Progetto - Splunk

Indice

1. Introduzione

Questo report presenta un'analisi approfondita dei log di sistema raccolti attraverso Splunk, con l'obiettivo di identificare potenziali minacce alla sicurezza e attività sospette all'interno della nostra infrastruttura IT. L'analisi si concentra su vari aspetti della sicurezza, tra cui tentativi di accesso non autorizzato, attività di ricognizione e potenziali attacchi mirati.

2. Sintesi Esecutiva

L'analisi dettagliata dei log dei nostri sistemi ha portato alla luce alcune attività potenzialmente malevole che suggeriscono tentativi di attacco intenzionali e mirati. Questi eventi evidenziano rischi per la sicurezza dei nostri dati e infrastrutture. Le attività sospette rilevate comprendono tentativi di accesso non autorizzato tramite attacchi di forza bruta su SSH, attività di ricognizione avanzata tramite enumerazione di sessioni e processi, automazione anomala di azioni sul sito web e possibili attacchi di credential stuffing e SQL injection.

3. Metodologia

L'analisi è stata condotta utilizzando Splunk, una piattaforma avanzata per l'analisi dei log. Sono state eseguite query mirate per identificare pattern sospetti nei log di sistema, con particolare attenzione ai tentativi di accesso falliti, alle sessioni SSH, agli errori del server e alle attività anomale sul sito web. Le query Splunk utilizzate sono dettagliate nell'Appendice A.

4. Analisi dei Log

4.1 Tentativi di Accesso Brute Force su SSH

Osservazioni: Nei log di accesso SSH, abbiamo riscontrato diversi tentativi di login falliti che seguono il modello tipico di un attacco di **forza bruta**. Questo attacco mira a ottenere accesso al sistema tentando un gran numero di combinazioni di credenziali. Sono emersi alcuni indirizzi IP ricorrenti, che evidenziano la presenza di bot o attaccanti automatizzati.

4.2 Ricognizione tramite Enumerazione di Sessioni e Processi

Osservazioni: L'analisi dei log ha mostrato diversi accessi che sembrano mirare a raccogliere dettagli su processi e sessioni attivi. Questo pattern è comune in fase di **ricognizione**, quando un attaccante cerca di ottenere informazioni che potrebbero essere utilizzate in un attacco successivo, mirato a sfruttare vulnerabilità specifiche.

4.3 Attività Sospette di Automazione sul Sito Web

Osservazioni: L'analisi dei log HTTP mostra una frequenza sospetta di azioni come "addtocart" e "changequantity," che potrebbero indicare la presenza di bot malevoli. Questi bot potrebbero essere utilizzati per **scraping dei dati** o **frodi tramite azioni automatizzate**, simulando il comportamento di utenti reali.

5. Report Conclusivo

Il report conclusivo include una sintesi dettagliata delle minacce identificate, dei rischi associati e delle azioni raccomandate per mitigare tali rischi. Sono state identificate diverse categorie di attacchi potenziali, tra cui tentativi di accesso brute force, attività di ricognizione, automazione sospetta e possibili attacchi di credential stuffing e SQL injection.

6. Conclusioni e Prossimi Passi

L'analisi dei log rivela che il sistema è stato oggetto di tentativi di attacco su più fronti, suggerendo che la nostra infrastruttura attira attivamente interesse da parte di attaccanti esterni. Per rafforzare la sicurezza dei nostri sistemi e prevenire possibili compromissioni, è cruciale adottare le seguenti misure:

1. **Blocco IP e autenticazione avanzata** per limitare l'accesso SSH a utenti verificati.
2. **Monitoraggio avanzato** delle attività di enumerazione e alerting su azioni sospette.
3. **Controllo e limitazione delle API** e protezione anti-bot sul sito web per ridurre il rischio di automazione malevola e scraping.
4. **Implementazione di meccanismi di difesa** per SQL injection e monitoraggio dei tentativi di credential stuffing.

7. Glossario dei Termini Tecnici

Di seguito sono riportati i principali termini tecnici utilizzati nel report:

- **Brute Force**: Tecnica di attacco che tenta di indovinare password o chiavi provando sistematicamente tutte le possibili combinazioni.
- **SSH (Secure Shell)**: Protocollo di rete crittografico per l'accesso remoto sicuro a sistemi informatici.
- **Credential Stuffing**: Tipo di attacco informatico in cui vengono utilizzate coppie di nomi utente e password rubate per accedere fraudolentemente ad altri account utente.
- **SQL Injection**: Tecnica di attacco che sfrutta vulnerabilità nel codice dell'applicazione per manipolare o recuperare dati dal database.
- **API (Application Programming Interface)**: Set di definizioni e protocolli per la creazione e l'integrazione di software applicativi.
- **CAPTCHA**: Test utilizzato per determinare se l'utente è un essere umano o un computer.
- **2FA (Two-Factor Authentication)**: Metodo di sicurezza che richiede due forme diverse di autenticazione per accedere a un account.

8. Appendici

Appendice A: Query Splunk Utilizzate

A.1 Identificazione dei tentativi di accesso falliti

```
source="tutorialdata.zip:*" sourcetype="secure.log" | searc
h "failed password" | search user
```

A.2 Sessioni SSH aperte con successo per l'utente "djohnson"

```
source="tutorialdata.zip:*" sourcetype="secure.log" | searc
h sshd | search "session opened for user djohnson"
```

A.3 Dettagli delle sessioni SSH aperte per "djohnson"

```
source="tutorialdata.zip:*" sourcetype="secure.log" | rex
"Accepted password for (?<user_id>\\S+)" | where user_id="d
johnson"
| table _time user_id | rename _time as "Timestamp", user_i
d as "ID Utente" | sort - _time
```

A.4 Tentativi di accesso falliti da IP specifico

```
source="tutorialdata.zip:*" sourcetype="secure.log" | searc
h "86.212.199.60" | search "failed" | search user | search
port
```

A.5 Estrazione dettagli tentativi di accesso falliti

```
source="tutorialdata.zip:*" sourcetype="secure.log" | searc
h "86.212.199.60" | search "failed password"
| rex "Failed password for (?:invalid user )?(?<username>
\\S+) from (?<src_ip>\\S+) port (?<port>\\d+)"
| table _time username port | rename _time as "Timestamp",
```

```
username as "Nome Utente", port as "Numero di Porta" | sort
- _time
```

