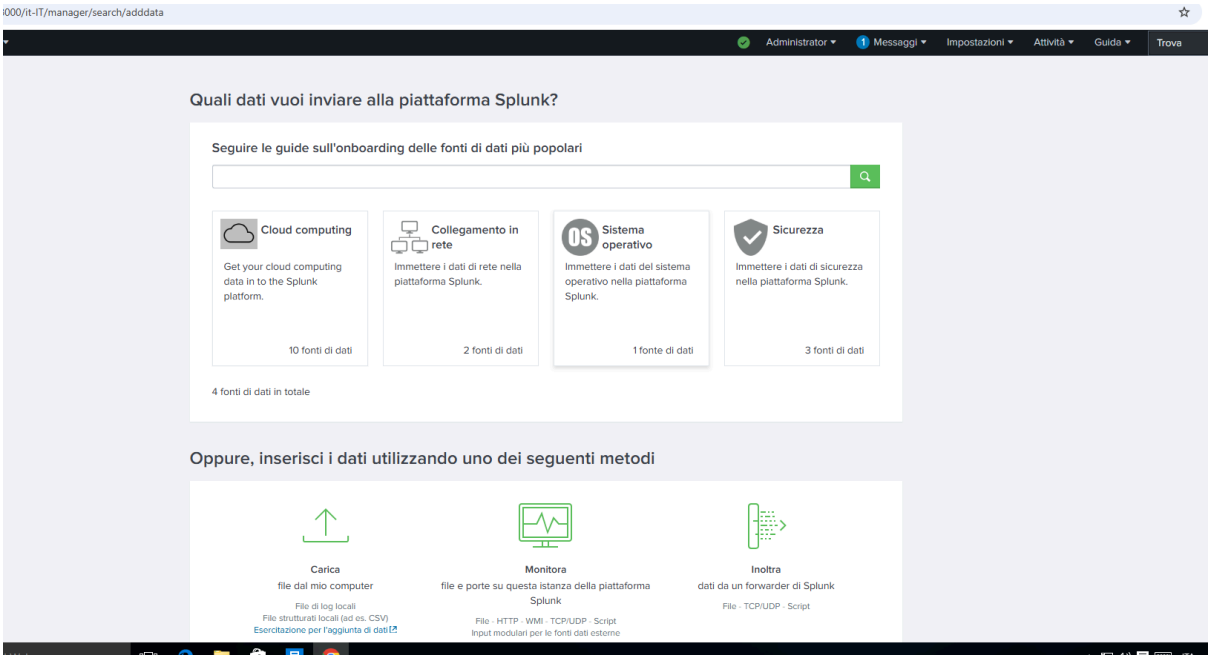
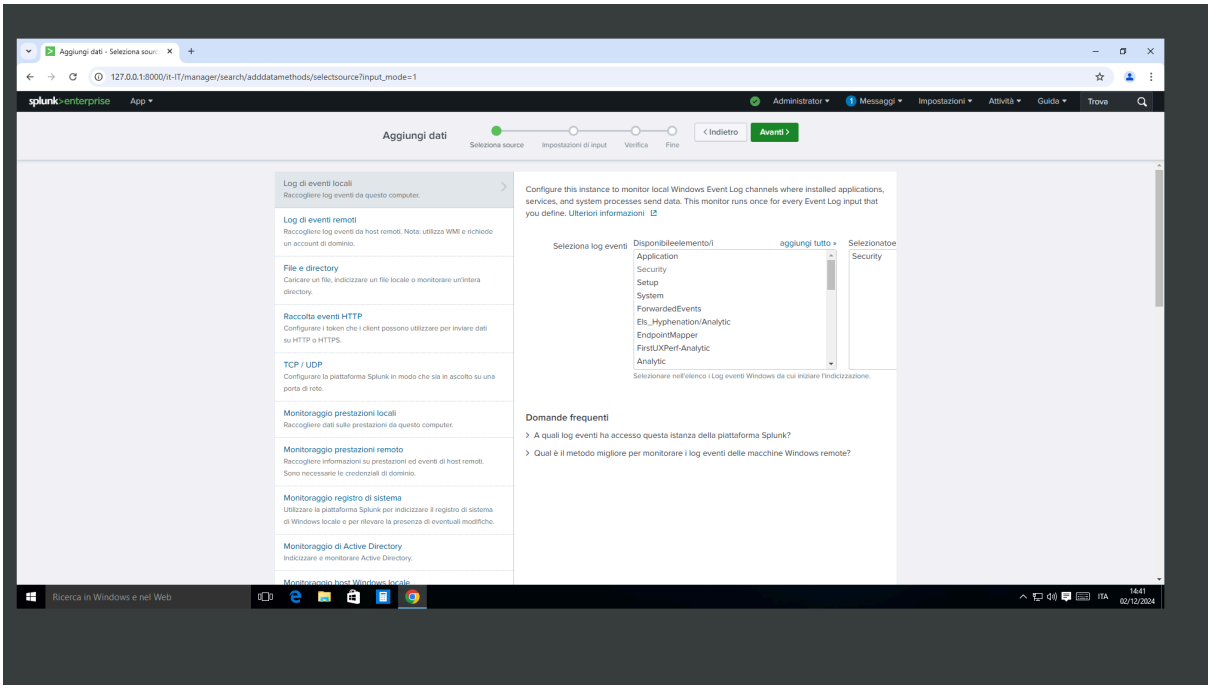
S10L1 - Splunk su Metasploitable

