Report Splunk

1. Introduzione

1.1 Scopo del documento

Fornire un'analisi strutturata delle attività SSH e HTTP rilevate nei log Splunk, evidenziando pattern sospetti e possibili vulnerabilità.

1.2 Sintesi dell'analisi

Sono stati analizzati tentativi di accesso falliti, connessioni riuscite per l'utente djohnson, tentativi da IP specifico e errori HTTP 500.

2. Metodologia

2.1 Origine dei dati

Dati esportati da Splunk tramite query SPL personalizzate.

2.2 Periodo di riferimento

Intervallo 'Sempre', comprendente tutti gli eventi registrati.

2.3 Struttura delle query SPL

Le query sono state strutturate per filtrare, estrarre campi e aggregare dati per IP, utente e motivo di fallimento.

3. Tentativi di accesso falliti – Completi

3.1 Query SPL

```
index=* "Failed password"
| rex "Failed password for( invalid user)? (?<username>\S+)"
| rex "from (?<src_ip>\d{1,3}(?:\.\d{1,3}){3})"
| eval reason=if(match(_raw,"invalid user"),"invalid user","password
incorrect")
| table _time, src_ip, username, reason
```

3.2 Spiegazione della Query

index=* "Failed password": Filtra tutti gli eventi contenenti la stringa.

rex ... username: Estrae il nome utente.

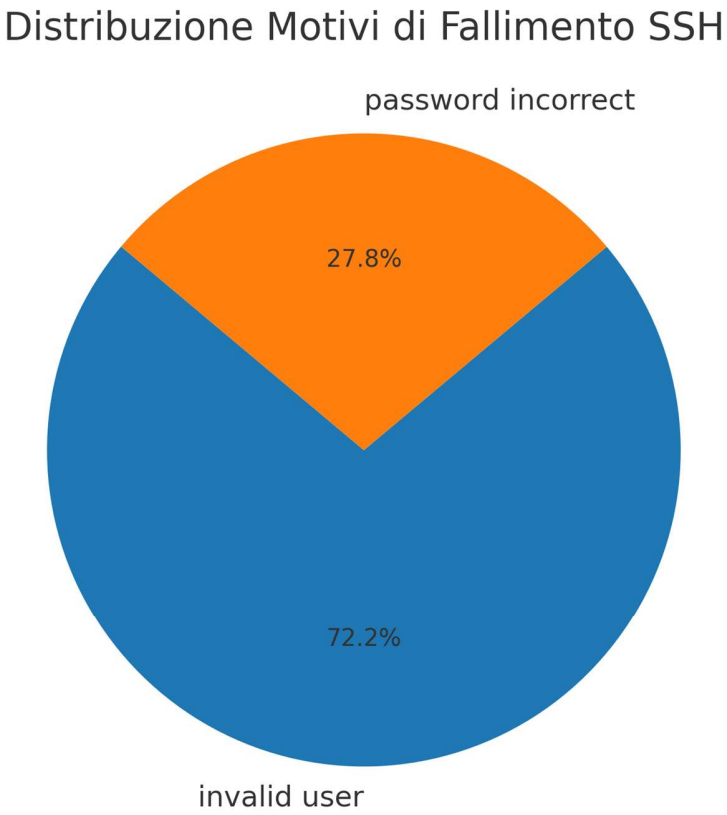
rex ... src_ip: Estrae l'indirizzo IP sorgente.

eval reason=...: Classifica il motivo come invalid user o password incorrect.

table ...: Mostra solo i campi rilevanti.

3.3 Risultati e Osservazioni

Sono stati rilevati **133012** tentativi falliti. La distribuzione mostra prevalenza di *'invalid user'*.



4. Accessi riusciti SSH – Utente djohnson

4.1 Query SPL

```
index=* "Accepted password" "djohnson"
| rex "for (?<username>\S+) from (?<src_ip>\d{1,3}(?:\.\d{1,3}){3})"
| search username="djohnson"
```

```
| table _time, username, src_ip
| sort - _time
```

4.2 Spiegazione della Query

Filtra eventi Accepted password con djohnson.

rex.... : Estrae username e IP sorgente.