A.6 IP con più di 5 tentativi di accesso falliti

```
source="tutorialdata.zip:*" sourcetype="secure.log" | rex
"Failed password for (?:invalid user )?(?<username>\\S+) fr
om (?<src_ip>\\S+)"
| stats count as attempts by src_ip | where attempts > 5
| table src_ip attempts | rename src_ip as "Indirizzo IP",
attempts as "Numero di Tentativi" | sort - attempts
```

A.7 Log con "Internal Server Error"

```
source="tutorialdata.zip:*" sourcetype="secure.log" | searc
h "HTTP 1.1" "500"
```

A.8 Organizzazione errori "500"

```
source="tutorialdata.zip:*" sourcetype="secure.log" | searc
h "500"
| table _time host uri status | rename _time as "Timestam
p", host as "Host", uri as "URL", status as "Stato" | sort
- _time
```

Appendice B: Esempi di Log Rilevanti

Questa sezione includerebbe esempi specifici di log che hanno evidenziato le attività sospette discusse nel report principale. Per motivi di privacy e sicurezza, i dati sensibili sarebbero oscurati.

Appendice C: Statistiche Dettagliate

Qui verrebbero inserite tabelle e grafici dettagliati che mostrano le statistiche complete relative alle attività sospette rilevate, inclusi:

- Distribuzione temporale dei tentativi di accesso falliti

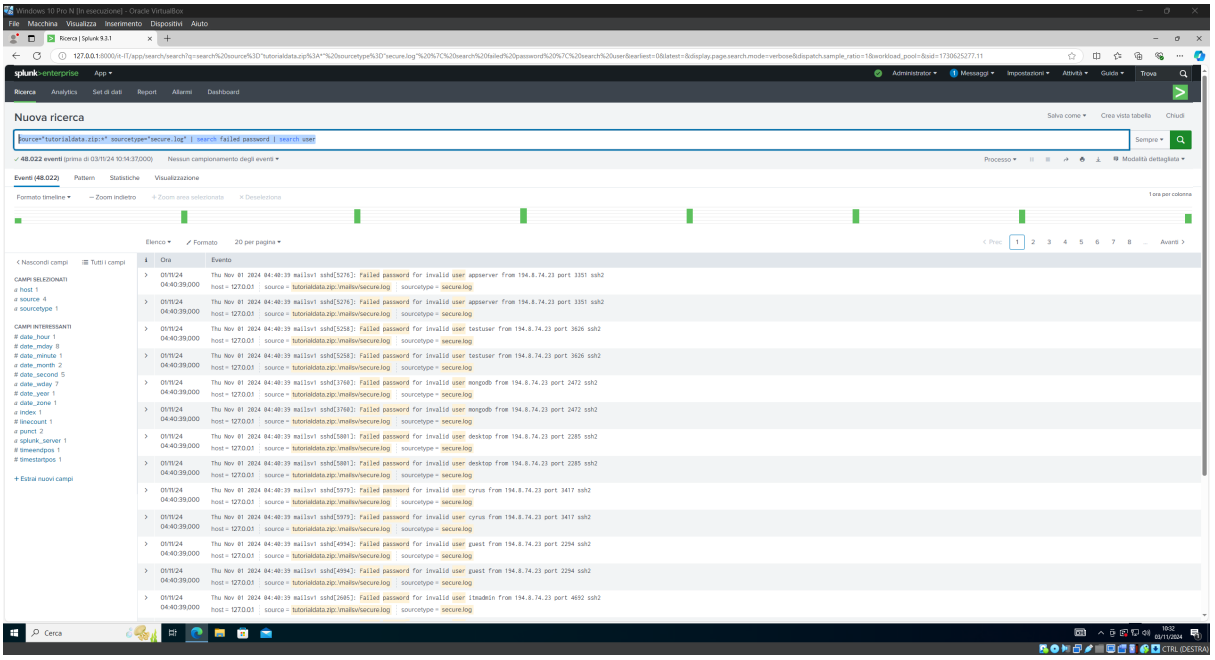
- Top 10 degli indirizzi IP sorgente per tentativi di accesso non autorizzati
- Frequenza degli errori 500 nel tempo
- Distribuzione delle porte utilizzate negli attacchi

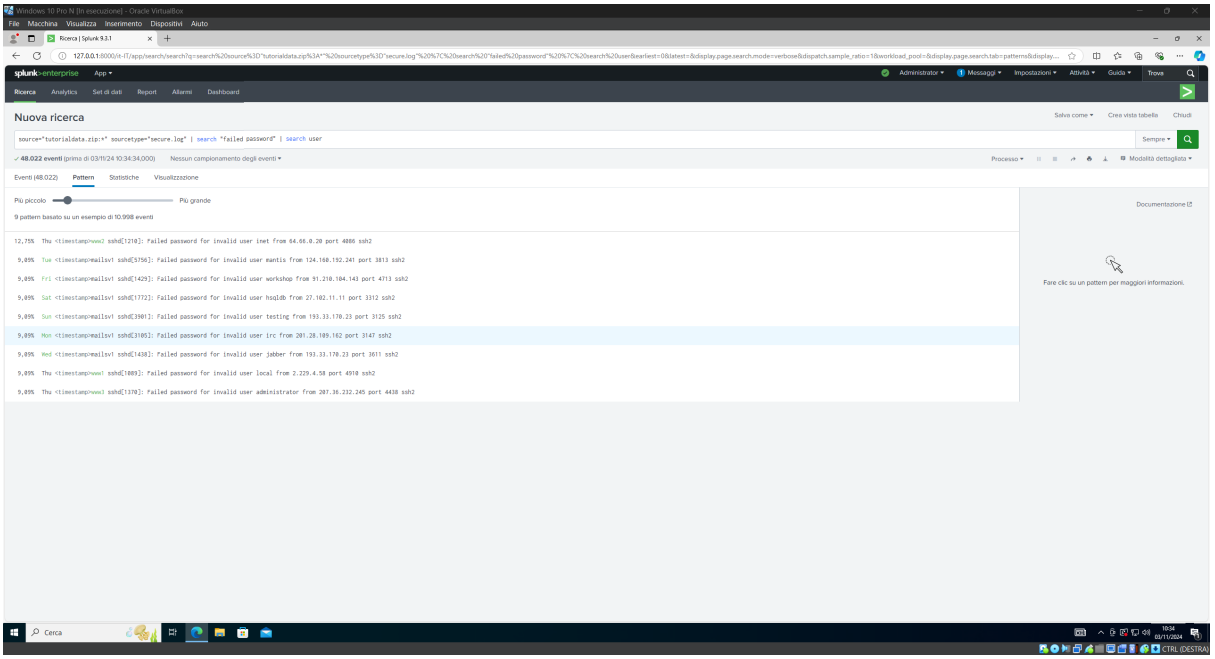
Esecuzione Analisi

1. Identificare tutti i tentativi di accesso falliti "Failed password" per utenti specifici

```
source="tutorialdata.zip:*" sourcetype="secure.log" | searc
h "failed password" | search user
```

