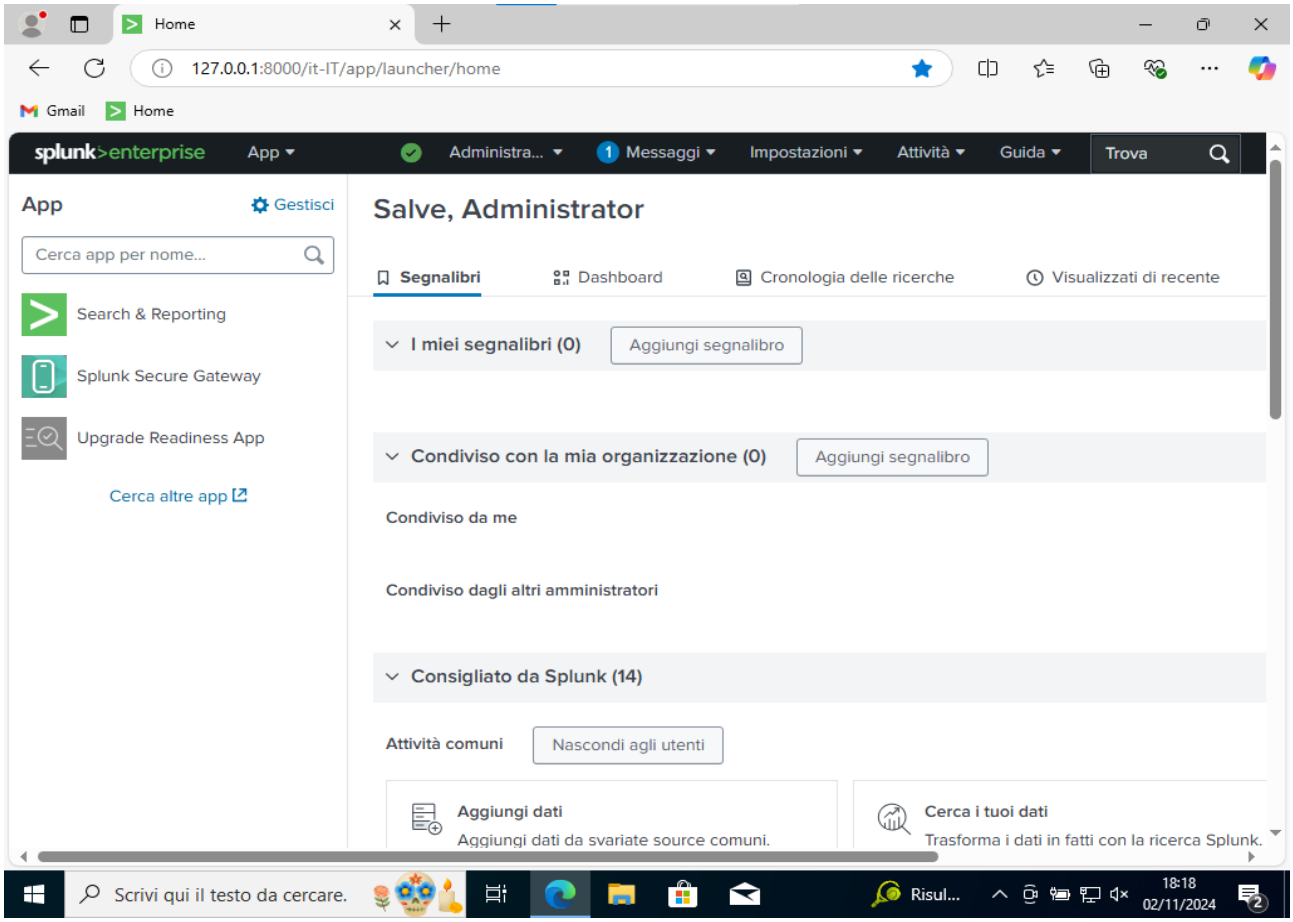
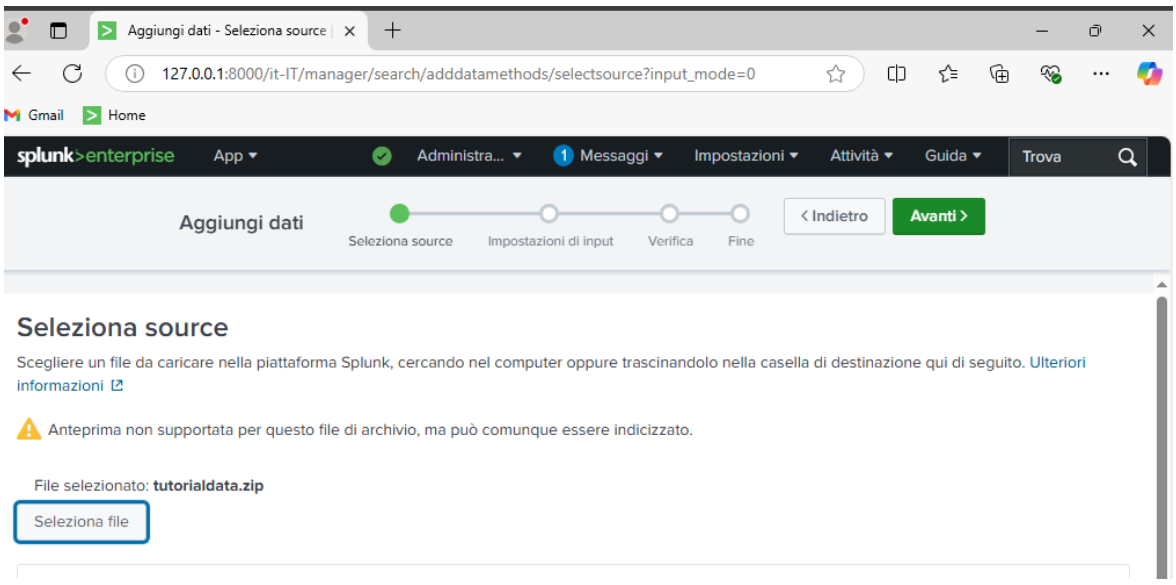