Durante questa attività, mi sono concentrato sulla configurazione della modalità "Monitora" in Splunk, un potente strumento per l'analisi dei dati. Questo esercizio ha previsto l'impostazione della modalità di monitoraggio, che permette di raccogliere e analizzare automaticamente dati da diverse fonti.

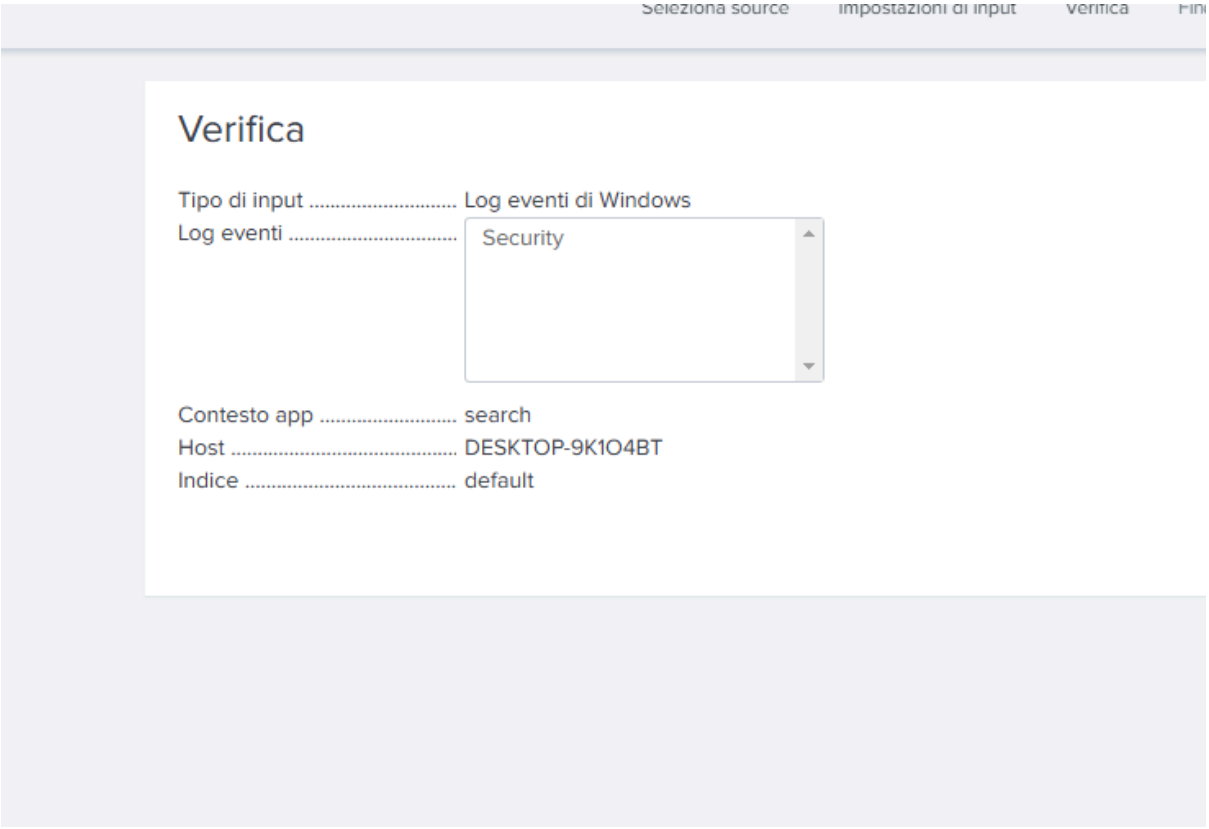
Per iniziare, è stato necessario accedere alla piattaforma Splunk e verificare la disponibilità del pannello di controllo amministrativo. Questo passaggio iniziale garantisce che l'ambiente sia pronto per accogliere nuove configurazioni. Lo screenshot catturato conferma che l'accesso è stato completato correttamente.



Per configurare il monitoraggio, ho selezionato la modalità "Monitora" e scelto di tracciare la categoria "security", un'opzione che consente di raccogliere eventi relativi alla sicurezza direttamente dai registri di sistema. Questa decisione era mirata a osservare eventi rilevanti per analisi di sicurezza. Lo screenshot mostra chiaramente l'impostazione corretta e l’opzione "security" selezionata.

