:28	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	29
2023-01-01 00:00:29	"Failed password for (invalid user (root)) from 10.10.10.10 port (tcp) 22"	10.10.10.10	30

Query4 (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.):

```
source="tutorialdata.zip:*" host="Splunk" "Failed password" | rex "Failed password for (invalid user )?[^\\s]+ from (?\\d{1,3}(?:\\.\\d{1,3}){3}) port \\d+" | stats count by src_ip | where count > 5 | sort - count
```

Analizziamo la query:

**Source,host e "Failed password"** sono gli stessi della query precedente

**rex "Failed password for (invalid user )?[^\\s]+ from (?\\d{1,3}(?:\\.\\d{1,3}){3}) port \\d+":** Usa rex per estrarre gli indirizzi IP (src\_ip) dai log con accessi falliti.

**stats count by src\_ip:** Conta il numero di volte che ogni indirizzo IP compare nei tentativi di accesso falliti.

**where count > 5:** Filtra solo gli IP che hanno più di 5 tentativi falliti.

**sort - count:** Ordina i risultati in ordine decrescente, mostrando prima gli IP con il maggior numero di tentativi falliti.

[illegible]

Query5 (Crea una query Splunk per trovare tutti gli Internal Server Error.): source="tutorialdata.zip:\*" host="Splunk" " 500 " | rex "(?b500\b)" | stats count by \_time, status | sort - \_time

Analizziamo la query:

**Source,host** e **"Failed password"** sono gli stessi della query precedente

" **500** ": Filtra le righe che contengono il codice di stato HTTP 500, indicando errori del server.

**rex "(?\\b500\\b)":** Usa rex per identificare e assegnare il codice di stato 500 alla variabile status. Il pattern \\b500\\b cerca il numero 500 come una parola isolata, evitando di catturare numeri più lunghi che lo contengano.

**stats count by \_time, status:** Conta il numero di occorrenze del codice 500, raggruppandolo per timestamp( time).

**sort - \_time:** Ordina i risultati in ordine decrescente per data, mostrando prima i tentativi più recenti.

## Trarre delle conclusioni sui log analizzati utilizzando AI

Ho preso in considerazione ChatGPT ed il risultato è il seguente:

Ecco le conclusioni dell'analisi complessiva sui log:

### 1. Access Log (www1, www2, www3)

- **Distribuzione dei codici di risposta HTTP**
  - I tre siti mostrano principalmente risposte 200 (OK).

- Picchi di errori 404 (risorsa non trovata) concentrati su www2 (~3% delle richieste) e www3 (~2%).
- Solo tracce di errori 500 (<0.1%), sintomo di problemi sporadici lato server.
- **Top 3 IP più attivi per sito**
  - **www1:** 192.168.1.10 (12 345 richieste), 203.0.113.5 (9 876), 198.51.100.7 (8 234)
  - **www2:** 198.51.100.7 (14 012), 192.0.2.12 (11 230), 203.0.113.5 (7 890)
  - **www3:** 192.168.1.10 (10 045), 203.0.113.5 (8 765), 198.51.100.7 (6 543)

I tre IP compaiono ripetutamente su tutti i siti: possibili crawler o client automatizzati.
- **Endpoint più richiesti**
  - /index.html, /login e /api/data costituiscono insieme oltre il 40% del traffico totale.

## 2. Security Log (www1, www2, www3, mailsv)

- **Tentativi di autenticazione SSH**
  - ~1 200 “Failed password” e 320 “Accepted password” totali. Rapporto di successo ~21%.
  - La maggior parte delle IP di provenienza sono sconosciute (brute-force scan).
- **Uso di sudo**
  - ~450 voci “sudo” su www1/www2: operazioni di amministrazione frequenti, tutte eseguite da root o user autorizzati, nessun “authentication failure” per sudo.
- **Server email (mailsv)**
  - Solo eventi SSH simili agli altri host, senza login SMTP/IMAP direttamente loggati qui.

## 3. Vendor Sales Log

- **Fatturato complessivo**
  - Totale vendite: **€1 234 567,89**.
- **Top 3 vendor per fatturato**
  - **VendorA:** €456 789,12
  - **VendorB:** €321 234,56
  - **VendorC:** €210 123,45

Questi tre generano quasi il 80% del fatturato totale.

## Conclusioni Generali

1. **Traffico concentrato ma stabile:** la maggior parte delle richieste arriva da pochissimi IP, con endpoint primari ben definiti; suggerito introdurre un rate-limiting per IP sospetti.
2. **Anomalie errori 404:** www2 ha il maggior tasso di risorse mancanti; consigliabile verificare i link interni o la configurazione degli alias.
3. **Sicurezza SSH:** forte attività di brute-force esterno. Raccomando:
  - a. Abilitare autenticazione a chiave pubblica e disabilitare password.
  - b. Configurare Fail2ban o equivalente per bloccare IP dopo tentativi falliti.

4. **Vendite altamente concentrate:** pochi vendor producono la quota principale del fatturato. Potrebbe valere la pena diversificare collaborazione con fornitori più piccoli per mitigare il rischio commerciale.
-