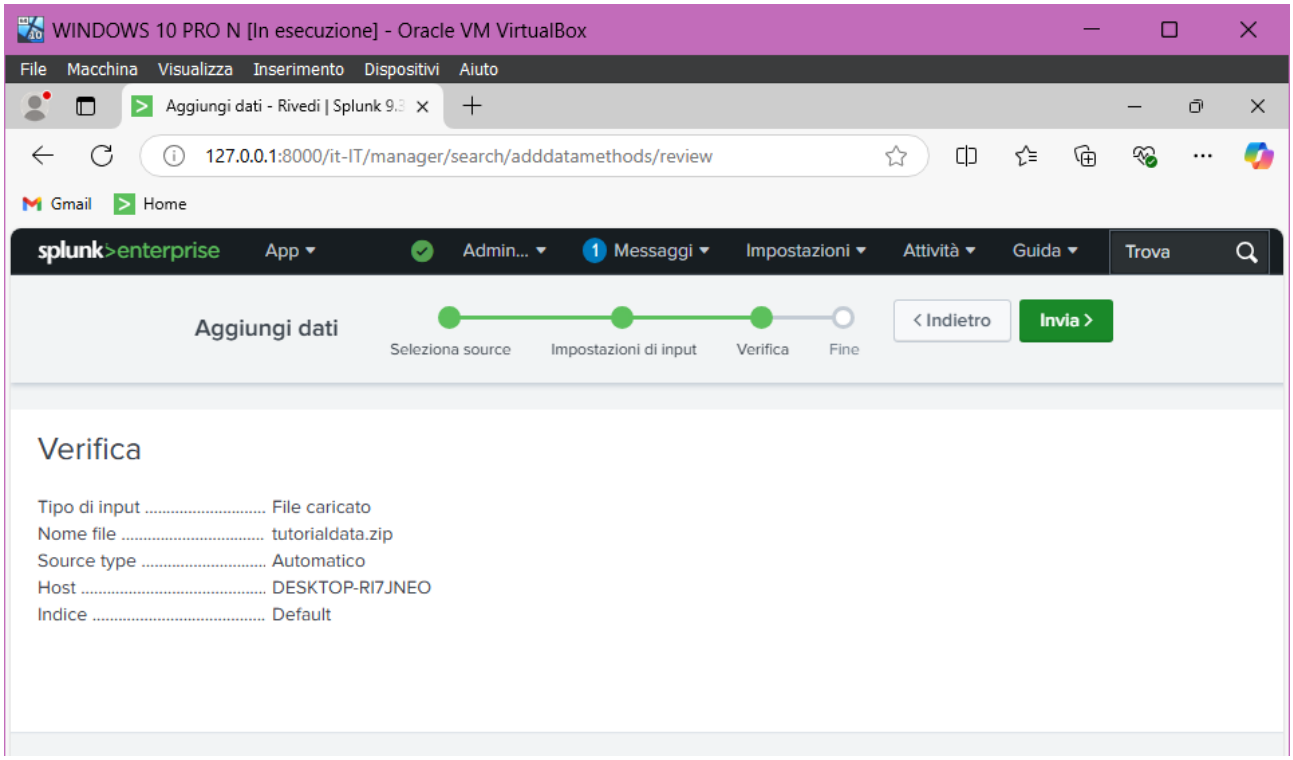
STEP 1: ACCESSO A SPLUNK E CARICAMENTO FILE tutorialdata.zip

