Task 16/01/25: File di Log di Windows

Traccia

Obiettivo dell'Esercizio:

Configurare e gestire i file di log della sicurezza utilizzando il Visualizzatore eventi di Windows.

Passaggi da Seguire:

1. Accedere al Visualizzatore Eventi:

- Apri il Visualizzatore eventi premendo Win + R per aprire la finestra "Esegui".
- Digita eventvwr e premi Invio.

2. Configurare le Proprietà del Registro di Sicurezza:

- Nel pannello di sinistra, espandi "Registri di Windows" e seleziona "Sicurezza".

Task 16/01/25: File di Log di Windows

Report

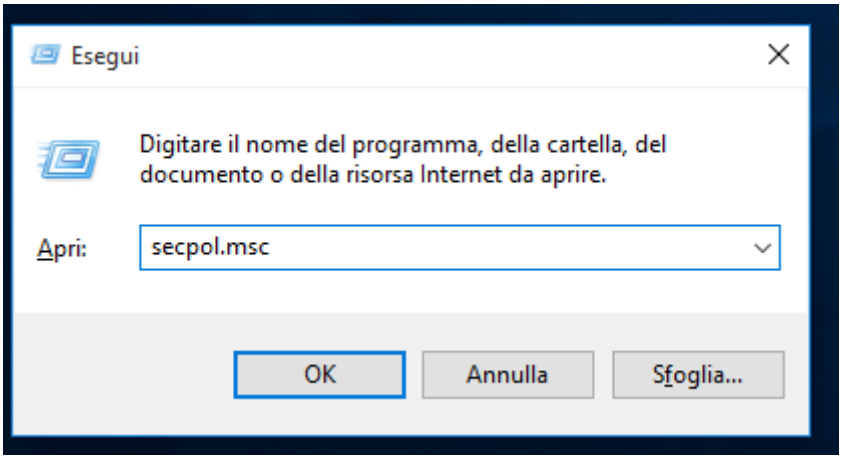
Introduzione:

In questa attività, ho configurato il sistema operativo Windows per monitorare e registrare gli eventi di accesso al sistema, inclusi login riusciti e falliti. Sono stati utilizzati strumenti integrati come i Criteri di Sicurezza Locali e il Visualizzatore Eventi per abilitare il controllo, gestire i log di sicurezza e creare visualizzazioni personalizzate per semplificare l'analisi degli eventi. Questo approccio consente una migliore gestione della sicurezza del sistema.

