Corso Cyber Security & Ethical hacking
Studente: Adjetey Isabelle

Progetto Fine M6

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.

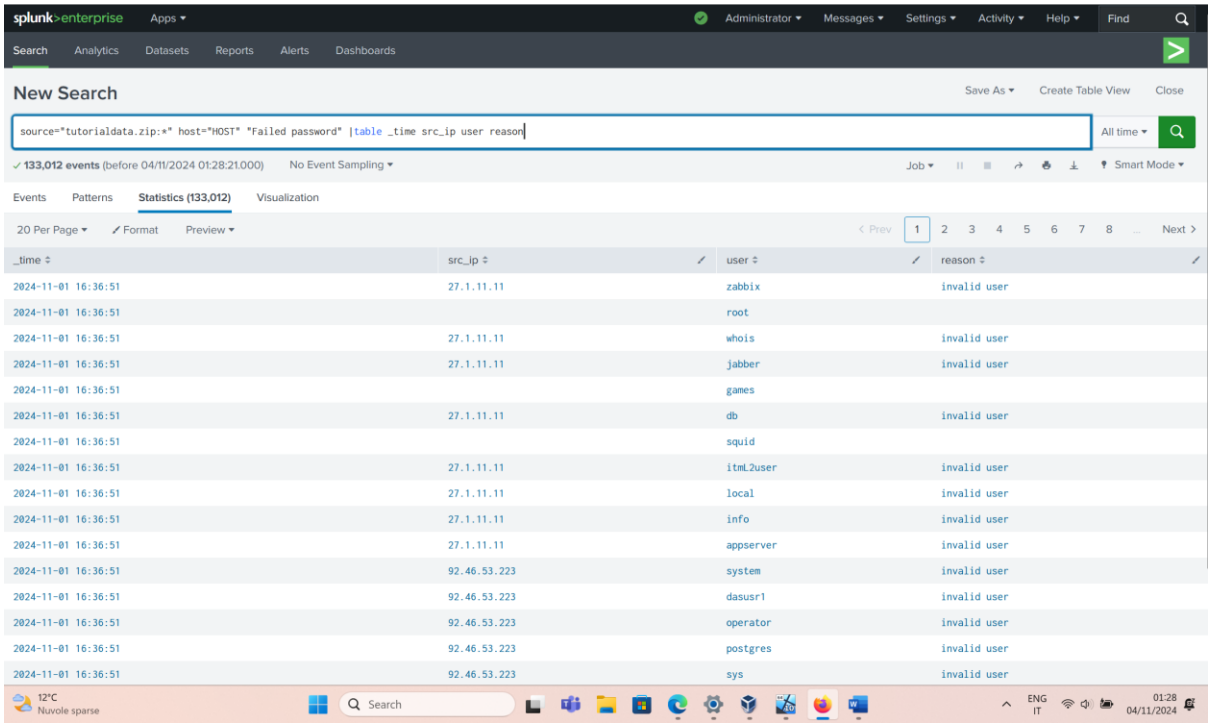
● Crea una query Splunk per trovare tutti gli Internal Server Error.

Trarre delle conclusioni sui log analizzati utilizzando AI.

Corso Cyber Security & Ethical hacking
Studente: Adjetey Isabelle

1 . 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.

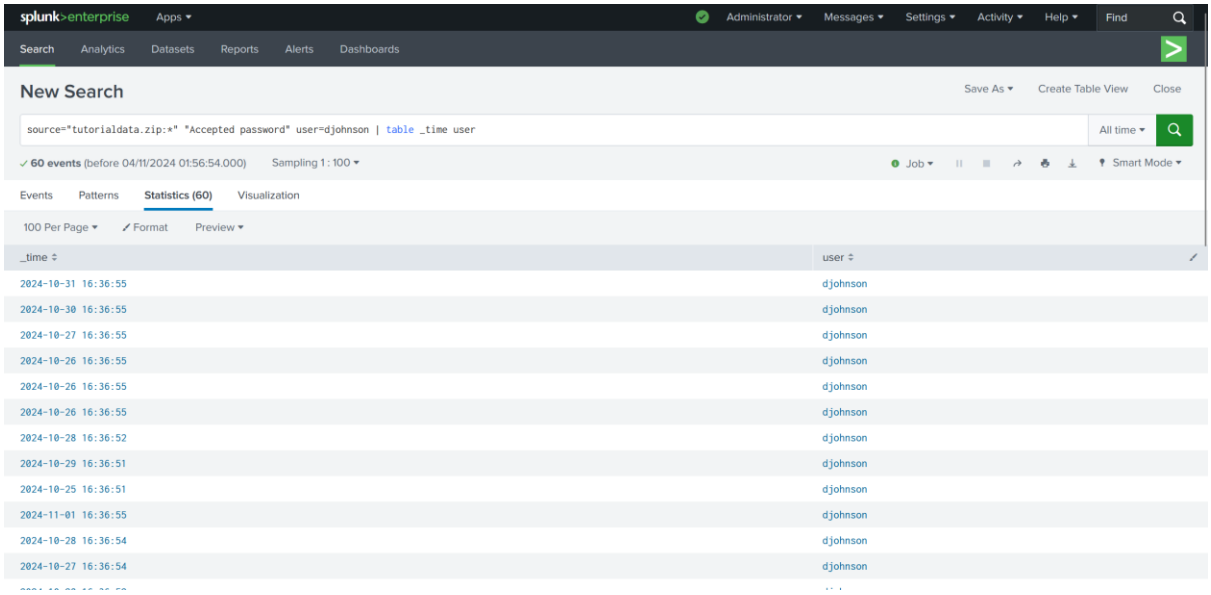
source="tutorialdata.zip:*" host="HOST" "Failed password" |table _time src_ip user reason