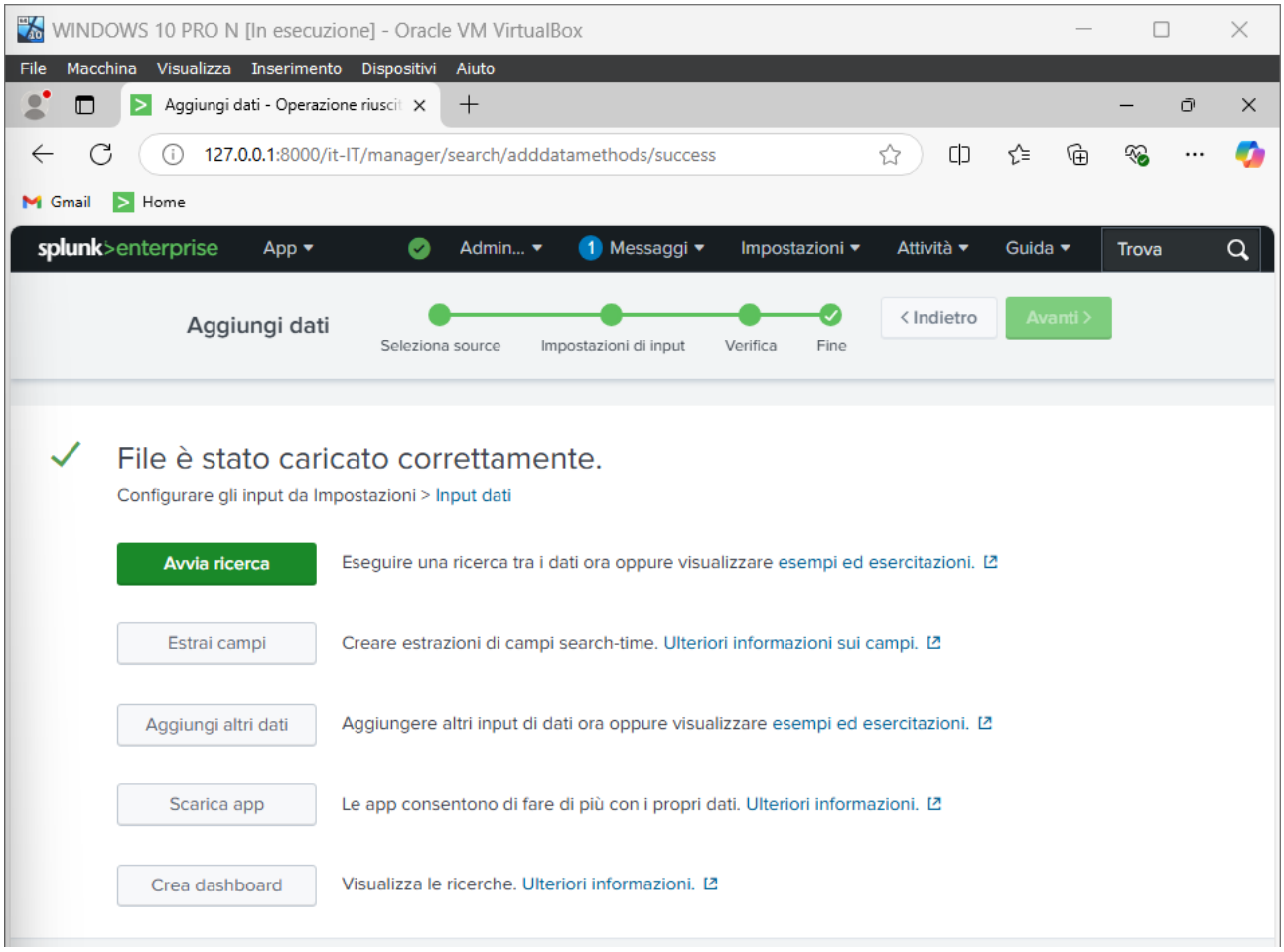
Vado su localhost 8000 e accedo con le mie credenziali

