

Analisi log di accesso



W24D4.pdf
PDF

mi puoi trarre delle conclusioni da questo file?



Il file che hai caricato contiene una serie di esercizi che riguardano l'analisi dei log di accesso e l'individuazione di eventi specifici tramite query, presumibilmente in un sistema come Splunk o simile. Ecco le conclusioni principali tratte dal documento:

1. **Accessi con password errata:** Viene descritta una query per identificare i tentativi falliti di accesso usando "Failed Password". Include anche l'uso di timestamp e indirizzi IP, e la possibilità di estrarre il motivo del fallimento con un'espressione regolare.
2. **Sessioni di accesso riuscite per un utente specifico:** La query cerca accessi con successo usando "Accepted Password" e filtra per l'utente "djohnson", mostrando il timestamp e un ID utente estratto con una regex.
3. **Accessi falliti da un IP specifico:** La query identifica tentativi di accesso non riusciti provenienti da un indirizzo IP specifico, mostrando timestamp, nome utente e numero di porta.
4. **IP con più di 5 tentativi falliti:** Si descrive una query per elencare gli indirizzi IP con più di 5 tentativi di accesso falliti. L'uso di regex cattura gli IP, mentre un'aggregazione (stats count) e un filtro (where) trovano quelli con più tentativi.
5. **Errori del server interno:** Per filtrare errori HTTP con codici 5xx (es., 500, 502), si utilizza una query che raggruppa per codice di stato, host e sorgente, ordinando eventualmente per numero di occorrenze.

Queste query e approcci sono utili per attività di **monitoraggio della sicurezza informatica**, individuazione di tentativi di **accesso sospetti**, e **analisi degli errori di sistema**. Se hai bisogno di ulteriori dettagli o suggerimenti su come ottimizzare queste analisi, fammelo sapere!