1. Abilitazione del Monitoraggio tramite i Criteri di Sicurezza Locali

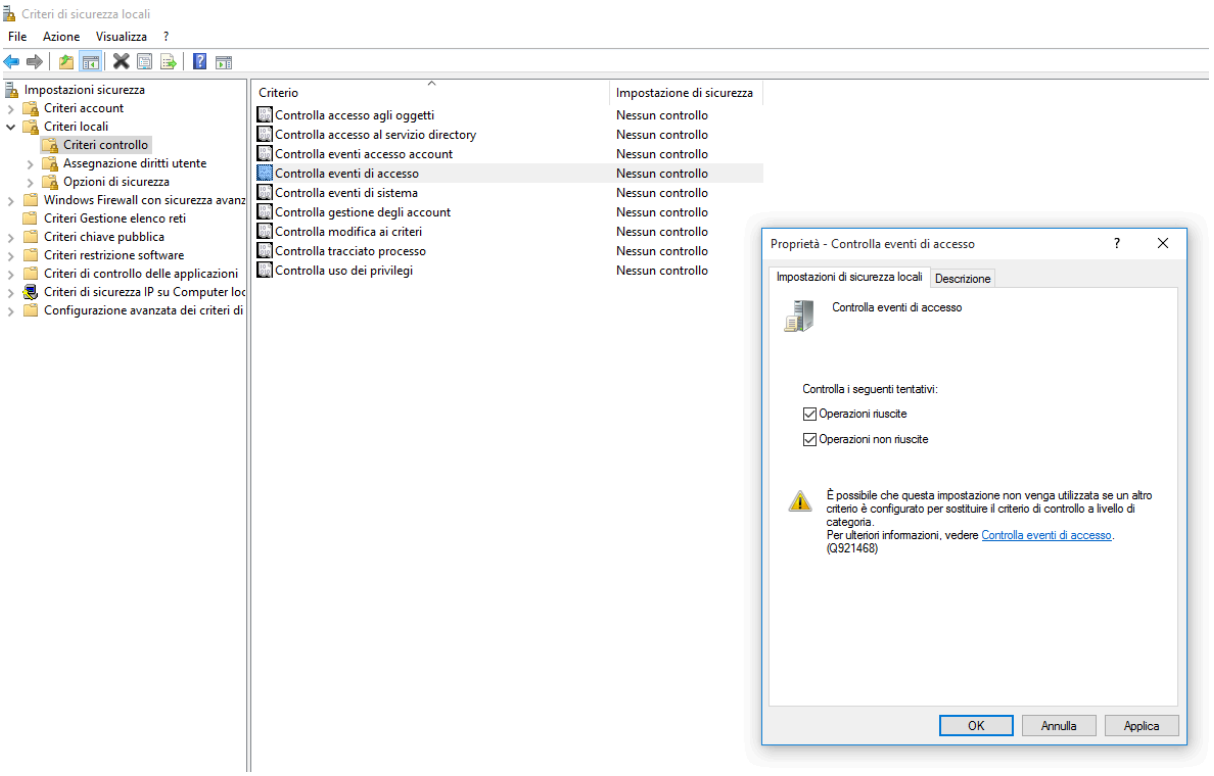
Accesso ai Criteri di Sicurezza Locali

- Aperta la finestra "Esegui" con Win + R.
- Digitato il comando secpol.msc e premuto Invio.



Configurazione dei Criteri di Controllo

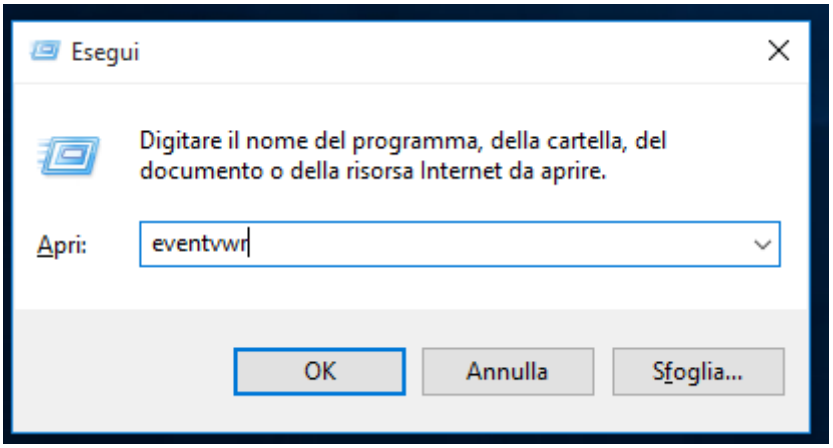
- Navigato in Criteri Locali > Criteri di Controllo.
- Modificata l'impostazione Controlla eventi di accesso:
    - Selezionato Operazioni riuscite e Operazioni non riuscite.