Poi nella schermata aggiungo il file e lo carico, successivamente verifico che i dati siano stati caricati correttamente e che Splunk li abbia indicizzati.





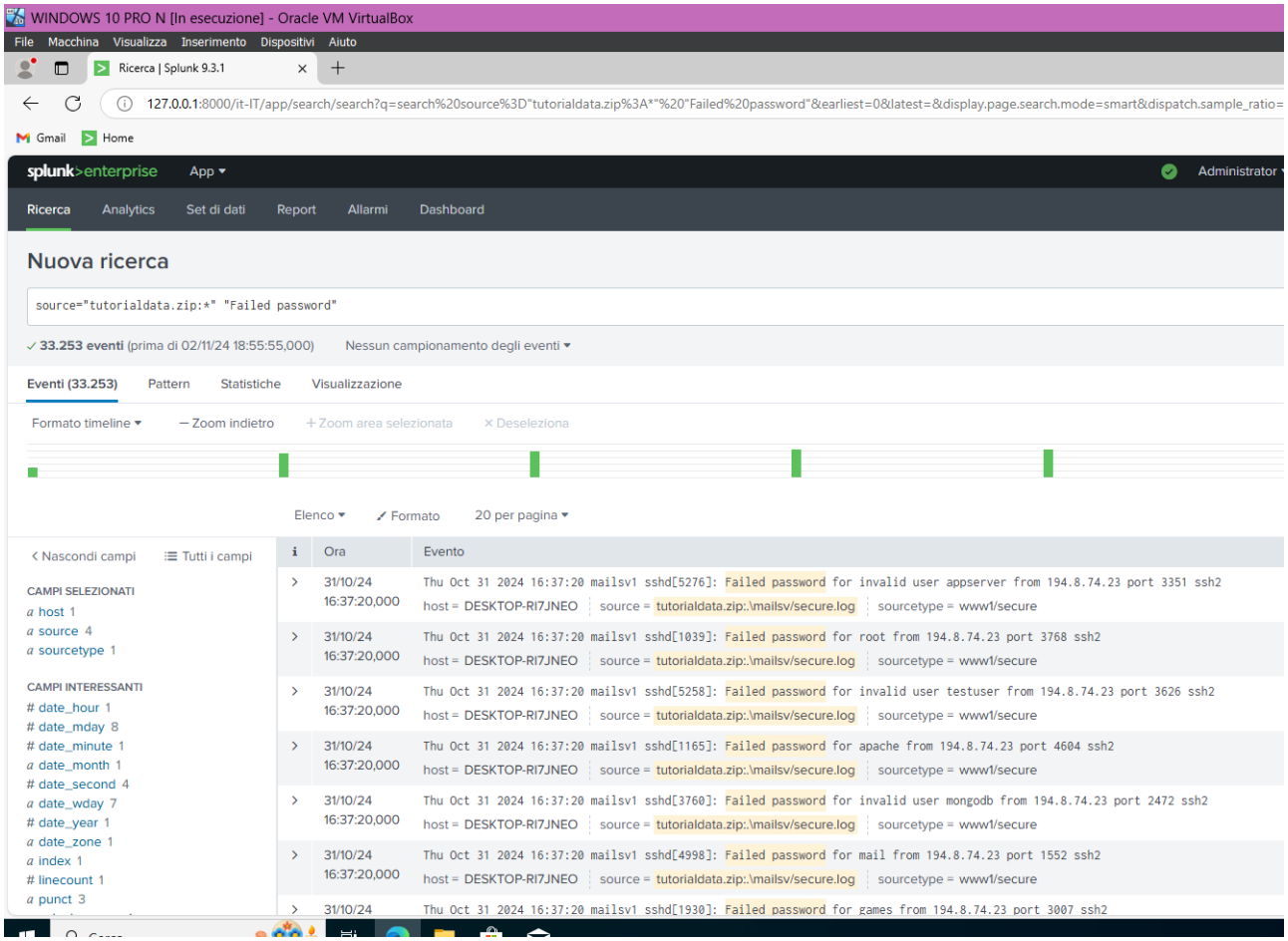

WINDOWS 10 PRO N [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Aggiungi dati - Rivedi | Splunk 9.
127.0.0.1:8000/it-IT/manager/search/adddatamethods/review
Gmail Home
splunk>enterprise App Admin... 1 Messaggi Impostazioni Attività Guida Trova
Aggiungi dati
Seleziona source Impostazioni di input Verifica Fine
< Indietro Invia >
Verifica
Tipo di input ..... File caricato
Nome file ..... tutorialdata.zip
Source type ..... Automatico
Host DESKTOP-RI7JNEO
Indice ..... Default

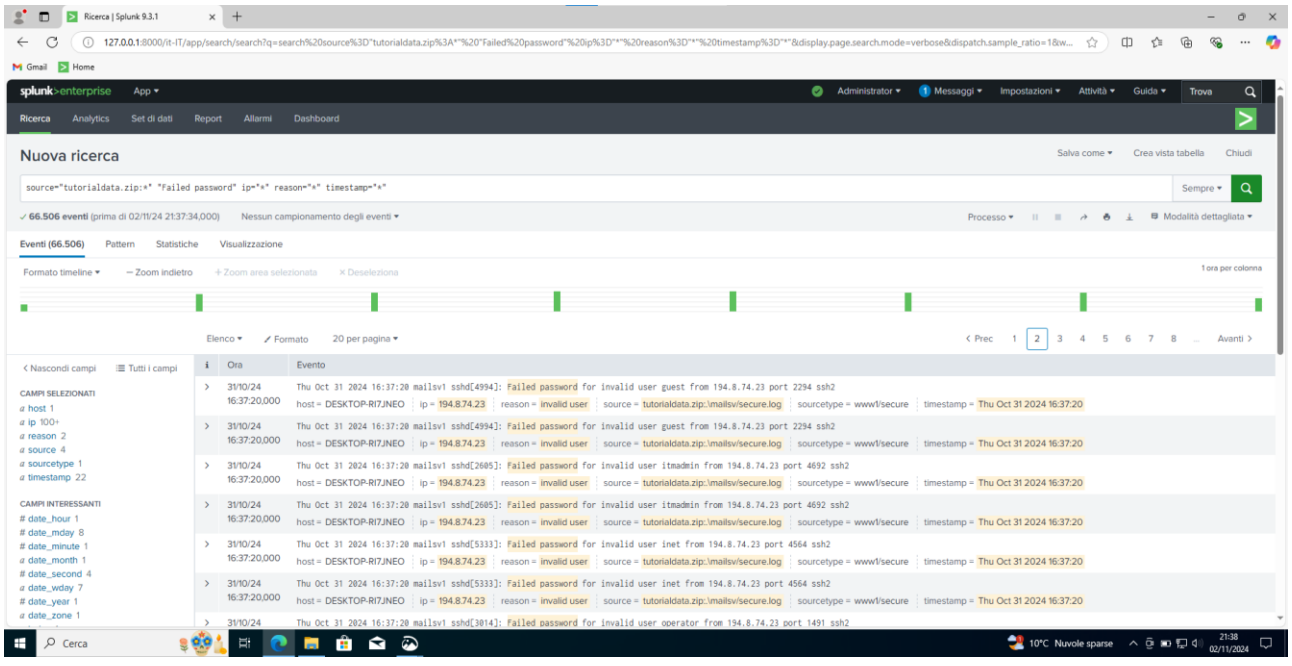

WINDOWS 10 PRO N [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Aggiungi dati - Operazione riusci
127.0.0.1:8000/it-IT/manager/search/adddatamethods/success
Gmail Home
splunk>enterprise App Admin... 1 Messaggi Impostazioni Attività Guida Trova
Aggiungi dati
Seleziona source Impostazioni di input Verifica Fine
< Indietro Avanti >
File è stato caricato correttamente.
Configurare gli input da Impostazioni > Input dati
Avvia ricerca
Eseguire una ricerca tra i dati ora oppure visualizzare esempi ed esercitazioni.
Estrai campi
Creare estrazioni di campi search-time. Ulteriori informazioni sui campi.
Aggiungi altri dati
Aggiungere altri input di dati ora oppure visualizzare esempi ed esercitazioni.
Scarica app
Le app consentono di fare di più con i propri dati. Ulteriori informazioni.
Crea dashboard
Visualizza le ricerche. Ulteriori informazioni.