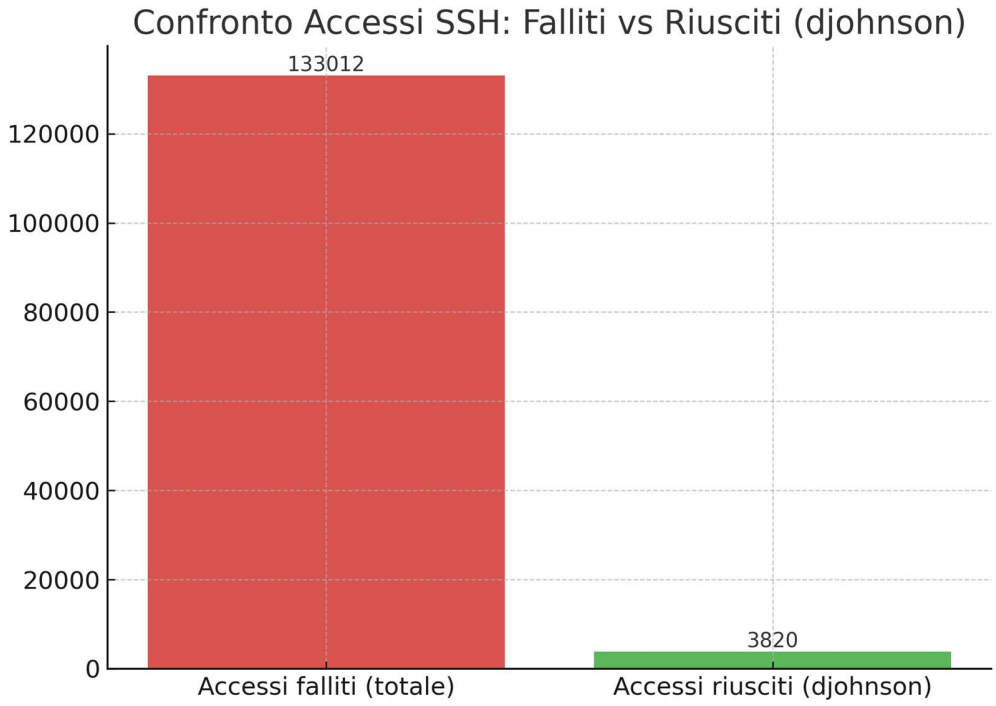
search username=...: Conferma che sia djohnson.

table: Mostra timestamp, username e IP.

sort: Ordina in ordine decrescente.

4.3 Risultati e Osservazioni

Sono state registrate **3820** connessioni riuscite.



5. IP con più di 5 tentativi falliti

5.1 Query SPL

```
index=* "Failed password"
| rex "from (?<src_ip>\d{1,3}(?:\.\d{1,3}){3})"
| stats count AS tentativi by src_ip
| where tentativi > 5
| sort - tentativi
```

5.2 Spiegazione della Query

rex: Estrae l'IP sorgente.

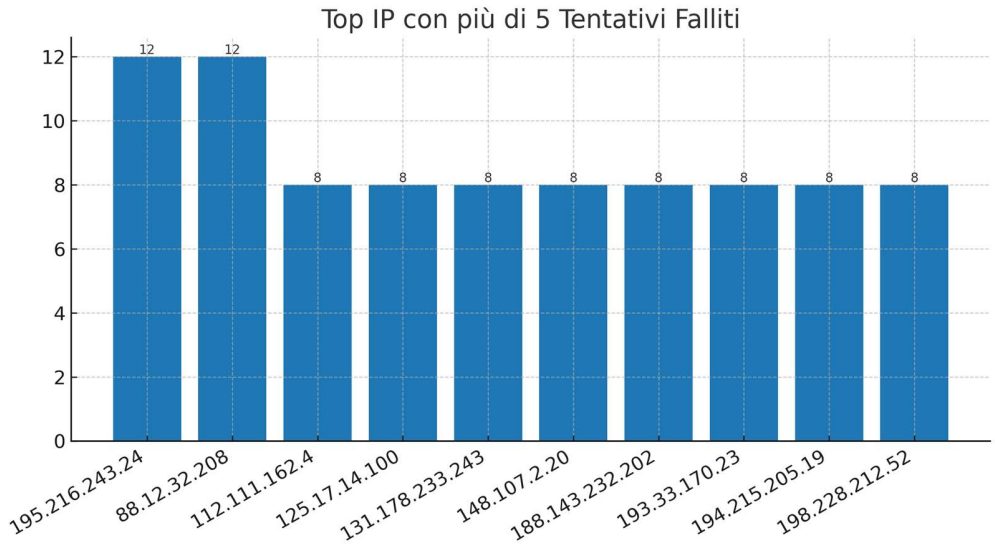
stats count: Calcola tentativi per IP.

where tentativi > 5: Filtra IP più attivi.

sort: Ordina per numero di tentativi.

5.3 Risultati e Osservazioni

Classifica dei primi 10 IP che hanno superato i 5 tentativi falliti.



6. Errori HTTP 500

6.1 Query SPL

```
index=* ("Internal Server Error" OR "500")
| table _time, host, source, sourcetype, _raw
| sort - _time
```

6.2 Spiegazione della Query

Filtro: Cerca Internal Server Error o 500.

table: Mostra campi essenziali.

sort: Ordina in ordine decrescente.

6.3 Risultati e Osservazioni

Totale eventi HTTP 500: 3124