# PROGETTO DI FINE MODULO M6

**1) 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.**

```
index=main sourcetype=secure.log "Failed password"
| rex "Failed password for (invalid user )?(?<username>\S+) from
(?<src_ip>\d{1,3}(?:\.\d{1,3}){3})"
| eval reason="Failed password"
| table _time, src_ip, username, reason
```

**Spiegazione:**

Questa query cerca tutti i messaggi contenenti "Failed password" nei log di sicurezza. Estrae il nome utente, l'indirizzo IP di origine e aggiunge una colonna con il motivo dell'errore.

**2) 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.**

```
index=main sourcetype=secure.log "session opened for user djohnson"
| rex "session opened for user (?<username>\w+) by
\((uid=(?<uid>\d+))\)"
| table _time, username, uid
```

**Spiegazione:**

La query filtra i messaggi che indicano l'apertura di una sessione SSH per l'utente 'djohnson' ed estrae l'ID utente (uid) dal messaggio.

**3) 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.**

```
index=main sourcetype=secure.log "Failed password" "86.212.199.60"
| rex "Failed password for (invalid user )?(?<username>\S+) from \S+
port (?<port>\d+)"
| table _time, username, port
```

**Spiegazione:**

Questa query cerca tentativi falliti provenienti dallo specifico indirizzo IP e mostra il nome utente e la porta.

**4) 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.**

```
index=main sourcetype=secure.log "Failed password"
| rex "from (?<src_ip>\d{1,3}(?:\.\d{1,3}){3})"
| stats count by src_ip
| where count > 5
```

**Spiegazione:**

La query raggruppa i tentativi falliti per indirizzo IP e restituisce solo quelli con più di 5 tentativi.

**5) Crea una query Splunk per trovare tutti gli Internal Server Error.**

```
index=main sourcetype=access.log "500"
| rex "(?<status>500)"
| table _time, status, host, uri_path
```

**Spiegazione:**

Questa query cerca errori HTTP 500 nei log di accesso, indicando errori interni del server.

**6) Trarre delle conclusioni sui log analizzati utilizzando AI.**

**Conclusioni basate sull'analisi dei log (con supporto AI)**

1. **Tentativi di accesso falliti frequenti**
    - I log mostrano un numero significativo di messaggi con "Failed password", spesso da parte di utenti inesistenti (invalid user), indicando probabili tentativi di brute-force.
    - Alcuni IP si ripetono nei tentativi, suggerendo che gli attaccanti stanno automatizzando gli accessi da fonti specifiche.
2. **Accessi riusciti – Sorveglianza utenti specifici**

- È stato rilevato che l'utente "djohnson" ha aperto correttamente sessioni SSH. Questo suggerisce che l'account è attivo e utilizzato, ma anche che dovrebbe essere monitorato in caso di escalation di privilegi o accessi anomali.

3. **Minaccia mirata da IP specifici**
    - L'indirizzo IP 86.212.199.60 è coinvolto in tentativi di accesso falliti. Questo comportamento mirato potrebbe indicare un attaccante consapevole dell'ambiente o in fase di ricognizione.
4. **Comportamento sospetto ripetuto**
    - Alcuni indirizzi IP hanno superato il limite di 5 tentativi falliti: questo è un chiaro indicatore di attacco (IOC). Questi IP andrebbero inseriti in una lista di blocco temporanea o permanente (blacklist).
5. **Errori di tipo 500 nel server web**
    - La presenza di errori 500 nei log di accesso web suggerisce malfunzionamenti lato server. Potrebbero essere causati da problemi di configurazione, bug del codice, o in alcuni casi, tentativi di exploit.

---

🛡️ **Raccomandazioni (generate con supporto AI):**

- Implementare meccanismi di blocco IP automatico dopo N tentativi falliti.
- Abilitare il fail2ban per proteggere SSH e servizi esposti.
- Verificare l'integrità delle applicazioni web a fronte di errori HTTP 500 ricorrenti.
- Rivedere gli account attivi (come djohnson) e applicare criteri di least privilege.
- Attivare alert in Splunk per pattern anomali ricorrenti (tentativi falliti, errori 500, accessi non in orari lavorativi).