STEP 2: CREAZIONE DELLE QUERY

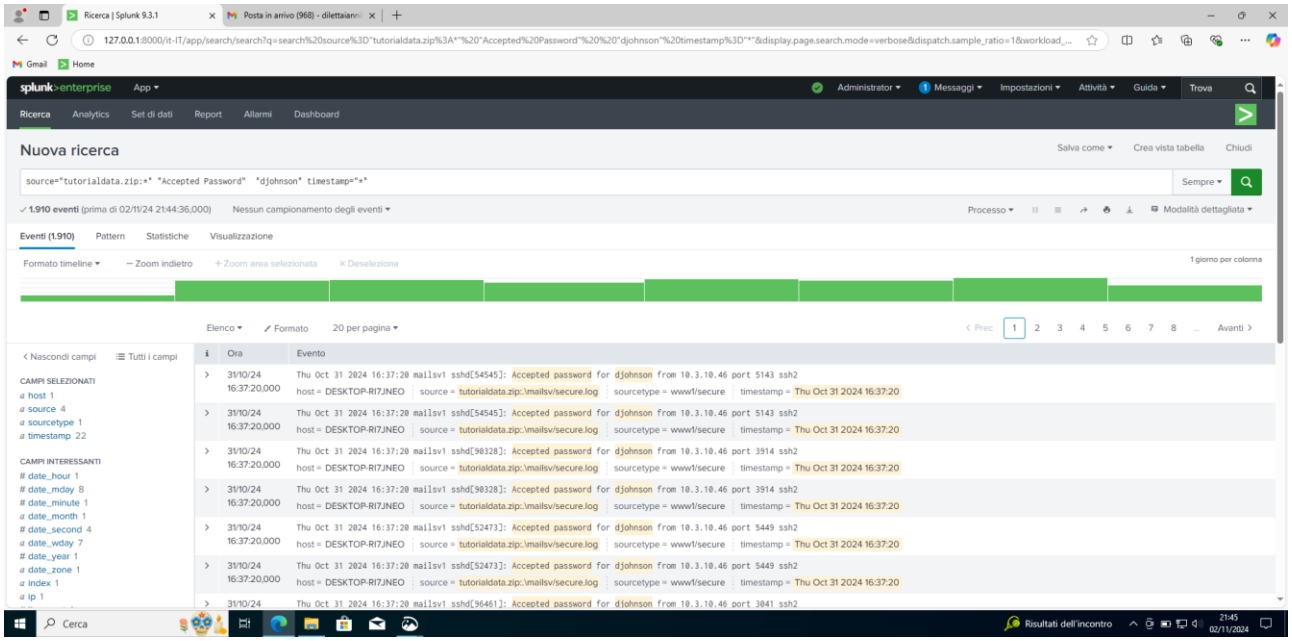
Avvio la ricerca e inizio a inserire le query nella barra di ricerca.

