**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

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

* 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

Immagine che contiene schermata, testo, software, Software multimediale

Descrizione generata automaticamente

* 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

Immagine che contiene schermata, testo, software, Software multimediale

Descrizione generata automaticamente

* 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

Immagine che contiene schermata, testo, software, Software multimediale

Descrizione generata automaticamente

* Quinta query

index="tutorial\_data" ("error" OR "500")

| table \_time host \_raw

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

* 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 si che non si creino problemi di alcun tipo (che non si portino avanti soprattutto).