2. Configurazione del Registro di Sicurezza

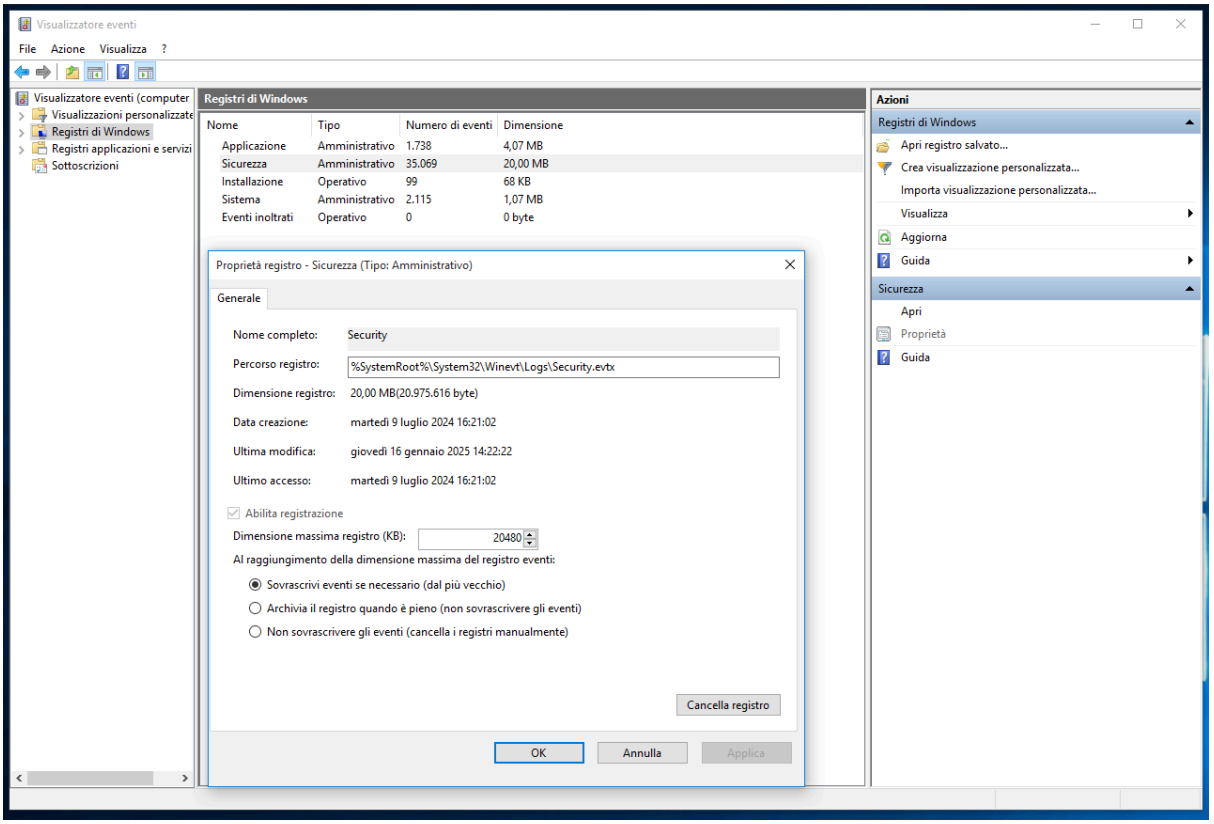
Accesso al Visualizzatore Eventi

- Aperta la finestra "Esegui" con Win + R.
- Digitato il comando eventvwr e premuto Invio.