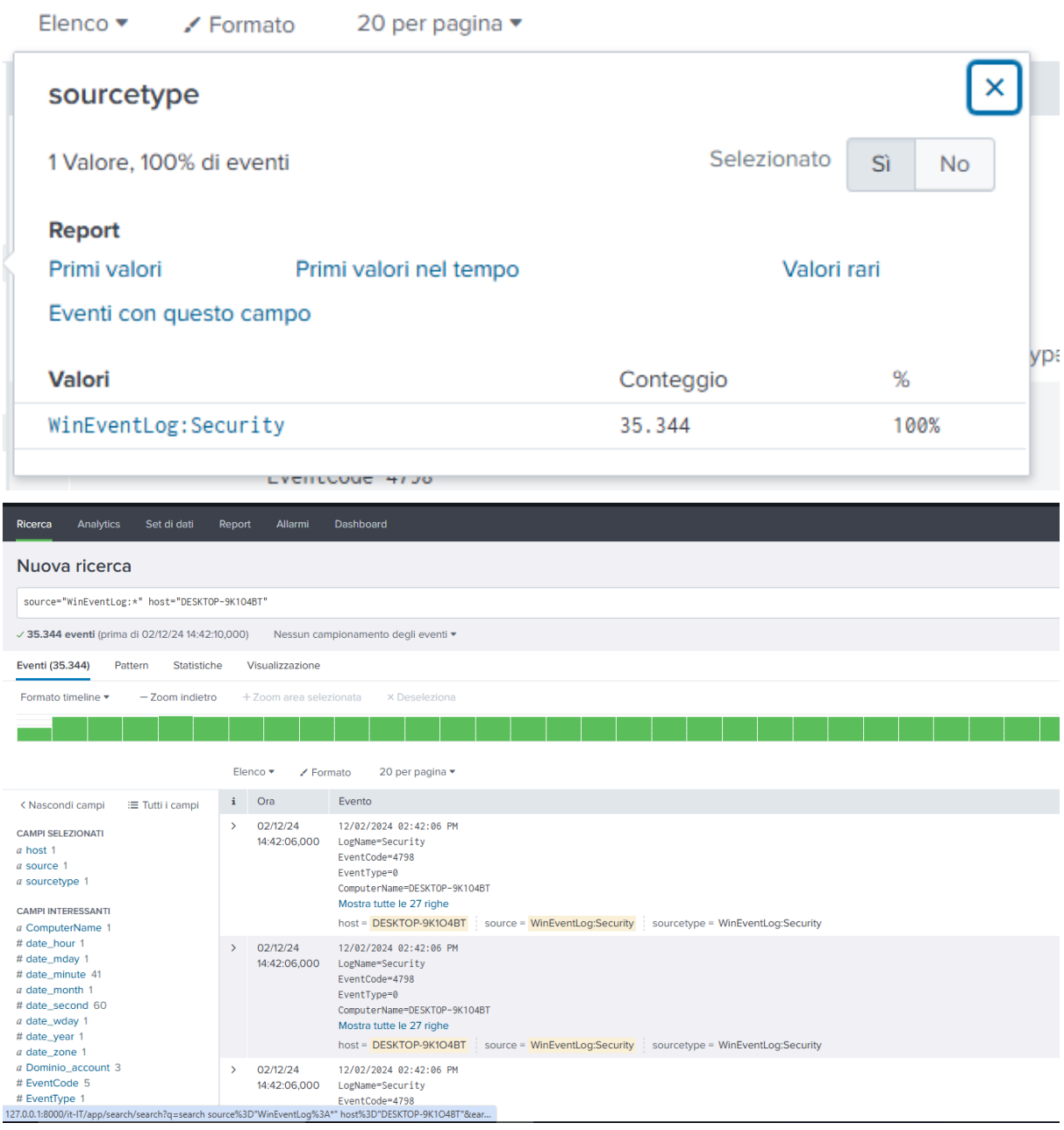


Ho poi proceduto a specificare le sorgenti dati da monitorare, indicando i percorsi dei file e applicando i filtri necessari per ottimizzare il processo di acquisizione. Questo passaggio garantisce che vengano raccolte solo informazioni pertinenti. Lo screenshot mostra il risultato di questa configurazione, con i parametri impostati in maniera dettagliata.



Infine, ho verificato che il monitoraggio fosse attivo e che Splunk stesse acquisendo i dati correttamente. In totale, il sistema ha rilevato 35.344 eventi, tutti provenienti dai registri di

sistema, a conferma del successo dell'operazione. Lo screenshot documenta la visualizzazione di questi risultati nella dashboard di Splunk, con gli eventi aggiornati in tempo reale.



L’attività ci ha permesso di capire quanto Splunk sia utile per monitorare e analizzare i dati, soprattutto quando si tratta di eventi legati alla sicurezza. Configurare la modalità "Monitora" con la categoria "security" si è rivelato un ottimo modo per raccogliere informazioni importanti dai registri di sistema. Questo mi ha permesso di vedere chiaramente le attività monitorate e di capire come Splunk possa essere davvero efficace per gestire eventi critici e migliorare la sicurezza.