- **Descrizione**: Questa query cerca tutti i tentativi di accesso falliti con il messaggio "failed password" e filtra i risultati che contengono il campo `user`. È utile per individuare gli utenti che hanno avuto problemi di accesso.

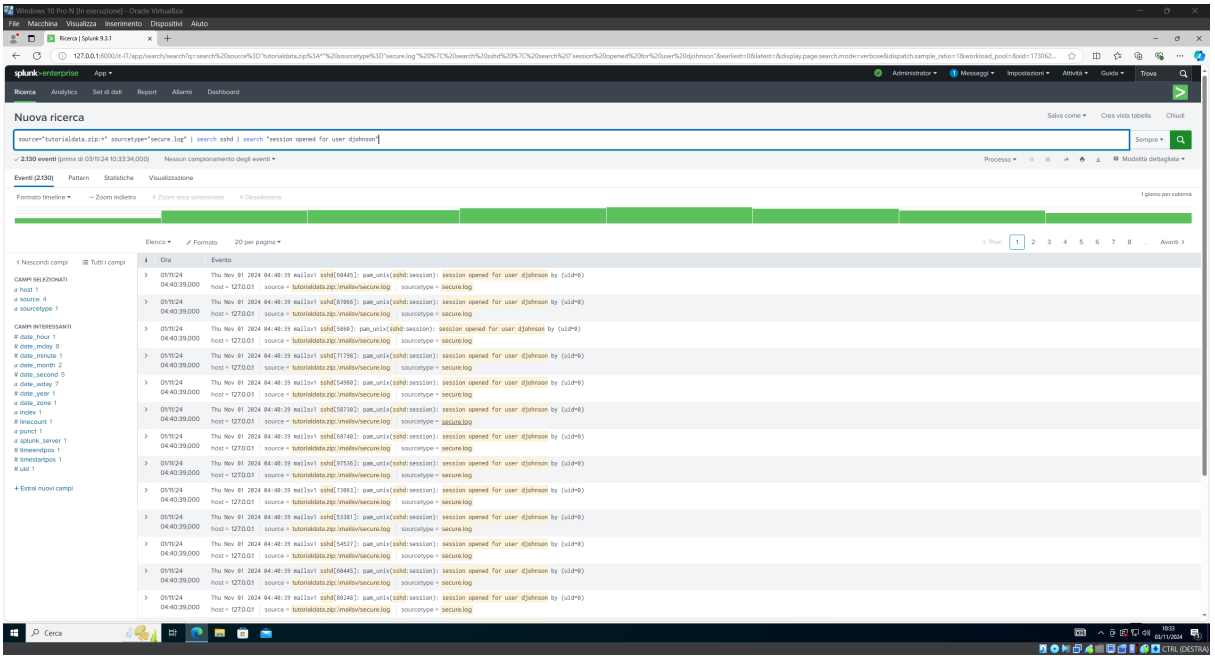


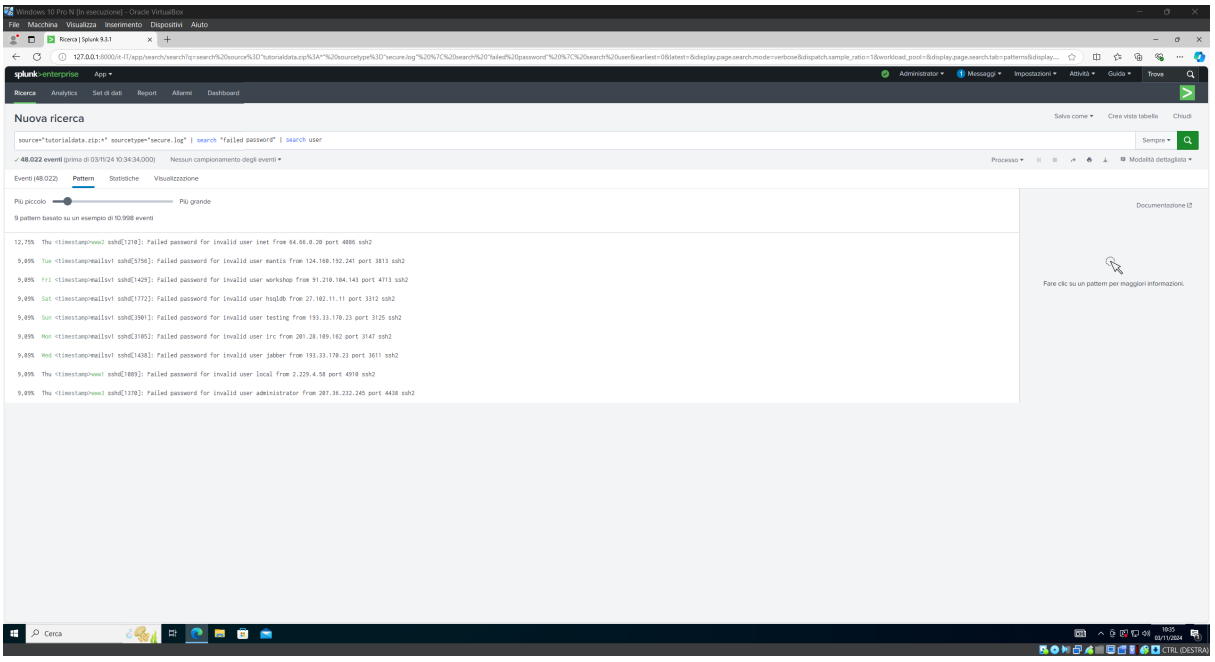


2. Trovare tutte le sessioni SSH aperte con successo per l'utente “djohnson”

```
source="tutorialdata.zip:*" sourcetype="secure.log" | searc
h sshd | search "session opened for user djohnson"
```

- **Descrizione**: Questa query cerca i log del servizio `sshd` e filtra i messaggi che indicano che una sessione SSH è stata aperta con successo per l'utente `djohnson`. Aiuta a identificare quando e quante volte l’utente `djohnson` ha effettuato l’accesso.