2. 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

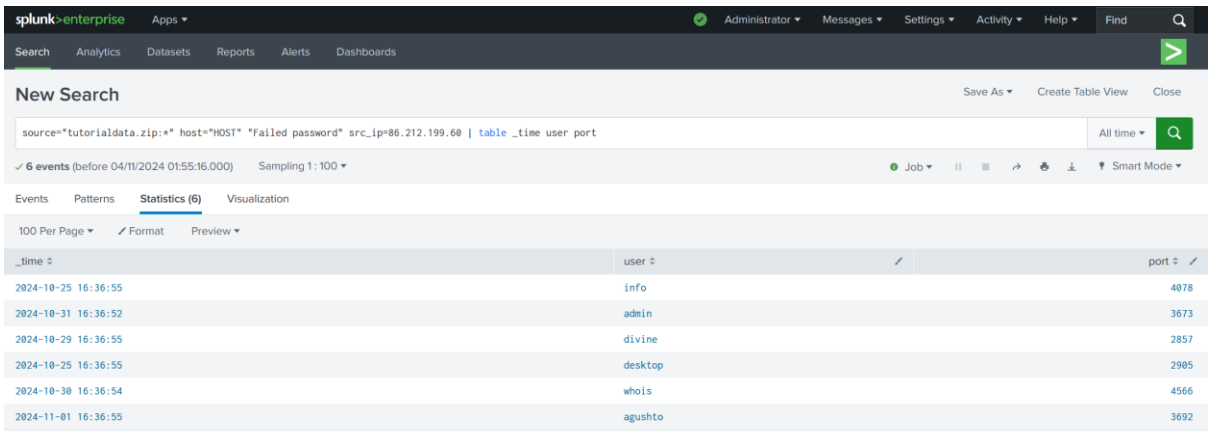
source="tutorialdata.zip:*" "Accepted password" user=djohnson | table _time user

Corso Cyber Security & Ethical hacking
Studente: Adjetey Isabelle



3. 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.

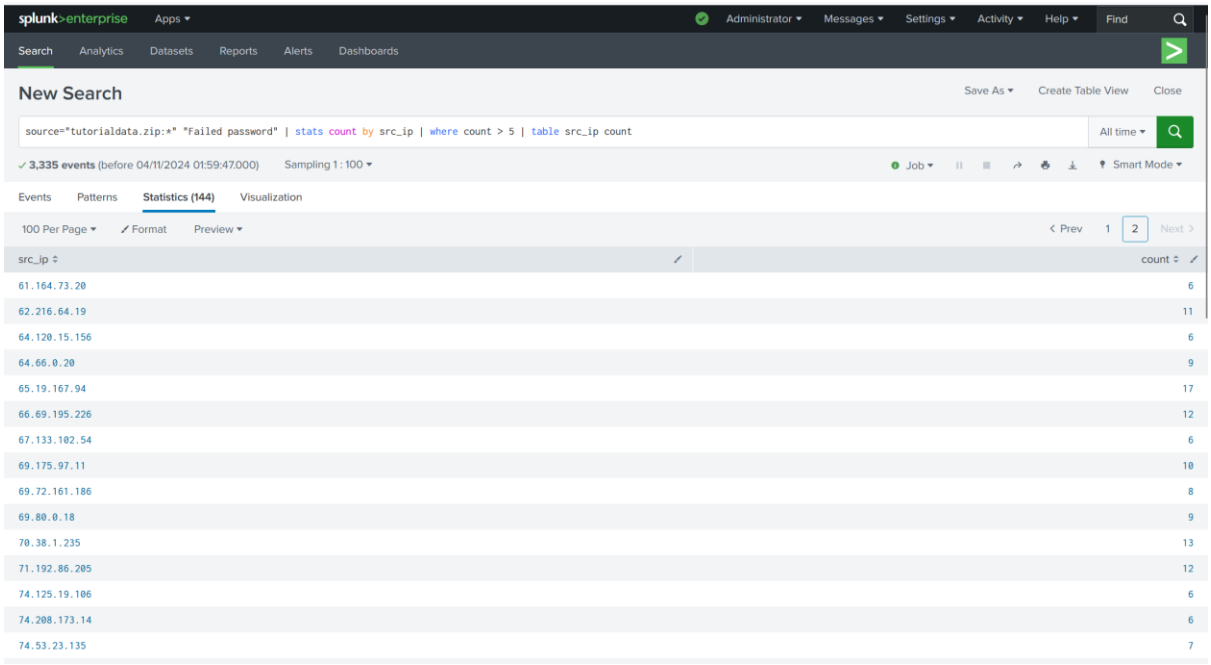
source="tutorialdata.zip:*" host="HOST" "Failed password" src_ip=86.212.199.60 | table _time user port



4. 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.