1. Query per identificare tutti i tentativi di accesso falliti “Failed password”

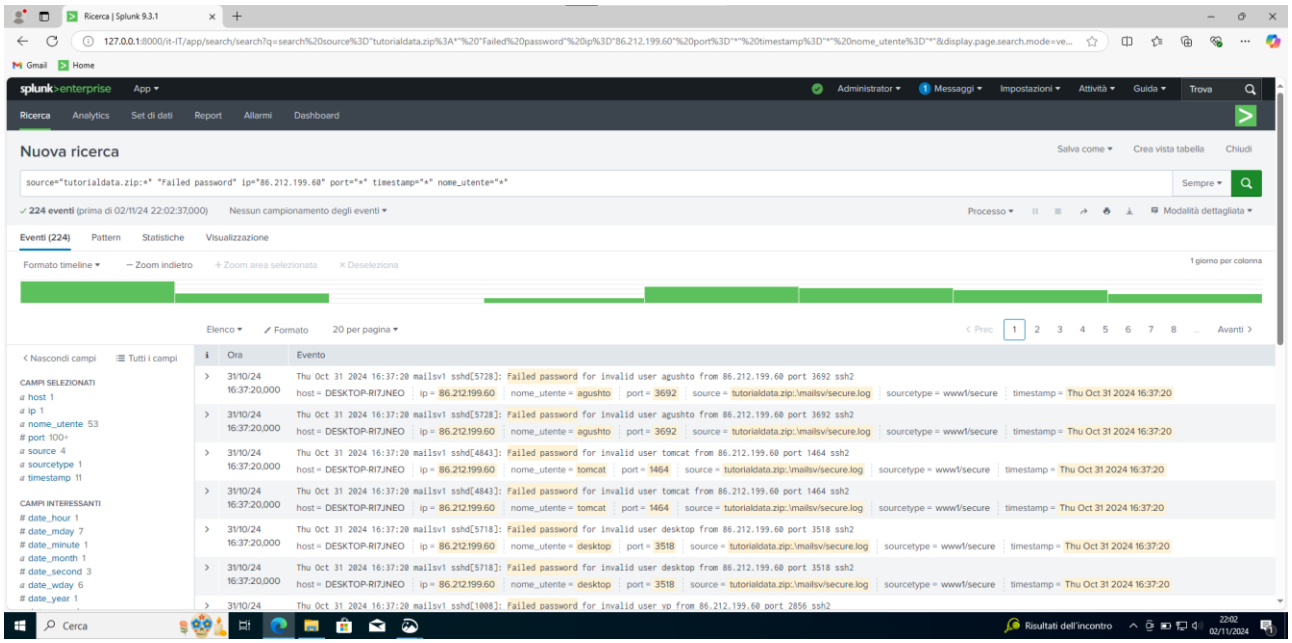




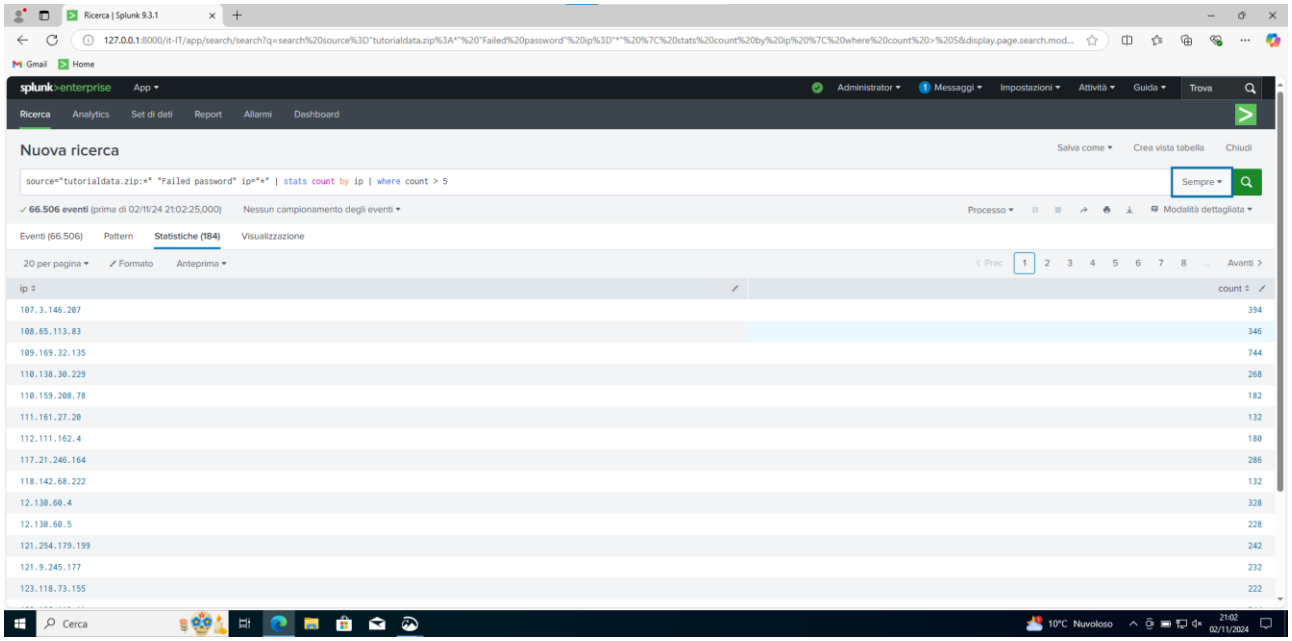
2. Query per trovare tutte le sessioni SSH aperte con successo per l'utente "djohnson"



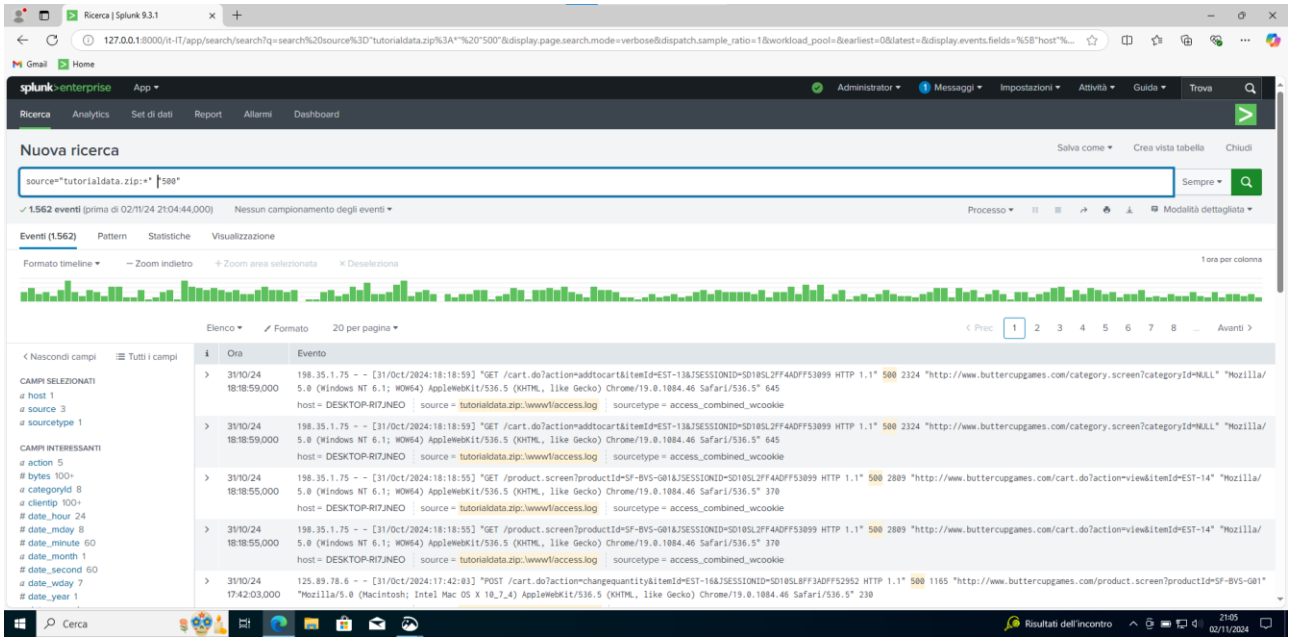
3. Query per rilevare i tentativi di accesso falliti provenienti dall'IP "86.212.199.60"