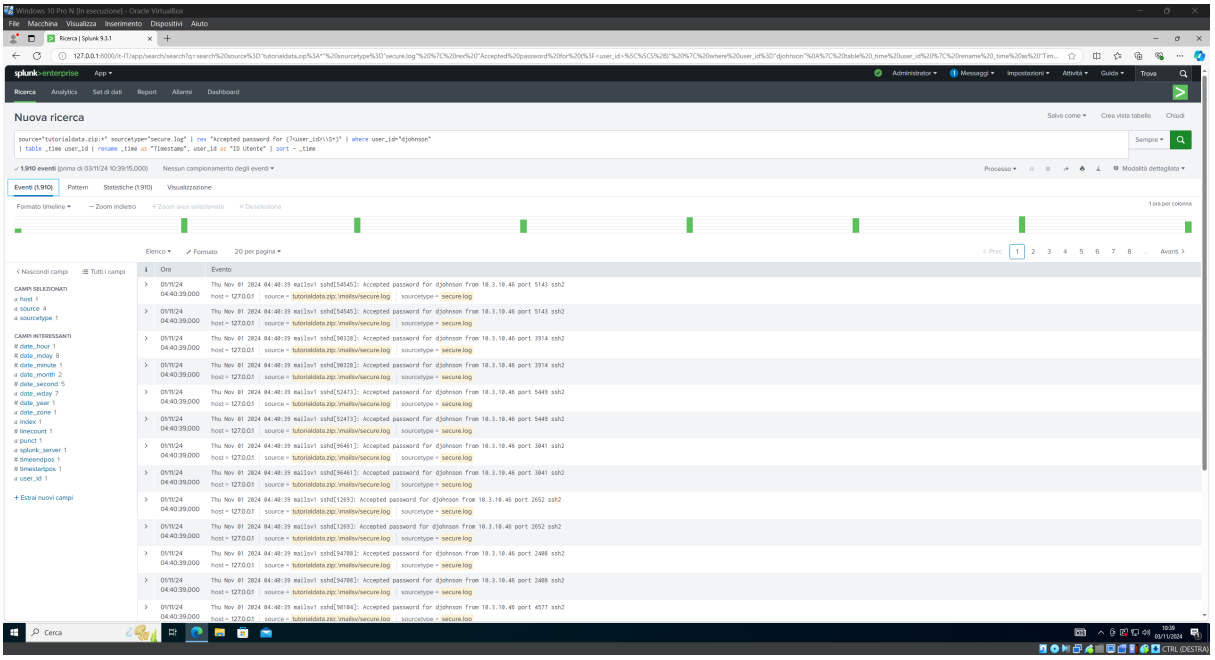




3. Trovare tutte le sessioni SSH aperte con successo per “djohnson” con dettagli

```
source="tutorialdata.zip:*" sourcetype="secure.log" | rex
"Accepted password for (?<user_id>\\S+)" | where user_id="d
johnson"
| table _time user_id | rename _time as "Timestamp", user_i
d as "ID Utente" | sort - _time
```

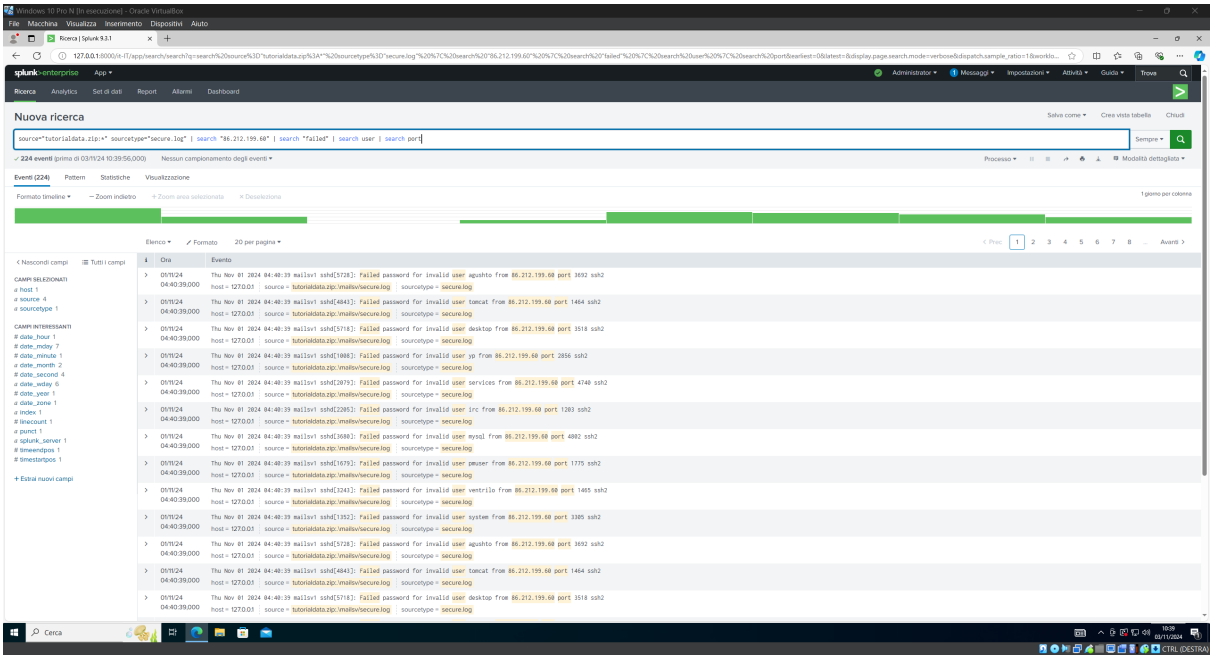
- **Descrizione**: Utilizzando l'espressione `rex`, questa query estrae l'`user_id` da tutti i messaggi che contengono "Accepted password" per `djohnson`. La query ordina i risultati per timestamp e li organizza in una tabella, mostrando il timestamp e l'ID utente.