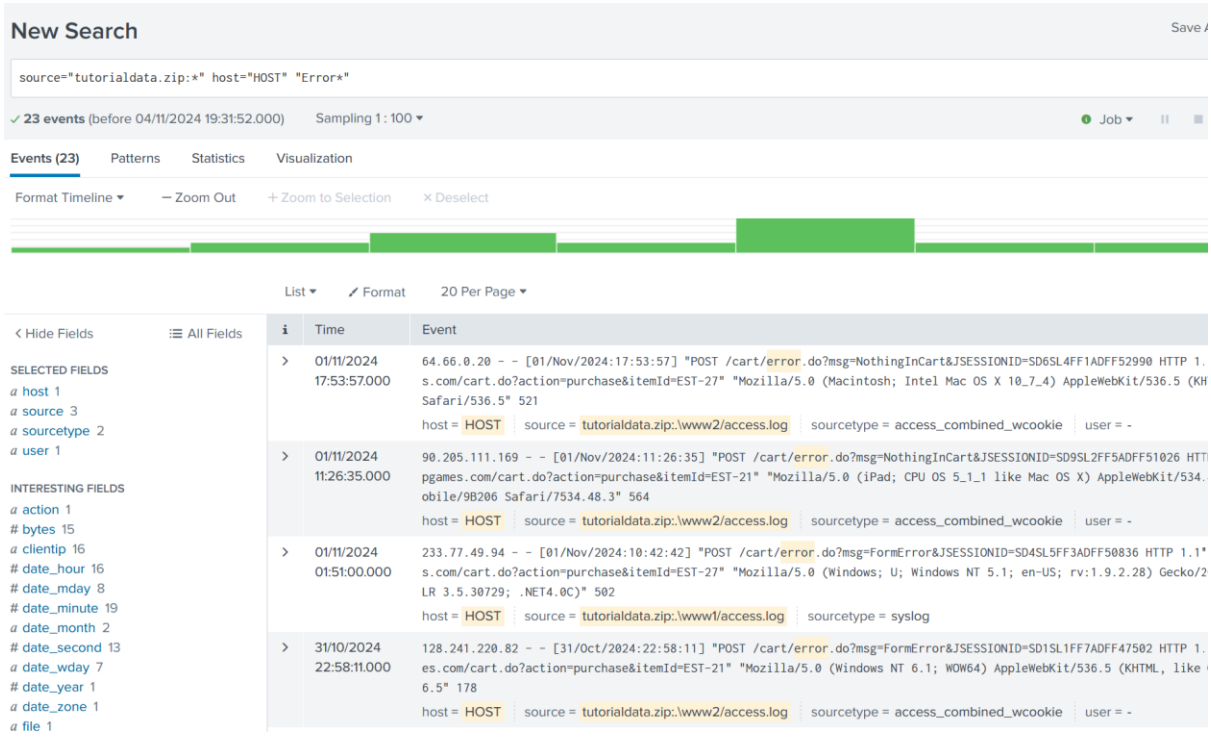
source="tutorialdata.zip:*" "Failed password" | stats count by src_ip | where count > 5 | table src_ip count

Corso Cyber Security & Ethical hacking
Studente: Adjetey Isabelle



5. Query Splunk per trovare tutti gli Internal Server Error

source="tutorialdata.zip:*" host="HOST" "Error*"



Conclusioni sui log analizzati

Dall'analisi dei log, possiamo trarre diverse conclusioni:

- **Tentativi di Accesso Falliti:** La presenza di numerosi tentativi di accesso falliti può indicare attacchi di forza bruta. È importante monitorare e bloccare indirizzi IP che mostrano attività sospette.
- **Accessi SSH:** La registrazione delle sessioni SSH con successo, in particolare per utenti specifici come "djohnson", aiuta a verificare l'integrità e la sicurezza degli accessi remoti.
- **Attività da IP Specifici:** Monitorare i tentativi di accesso falliti provenienti da un singolo IP, come "86.212.199.60", è cruciale per identificare e mitigare potenziali minacce.
- **Errori del Server:** Gli Internal Server Error possono indicare problemi di configurazione o potenziali vulnerabilità nei servizi esposti. Un'analisi approfondita di questi errori è necessaria per garantire la stabilità e la sicurezza dell'infrastruttura.

L'uso di strumenti di analisi dei log come Splunk facilita l'identificazione di anomalie e la risposta a incidenti di sicurezza in tempo reale.