4. Query per identificare tutti gli IP che presentano più di 5 tentativi di accesso falliti



5. Query per rilevare gli “Internal Server Error” (Codice errore 500)



Conclusioni sui log analizzati

Analisi dei Log sui Tentativi di Accesso Falliti

1. **Pattern di Accesso**
    - I tentativi di accesso falliti mostrano un pattern comune, ovvero l'uso di utenti non validi o sospetti, come "agushto", "tomcat", "appserver", "desktop", "root", "testuser", "administrator", "sys", "irc", ed "email". Questi utenti possono essere generati in maniera casuale o essere parte di liste di credenziali comunemente utilizzate dagli attaccanti in tentativi di brute force.
2. **Indirizzi IP di Origine**
    - Tra gli IP più frequenti, troviamo indirizzi come:
        - **86.212.199.60**: Ha effettuato numerosi tentativi di accesso falliti, utilizzando utenti differenti e varie porte, suggerendo l'uso di uno script automatizzato.
        - **194.8.74.23** e **203.45.206.135**: Entrambi hanno registrato accessi falliti multipli, a indicare una possibile campagna coordinata o attacchi ripetuti.
        - **IP interni** come **10.1.10.172** e **10.2.10.163** potrebbero indicare attacchi simulati per test interni o la compromissione di dispositivi locali che tentano accessi non autorizzati.
3. **Tentativi su Porte Diversificate**
    - Gli attacchi non si limitano alla porta SSH standard (22), ma sono distribuiti su porte casuali come 3351, 3768, 3626, 3692, 1464 e altre. Questa tecnica è nota per essere utilizzata per:
        - **Evitare il rilevamento**: Utilizzare porte diverse consente agli attaccanti di aggirare le regole di firewall statiche o di confondere i sistemi di monitoraggio.
        - **Sondare le configurazioni**: Gli attaccanti cercano di scoprire se ci sono servizi SSH o protocolli di accesso configurati su porte non standard.
4. **Volume dei Tentativi**
    - L'elevato numero di tentativi di accesso registrati in brevi intervalli di tempo è un indicatore chiave di attacchi brute force. Questi attacchi sono spesso eseguiti da bot o script automatizzati che tentano ripetutamente di accedere a un sistema utilizzando liste predefinite di nomi utente e password.

- Il comportamento evidenziato dai log suggerisce che alcuni IP, come **86.212.199.60**, siano responsabili di un numero significativo di tentativi in un arco di tempo ridotto, rafforzando l'ipotesi di un attacco brute force.

5. **Tipologia di Eventi Registrati**
    - I log riportano messaggi di errore come "Failed password for invalid user", indicando che il tentativo di accesso è stato effettuato con un nome utente non riconosciuto dal sistema. Altri eventi di accesso fallito, invece, possono riferirsi a tentativi con utenti esistenti ma con password errate.
    - Eventi come "Invalid user [nome_utente]" mostrano che l'attaccante sta cercando di accedere con utenti che non esistono, forse per verificare quali utenti siano effettivamente presenti nel sistema.

Potenziali Implicazioni

1. Tentativi di Attacco Brute Force:

- La ripetizione di tentativi di accesso falliti con nomi utente diversi e da IP ricorrenti indica un attacco brute force automatizzato. Questi attacchi mirano a indovinare le credenziali corrette sfruttando liste di utenti comuni e password deboli.
- Gli IP coinvolti provengono da località diverse, il che potrebbe indicare un attacco distribuito, eseguito tramite una botnet. Questo tipo di attacco sfrutta più computer compromessi per rendere più difficile l'identificazione della fonte e l'applicazione di contromisure.

2. Enumerazione Utenti:

- I tentativi falliti con utenti "invalidi" mostrano che l'attaccante potrebbe cercare di determinare quali nomi utente siano validi nel sistema. Questa tecnica, conosciuta come **enumerazione degli utenti**, è utile agli attaccanti per raccogliere informazioni preliminari prima di tentare attacchi mirati.
- Identificare utenti validi consente all'attaccante di restringere il campo di ricerca per tentativi futuri, aumentando la probabilità di successo.

3. Evasione del Monitoraggio:

- L'uso di porte non standard per i tentativi di accesso è una tecnica per aggirare le regole dei firewall o per evitare di essere facilmente individuati dai sistemi di monitoraggio. Questo comportamento suggerisce una consapevolezza da parte dell'attaccante delle misure di sicurezza potenzialmente presenti nella rete.

4. Rischi Interni:

- Gli accessi falliti da IP interni potrebbero indicare test legittimi o simulazioni di attacchi, ma potrebbero anche essere segnale di una compromissione interna. Un dispositivo compromesso all'interno della rete può rappresentare un rischio significativo poiché ha già superato le difese esterne.

Azioni Raccomandate per Mitigare i Tentativi di Accesso Falliti

1. Bloccare IP Sospetti

- **Implementazione di strumenti di blocco automatico**: Utilizzare strumenti come **fail2ban**, che analizzano i file di log e bloccano automaticamente gli IP sospetti dopo un numero prestabilito di tentativi di accesso falliti. Questo approccio è efficace per limitare attacchi brute force poiché isola rapidamente gli IP con comportamenti sospetti.
- **Lista nera (Blacklist)**: Mantenere una blacklist aggiornata di IP notoriamente malevoli o coinvolti in tentativi di attacco. Questi IP possono essere bloccati a livello di firewall per evitare ulteriori tentativi di accesso.