Gestione delle Proprietà del Registro di Sicurezza

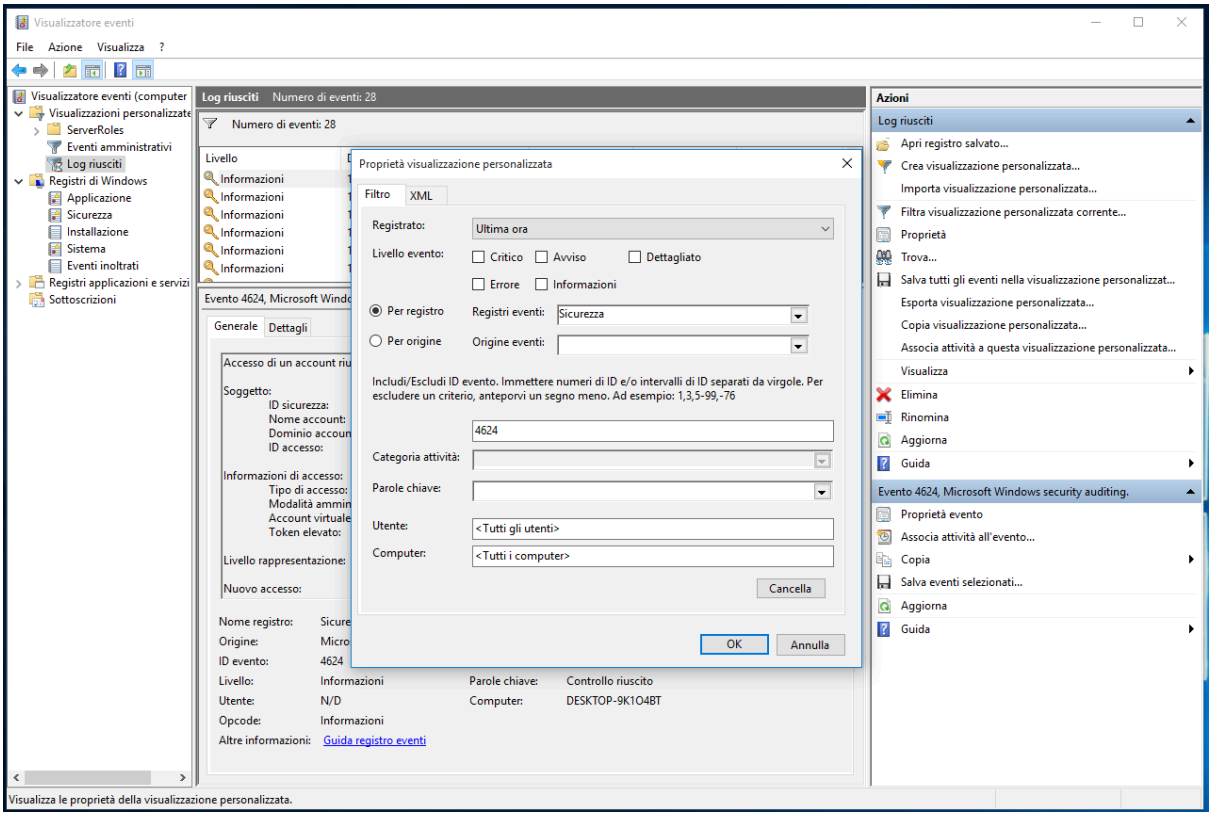
- Acceduto a Registri di Windows > Sicurezza.
- Modificate le seguenti impostazioni:
    - Dimensione massima del registro impostata a 20 MB.
    - Selezionato Sovrascrivi eventi se necessario.