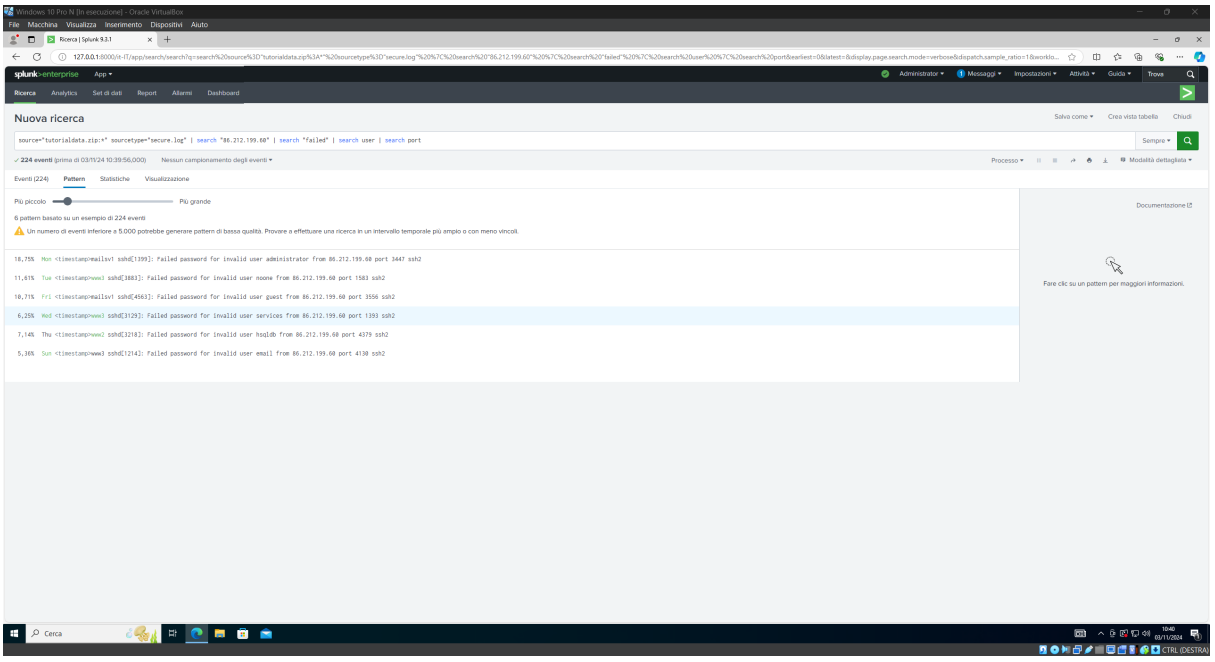


4. Trovare tutti i tentativi di accesso falliti dall'indirizzo IP "86.212.199.60"

```
source="tutorialdata.zip:*" sourcetype="secure.log" | search "86.212.199.60" | search "failed" | search user | search port
```

- **Descrizione**: Questa query filtra i log per individuare i tentativi di accesso falliti che provengono dall'indirizzo IP `86.212.199.60`, includendo il campo `user` e la porta. Questo permette di osservare i dettagli dei tentativi di accesso falliti da quell'IP specifico.



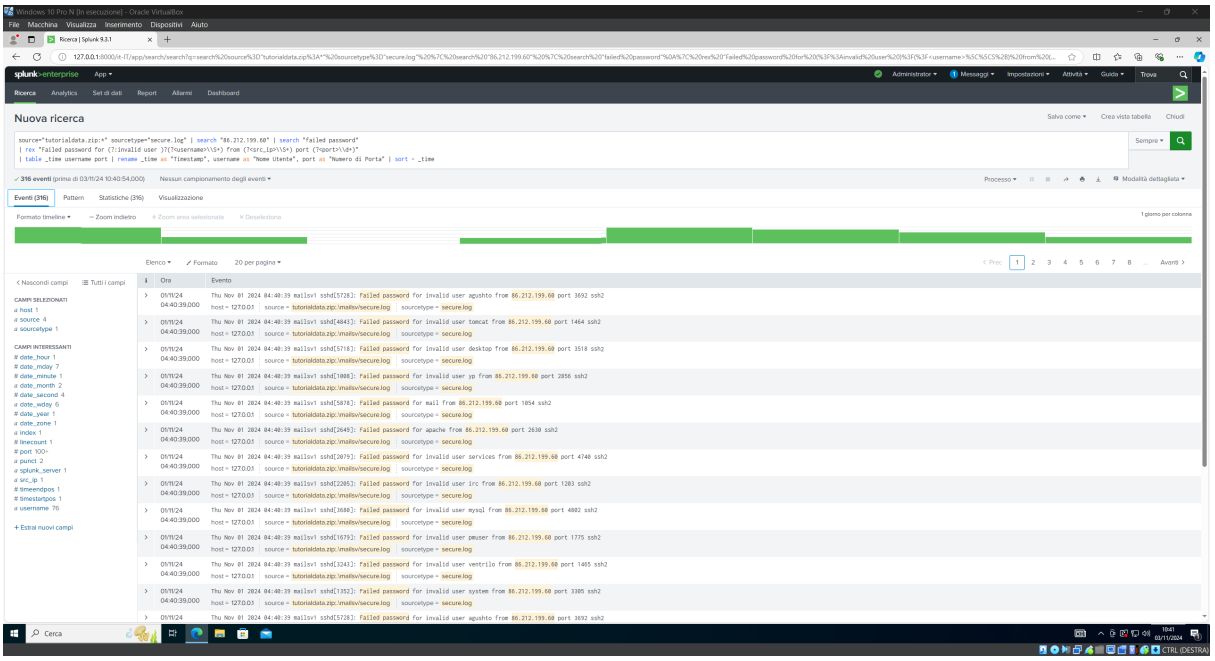


5. Estrarre tentativi di accesso falliti per IP specifico e visualizzare il numero di porta

```
source="tutorialdata.zip:*" sourcetype="secure.log" | searc
h "86.212.199.60" | search "failed password"
| rex "Failed password for (?:invalid user )?(?<username>
\\S+) from (?<src_ip>\\S+) port (?<port>\\d+)"
| table _time username port | rename _time as "Timestamp",
```

```
username as "Nome Utente", port as "Numero di Porta" | sort
- _time
```

