Configurazione e Analisi dei Log di Sicurezza Windows

1. Introduzione

Nell'ambito della gestione della sicurezza dei sistemi operativi, la capacità di monitorare chi accede al sistema e quando lo fa è fondamentale. In questa sessione, mi sono occupato di configurare il "Visualizzatore Eventi" (Event Viewer) aspetto cruciale spesso trascurato, di abilitare le policy di auditing necessarie affinché il sistema registri effettivamente i tentativi di accesso (Login) e di uscita (Logoff/Logon). L'obiettivo non è solo vedere una lista di eventi, ma capire come generarli e interpretarli per scopi forensi o di troubleshooting.

2. Strumenti Utilizzati

Per questo laboratorio virtuale ho utilizzato:

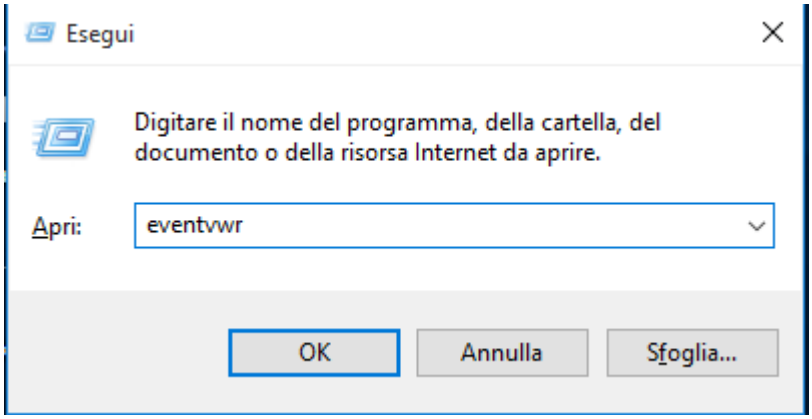
- **VirtualBox:** Per isolare l'ambiente di test.
- **Windows OS (Guest):** Il sistema target.
- **Event Viewer (eventvwr):** Per la consultazione dei log.
- **Local Security Policy (secpol.msc):** *Strumento essenziale* per dire a Windows di iniziare a tracciare gli eventi (senza questo, il Visualizzatore Eventi rimarrebbe muto su molti aspetti).

3. Svolgimento dell'Esercizio

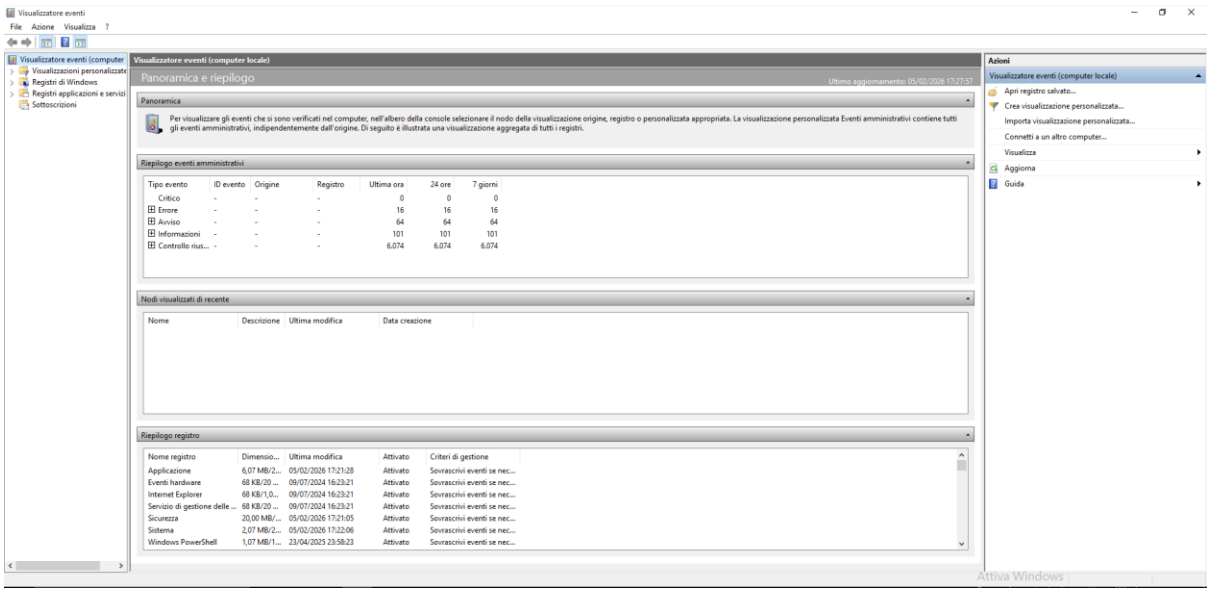
Accesso e Configurazione Iniziale del Log

Come prima cosa, ho seguito le istruzioni base per accedere allo strumento di log.