2. Audit degli Accessi

- **Verifica delle sessioni di accesso**: Controllare regolarmente gli accessi degli utenti, come l'attività dell'utente "djohnson" menzionata nei log, per verificare la legittimità e autenticità delle connessioni. Gli audit possono includere la revisione degli orari di accesso, la provenienza degli IP, e la corrispondenza con le normali abitudini lavorative degli utenti.
- **Identificazione di anomalie**: Utilizzare strumenti di analisi comportamentale che confrontano gli accessi con i modelli tipici per rilevare potenziali compromissioni o usi impropri delle credenziali.

3. Risoluzione dei Problemi del Server

- **Analisi degli errori HTTP 500**: Approfondire le cause degli errori del server (codice 500) attraverso la revisione dei log degli errori e l'identificazione delle richieste che li hanno generati. Questi errori possono indicare problemi di configurazione o vulnerabilità sfruttabili.
- **Patch e aggiornamenti**: Assicurarsi che il server e le applicazioni web siano aggiornati con le ultime patch di sicurezza per evitare che le vulnerabilità possano essere sfruttate da attaccanti.
- **Stress test e monitoraggio delle prestazioni**: Condurre test di carico per identificare eventuali problemi di stabilità e configurare strumenti di monitoraggio per rilevare e segnalare picchi di errore in tempo reale.

4. Hardening del Server e Sicurezza degli Accessi

- **Disabilitare l'accesso root via SSH**: Configurare il server per impedire l'accesso diretto come utente root, richiedendo l'uso di un utente con privilegi limitati e l'elevazione dei permessi solo quando necessario (ad esempio, tramite sudo).
- **Configurazione del tempo di blocco**: Impostare un blocco temporaneo per gli account dopo un numero definito di tentativi di accesso falliti. Questa misura impedisce che un attacco brute force possa procedere senza interruzioni.
- **Autenticazione basata su chiavi SSH**: Sostituire l'accesso basato su password con l'autenticazione basata su chiavi SSH per rendere più sicuro l'accesso remoto e ridurre drasticamente la possibilità di successo di un attacco brute force.

5. Monitoraggio e Risposta in Tempo Reale

- **Implementazione di un sistema di rilevamento delle intrusioni (IDS/IPS)**: Utilizzare sistemi come Snort o Suricata per monitorare il traffico di rete e i log del server in tempo reale, rilevando e rispondendo rapidamente a comportamenti sospetti.
- **Notifiche e alert**: Configurare notifiche automatiche per avvisare gli amministratori di sistema di attività anomale, come tentativi ripetuti di accesso falliti o accessi da IP sconosciuti o insoliti.
- **Analisi dei log con SIEM**: Implementare una soluzione di gestione delle informazioni e degli eventi di sicurezza (SIEM) come Splunk o Elastic Stack, per aggregare e analizzare i log in modo centralizzato, facilitando il rilevamento di attacchi sofisticati e la creazione di report dettagliati.

6. Educazione e Formazione

- **Sensibilizzazione del personale**: Formare gli utenti sul riconoscimento delle minacce e sulle migliori pratiche di sicurezza informatica, come l'uso di password forti e uniche e l'importanza del 2FA.
- **Procedure di risposta agli incidenti**: Definire e testare regolarmente le procedure per la risposta agli incidenti di sicurezza, assicurandosi che il team sia pronto a reagire in caso di tentativo di intrusione.

Conclusioni

Dall'analisi dettagliata dei log emerge un quadro chiaro della necessità di adottare un approccio proattivo e multilivello per la sicurezza del sistema. I numerosi tentativi di accesso falliti, spesso provenienti da IP ripetitivi e vari utenti non autorizzati, suggeriscono la presenza di attacchi brute force automatizzati o tentativi di enumerazione delle credenziali. Questi eventi sottolineano l'importanza di implementare misure di protezione mirate come il blocco automatico degli IP sospetti e l'utilizzo di tecniche di autenticazione più sicure, quali le chiavi SSH.

Gli accessi riusciti, sebbene possano sembrare legittimi, richiedono un audit regolare per garantire l'autenticità e prevenire l'uso improprio delle credenziali, come nel caso dell'utente "djohnson". Questa pratica, combinata con l'analisi comportamentale degli accessi, permette di individuare eventuali compromissioni o anomalie.

I numerosi errori HTTP 500 nei log indicano la possibilità di problemi di stabilità o configurazione del server che potrebbero essere sfruttati da attaccanti per causare disservizi o ottenere accessi non autorizzati. La risoluzione di questi errori e la protezione contro exploit noti e nuove vulnerabilità rappresentano un passaggio fondamentale per rafforzare la sicurezza.

Le azioni raccomandate per mitigare questi rischi comprendono l'adozione di strumenti di blocco automatico come **fail2ban**, l'uso di sistemi di rilevamento delle intrusioni (IDS/IPS), e l'implementazione di procedure di risposta agli incidenti. È altresì essenziale un approccio basato sull'educazione e la formazione continua del personale per minimizzare i rischi legati a errori umani e per migliorare la consapevolezza sulla sicurezza informatica.

In conclusione, un'infrastruttura IT sicura si basa su una combinazione di misure preventive, monitoraggio costante e risposte rapide agli incidenti. Investire in un sistema di difesa multilivello e in un monitoraggio approfondito permette non solo di rilevare e bloccare minacce in tempo reale, ma anche di prevenire attacchi futuri. La sicurezza è un processo continuo che richiede aggiornamenti costanti, l'analisi dei log, e la verifica delle politiche di accesso per proteggere l'integrità del sistema e dei dati aziendali.