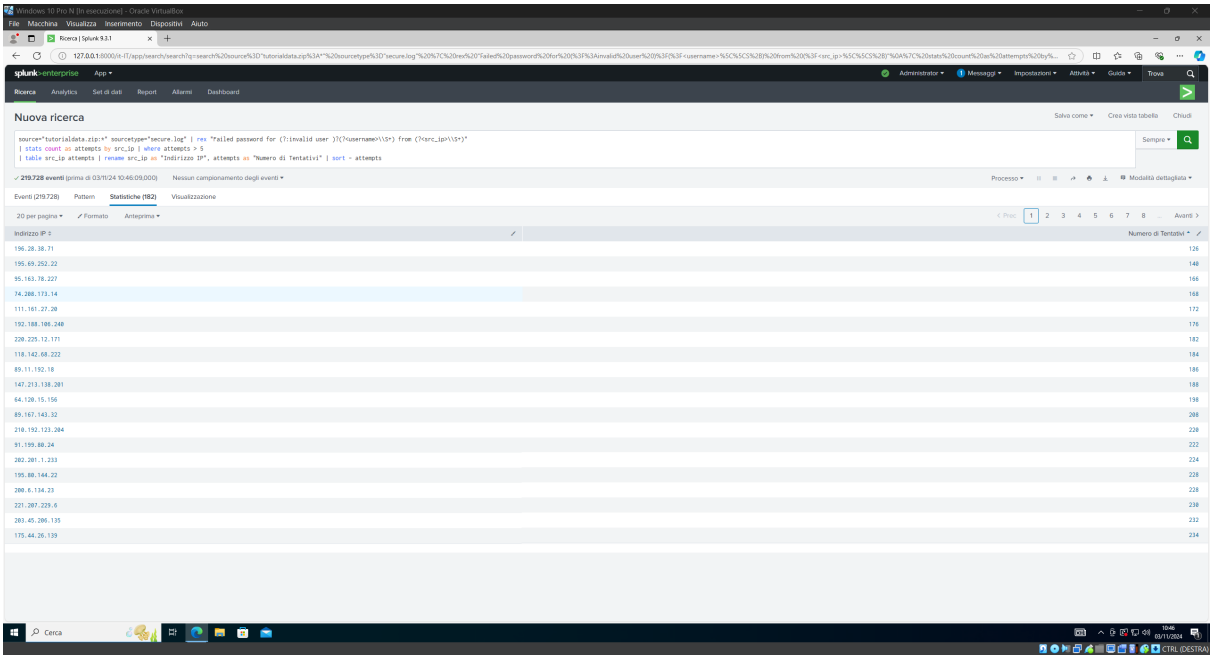
- **Descrizione**: Questa query individua i tentativi di accesso falliti dall'IP `86.212.199.60` e utilizza `rex` per estrarre `username`, `src_ip` e `port`. I risultati sono ordinati per timestamp e mostrano `Nome Utente`, `Numero di Porta` e `Timestamp`.

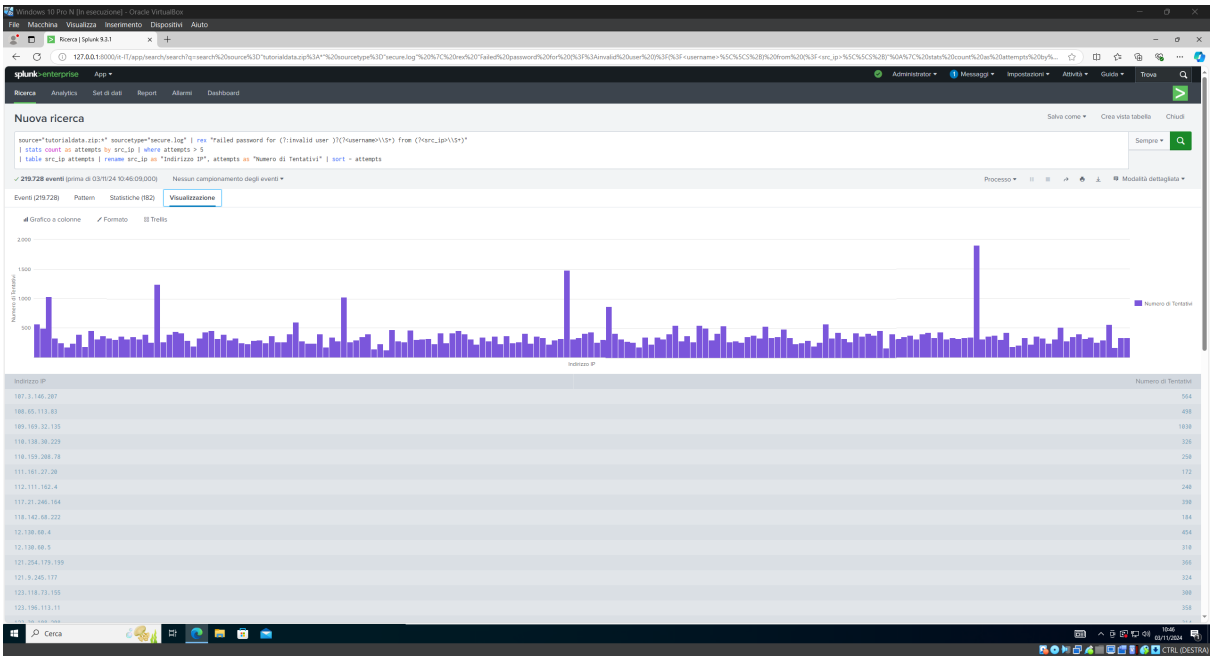


6. Identificare gli indirizzi IP con più di 5 tentativi di accesso falliti

```
source="tutorialdata.zip:*" sourcetype="secure.log" | rex
"Failed password for (?:invalid user )?(?<username>\\S+) fr
om (?<src_ip>\\S+)"
| stats count as attempts by src_ip | where attempts > 5
| table src_ip attempts | rename src_ip as "Indirizzo IP",
attempts as "Numero di Tentativi" | sort - attempts
```

- **Descrizione**: Questa query estrae gli indirizzi IP (`src_ip`) associati ai tentativi di accesso falliti e utilizza `stats` per contare il numero di tentativi per ogni IP. Mostra solo gli IP con più di 5 tentativi, ordinati dal più alto.

