

Splunk Enterprise interface showing search results for the query: `source="tutorialdata.zip:*" sourcetype="*" "session opened" "djohnson"`. The results show multiple "session opened" events for user "djohnson" with uid=0, indicating frequent access attempts.

Evento
Thu Nov 01 2024 04:36:40 mailsv1 sshd[60445]: pam_unix(sshd:session): session opened for user djohnson by (uid=0)
Thu Nov 01 2024 04:36:40 mailsv1 sshd[87066]: pam_unix(sshd:session): session opened for user djohnson by (uid=0)
Thu Nov 01 2024 04:36:40 mailsv1 sshd[5860]: pam_unix(sshd:session): session opened for user djohnson by (uid=0)
Thu Nov 01 2024 04:36:40 mailsv1 sshd[71798]: pam_unix(sshd:session): session opened for user djohnson by (uid=0)
Thu Nov 01 2024 04:36:40 mailsv1 sshd[54980]: pam_unix(sshd:session): session opened for user djohnson by (uid=0)
Thu Nov 01 2024 04:36:40 mailsv1 su: pam_unix(su:session): session opened for user root by djohnson(uid=0)

Conclusioni ChatGPT:

- **Accesso frequente con l'utente 'djohnson':** Gli eventi indicano che 'djohnson' ha aperto diverse sessioni nello stesso intervallo di tempo (01/11/2024 04:36:40). È insolito che molteplici sessioni vengano aperte simultaneamente dallo stesso utente, il che potrebbe essere indicativo di un comportamento anomalo o di un processo automatizzato.
- **UID 0 suggerisce privilegi elevati:** Gli eventi mostrano che le sessioni sono state aperte con uid=0, che generalmente corrisponde all'utente root o ad accessi con privilegi di amministratore. Questo suggerisce che 'djohnson' ha privilegi elevati o ha eseguito operazioni che richiedono l'accesso root. Se questo accesso non è previsto, potrebbe rappresentare un rischio per la sicurezza.
- **Possibile compromissione dell'account:** Dato che 'djohnson' sta effettuando molteplici accessi con UID 0, potrebbe essere utile verificare se questi accessi sono legittimi. Se 'djohnson' non è un account che dovrebbe avere privilegi amministrativi o se l'utente non ha effettuato manualmente questi accessi, è possibile che l'account sia stato compromesso.
- **Relazione con tentativi di brute-force precedenti:** In uno degli screenshot precedenti, abbiamo visto che ci sono stati tentativi di accesso falliti provenienti da un IP sospetto (86.212.199.60). È importante verificare se questi accessi di 'djohnson' potrebbero essere collegati, soprattutto se c'è stato un accesso riuscito in seguito a tentativi di brute-force su account di sistema.

Azioni consigliate:

- **Verifica dell'attività dell'utente 'djohnson':** Controllare con il team o con 'djohnson' (se è un utente reale) se ha effettivamente effettuato questi accessi, oppure se erano previsti automatismi che potrebbero averli generati.
- **Analisi approfondita dei log:** Controllare i log per eventi aggiuntivi correlati, ad esempio modifiche di sistema o trasferimenti di dati eseguiti durante queste sessioni, per assicurarsi che non siano state eseguite operazioni dannose.
- **Considerare la revisione dei privilegi:** Se 'djohnson' non è un utente che dovrebbe avere privilegi root, potrebbe essere opportuno rivedere i privilegi assegnati per garantire la conformità con le policy di sicurezza dell'organizzazione.

- **Configurare alert per accessi sospetti:** Implementare un sistema di notifica per gli accessi simultanei con UID elevato o per attività di accesso insolite per account privilegiati.

In sintesi, questa schermata indica attività sospette con l'utente 'djohnson', caratterizzate da accessi simultanei con privilegi 'root'. È importante verificare la legittimità di questi eventi per garantire la sicurezza del sistema ed evitare possibili compromissioni.