3. Creazione di Visualizzazioni Personalizzate

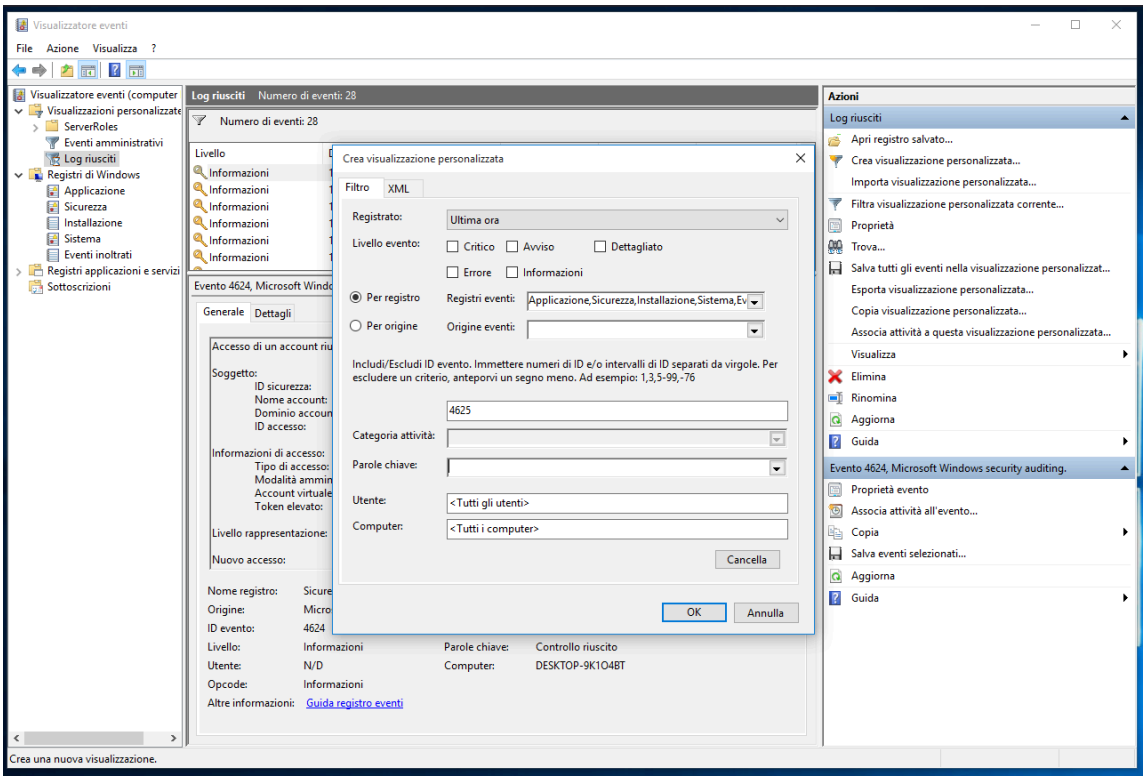
Visualizzazione per Login Riusciti

- Creato un filtro per registrare eventi con ID 4624 (accesso riuscito).



Visualizzazione per Login Falliti

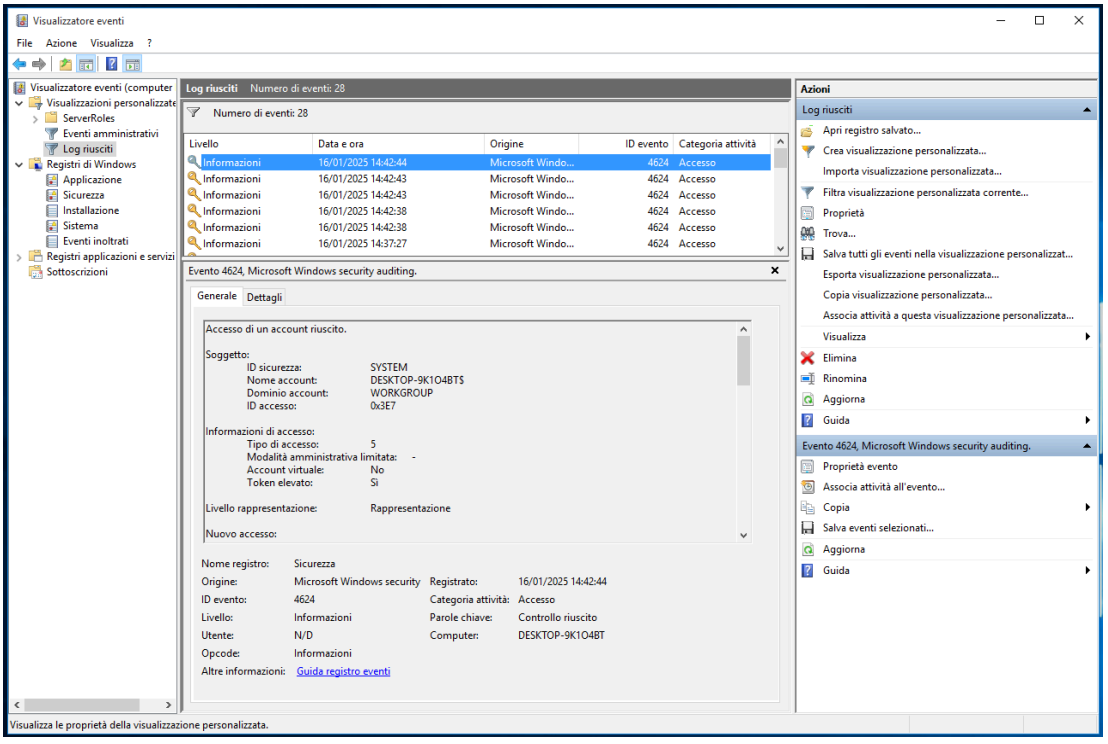
- Creato un filtro per registrare eventi con ID 4625 (accesso fallito).