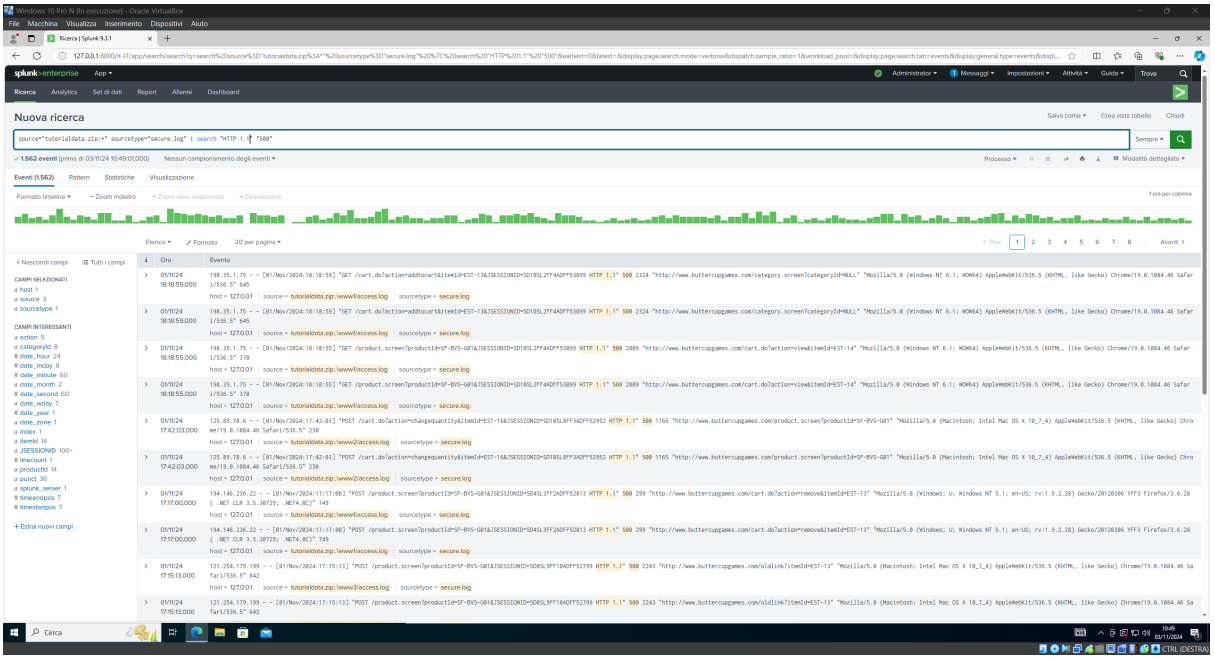




7. Trovare tutti i log con “Internal Server Error”

```
source="tutorialdata.zip:*" sourcetype="secure.log" | searc
h "HTTP 1.1" "500"
```

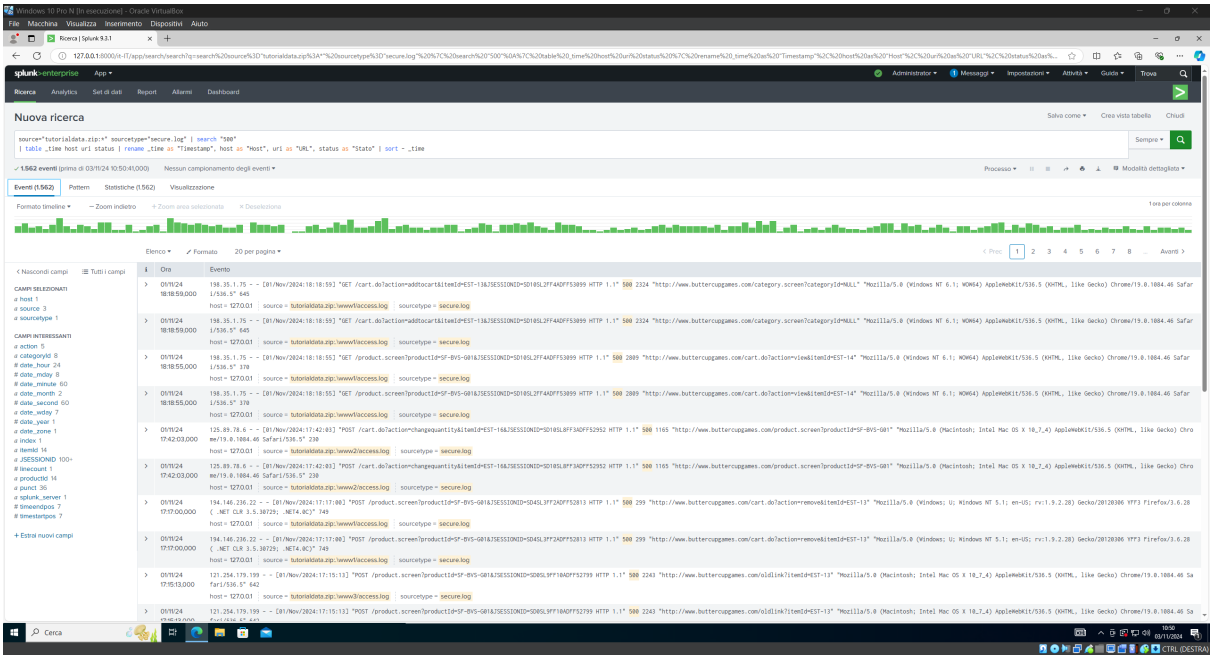
- **Descrizione**: Questa query individua tutti i log con codice di errore `500`, tipicamente indicativo di un “Internal Server Error” nei sistemi web. È utile per diagnosticare problemi server-side.



8. Trovare e organizzare tutti gli errori “500”

```
source="tutorialdata.zip:*" sourcetype="secure.log" | searc
h "500"
| table _time host uri status | rename _time as "Timestam
p", host as "Host", uri as "URL", status as "Stato" | sort
- _time
```

- **Descrizione**: Questa query cerca log di errore `500`, visualizzando una tabella con il timestamp, l’host, l’URL e lo stato. È utile per un'analisi dettagliata dei percorsi o pagine che hanno generato errori server.



Report Conclusivo dell'Analisi dei Log

Sintesi Esecutiva

L'analisi dettagliata dei log dei nostri sistemi ha portato alla luce alcune attività potenzialmente malevole che suggeriscono tentativi di attacco intenzionali e mirati. Questi eventi evidenziano rischi per la sicurezza dei nostri dati e infrastrutture. Le attività sospette rilevate comprendono tentativi di accesso non autorizzato tramite attacchi di forza bruta su SSH, attività di ricognizione avanzata tramite enumerazione di sessioni e processi, automazione anomala di azioni sul sito web e possibili attacchi di credential stuffing e SQL injection.

Le informazioni rilevate e le raccomandazioni fornite delineano un quadro di rischio, sottolineando l'importanza di rafforzare le misure di sicurezza e di continuare a monitorare le attività anomale sui nostri sistemi.

1. Tentativi di Accesso Brute Force su SSH

Osservazioni:

Nei log di accesso SSH, abbiamo riscontrato diversi tentativi di login falliti che seguono il modello tipico di un attacco di **forza bruta**. Questo attacco mira a ottenere accesso al sistema tentando un gran numero di combinazioni di credenziali. Sono emersi alcuni indirizzi IP ricorrenti, che evidenziano la presenza di bot o attaccanti automatizzati.

- **Indicazioni chiave**: Alcuni IP compaiono ripetutamente e tentano l'accesso in intervalli di tempo molto ravvicinati.
- **Rischi associati**: Un accesso non autorizzato potrebbe compromettere non solo i dati ma anche i servizi principali dell'organizzazione.

Azioni raccomandate:

- Implementare un sistema di blocco automatico dopo un numero definito di tentativi falliti.
- Attivare l'autenticazione a due fattori (2FA) per ridurre il rischio di compromissione.

2. Ricognizione tramite Enumerazione di Sessioni e Processi

Osservazioni:

L'analisi dei log ha mostrato diversi accessi che sembrano mirare a raccogliere dettagli su processi e sessioni attivi. Questo pattern è comune in fase di **ricognizione**, quando un attaccante cerca di ottenere informazioni che potrebbero essere utilizzate in un attacco successivo, mirato a sfruttare vulnerabilità specifiche.

- **Indicazioni chiave**: Presenza di connessioni che non mirano a ottenere accessi permanenti, ma piuttosto informazioni di sistema.
- **Rischi associati**: La raccolta di informazioni sensibili sui processi potrebbe consentire ad attaccanti esperti di pianificare attacchi più mirati.

Azioni raccomandate:

- Limitare l'accesso alle informazioni di sistema solo agli utenti autorizzati.
- Configurare alert per rilevare tentativi di enumerazione anomala delle risorse.

3. Attività Sospette di Automazione sul Sito Web

Osservazioni:

L'analisi dei log HTTP mostra una frequenza sospetta di azioni come "addtocart" e "changequantity," che potrebbero indicare la presenza di bot malevoli. Questi bot potrebbero essere utilizzati per **scraping dei dati** o **frodi tramite azioni automatizzate**, simulando il comportamento di utenti reali.

- **Indicazioni chiave**: Frequenza elevata di richieste ripetitive che replicano azioni di acquisto.
- **Rischi associati**: Possibile perdita di dati e impatti sulle performance del sito, oltre a un rischio di frode.

Azioni raccomandate:

- Integrare sistemi di CAPTCHA e blocchi per le richieste ripetitive e sospette.
- Monitorare e limitare il numero di richieste provenienti dallo stesso IP per le API sensibili.

4. Potenziali Attacchi Rilevati

a) Credential Stuffing

Osservazioni:

La presenza di numerosi tentativi di accesso falliti provenienti da specifici indirizzi IP è un potenziale indicatore di **credential stuffing**, una tecnica in cui gli attaccanti utilizzano credenziali compromesse per tentare di accedere a server SSH.

- **Indicazioni chiave**: IP ricorrenti con pattern di accesso falliti.
- **Rischi associati**: Possibile compromissione di account privilegiati, che potrebbe mettere a rischio sistemi chiave.

Azioni raccomandate:

- Configurare il sistema per bloccare temporaneamente gli IP con troppi tentativi falliti.
- Imporre il cambio delle password su base regolare e monitorare le attività di accesso sospette.

b) SQL Injection e Abuso delle API

Osservazioni:

Sebbene non sia rilevato direttamente dai log, i pattern anomali nelle richieste HTTP possono suggerire tentativi di attacco quali **SQL injection** o abuso delle API. Attività come l'abuso delle API potrebbe compromettere la riservatezza dei dati o esaurire le risorse di sistema.

- **Indicazioni chiave**: Presenza di richieste HTTP ripetute e con valori anomali.

- **Rischi associati**: Rischio di accesso non autorizzato ai dati e possibili effetti sulle performance del sistema.

Azioni raccomandate:

- Implementare controlli di input rigorosi per ridurre il rischio di SQL injection.
- Monitorare costantemente le richieste sospette e configurare alert per attività ripetitive non autorizzate.

Conclusioni

L'analisi dei log rivela che il sistema è stato oggetto di tentativi di attacco su più fronti, suggerendo che la nostra infrastruttura attira attivamente interesse da parte di attaccanti esterni. Per rafforzare la sicurezza dei nostri sistemi e prevenire possibili compromissioni, è cruciale adottare le seguenti misure:

1. **Blocco IP e autenticazione avanzata** per limitare l'accesso SSH a utenti verificati.
2. **Monitoraggio avanzato** delle attività di enumerazione e alerting su azioni sospette.
3. **Controllo e limitazione delle API** e protezione anti-bot sul sito web per ridurre il rischio di automazione malevola e scraping.
4. **Implementazione di meccanismi di difesa** per SQL injection e monitoraggio dei tentativi di credential stuffing.

Questa analisi sottolinea l'importanza del monitoraggio continuo della sicurezza e della configurazione di contromisure robuste. Investire in strumenti avanzati di sicurezza e gestione dei log permetterà di mantenere un elevato livello di sicurezza operativa e di prevenire possibili minacce future.