Risultati Ottenuti

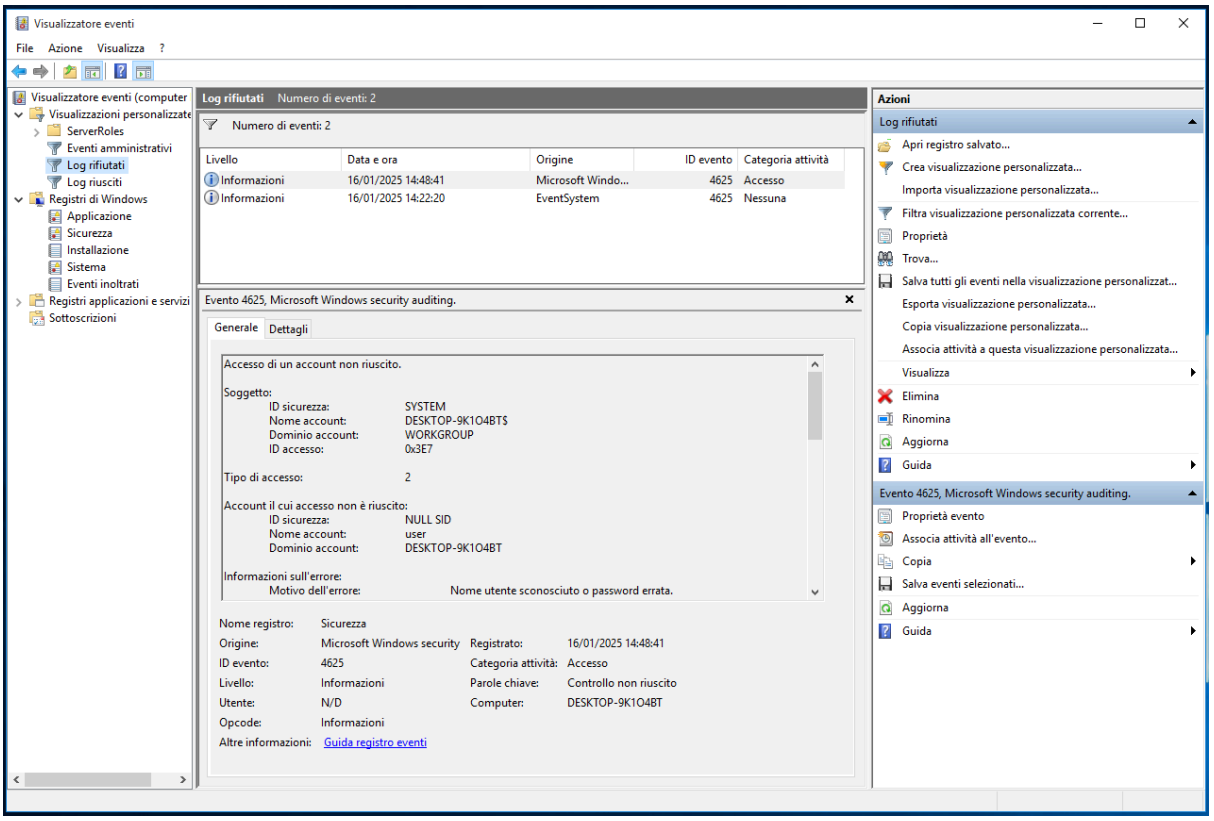
Login Riusciti (ID 4624)

- Evento registrato con dettagli completi sul nome account, dominio e tipo di accesso.



Login Falliti (ID 4625)

- Evento registrato con dettagli su nome utente errato o password non valida.



Conclusioni

La configurazione effettuata consente di:

- Monitorare efficacemente tutti gli accessi al sistema (riusciti e falliti).
- Gestire e analizzare i log di sicurezza tramite visualizzazioni personalizzate.
- Ottimizzare l'uso dello spazio per i registri e garantire la sovrascrittura automatica degli eventi più vecchi.