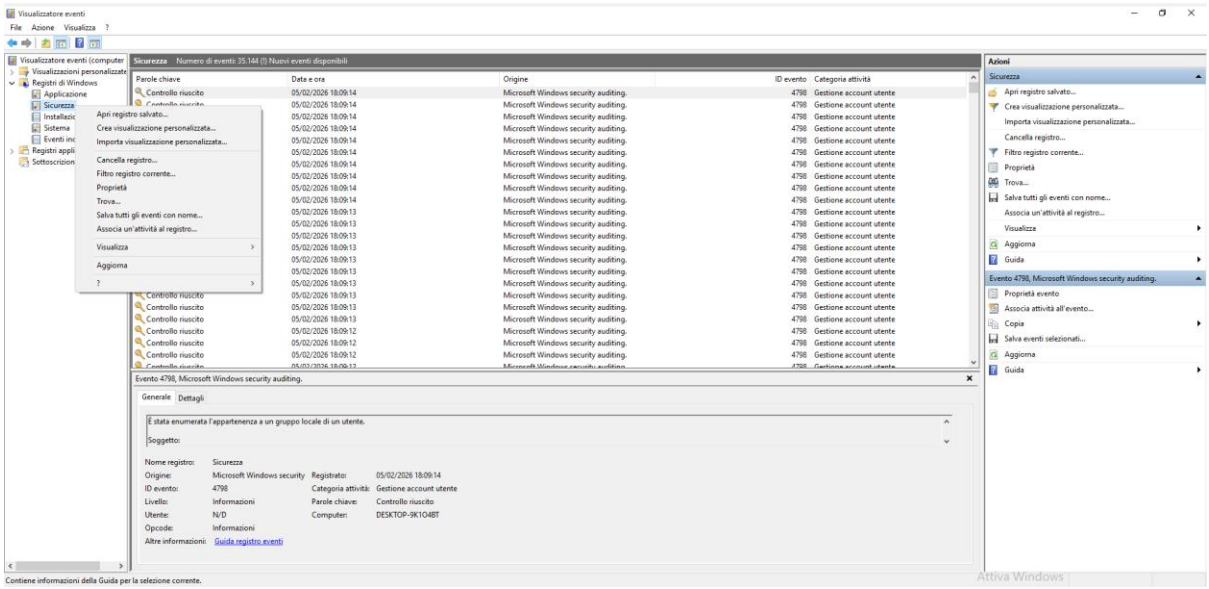
1. Ho premuto la combinazione di tasti Win + R sulla tastiera della macchina virtuale.
2. Nella finestra "Esegui", ho digitato il comando:



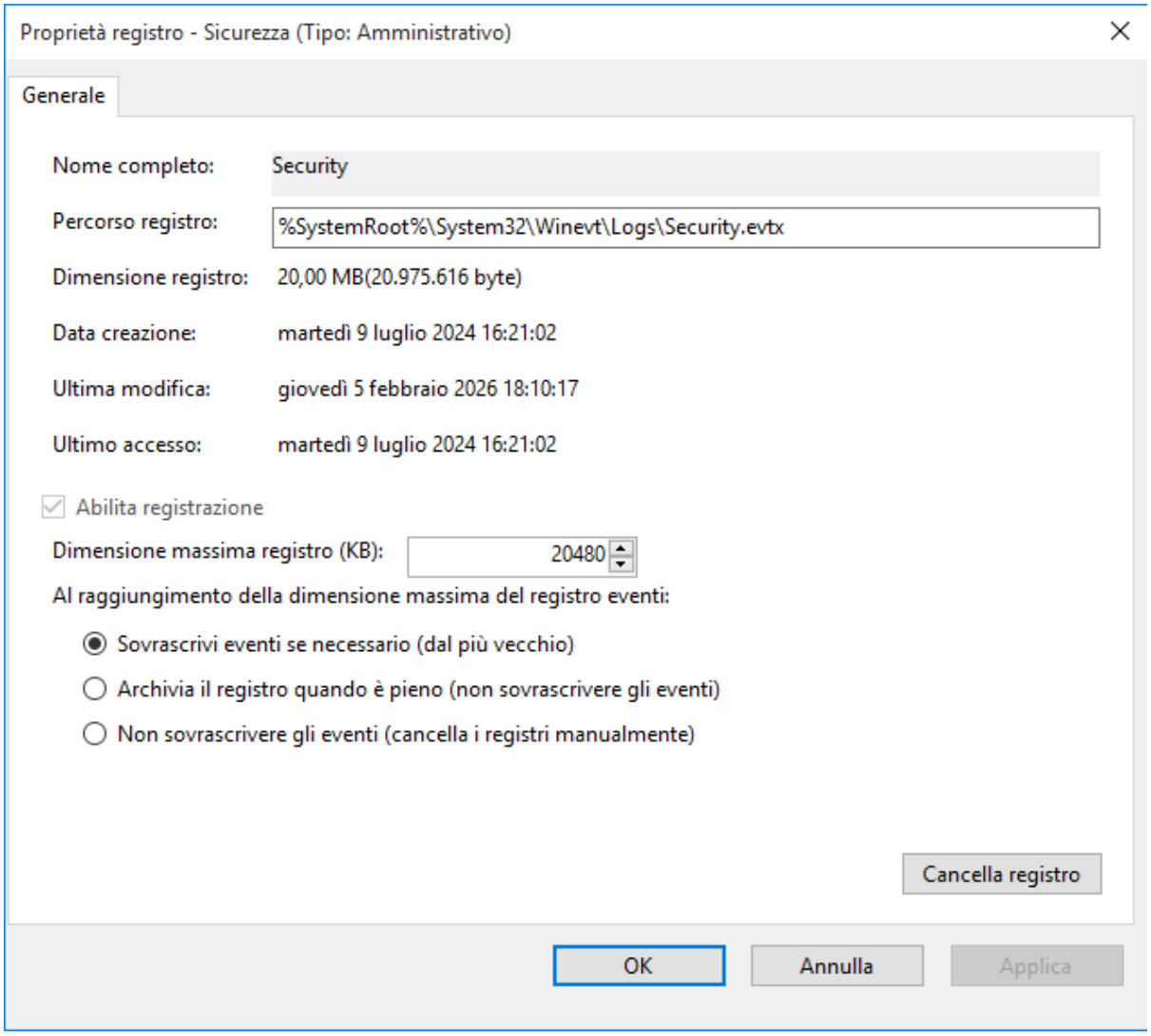
3. Ho premuto Invio. Si è aperta la console "Visualizzatore Eventi".



Una volta aperto, mi sono diretto nel pannello di sinistra, espandendo la voce **Registri di Windows** e cliccando su **Sicurezza**. Qui ho notato una lista di eventi. Tuttavia, l'esercizio richiedeva di "Configurare le Proprietà".



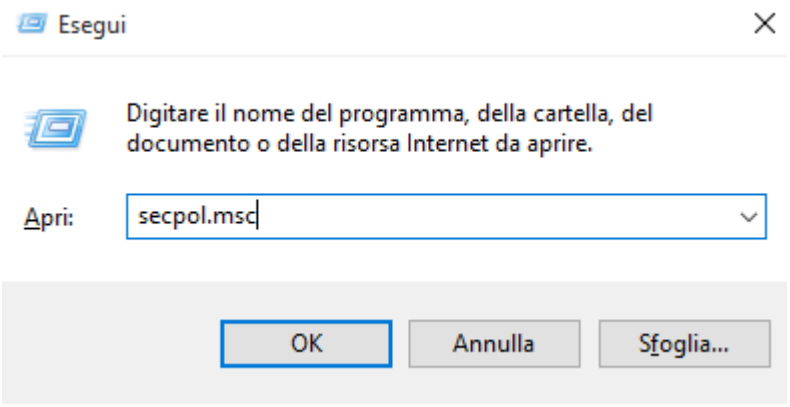
4. Ho fatto click destro su **Sicurezza** -> **Proprietà**.
    a. *Perché lo faccio?* Qui è dove decido quanto spazio dedicare ai log. Se il file si riempiesse, potrei perdere dati vecchi o bloccare il sistema (in configurazioni estreme).
    b. Ho verificato che l'opzione "Sovrascrivi eventi se necessario" fosse attiva, per evitare che il log si blocchi una volta pieno.



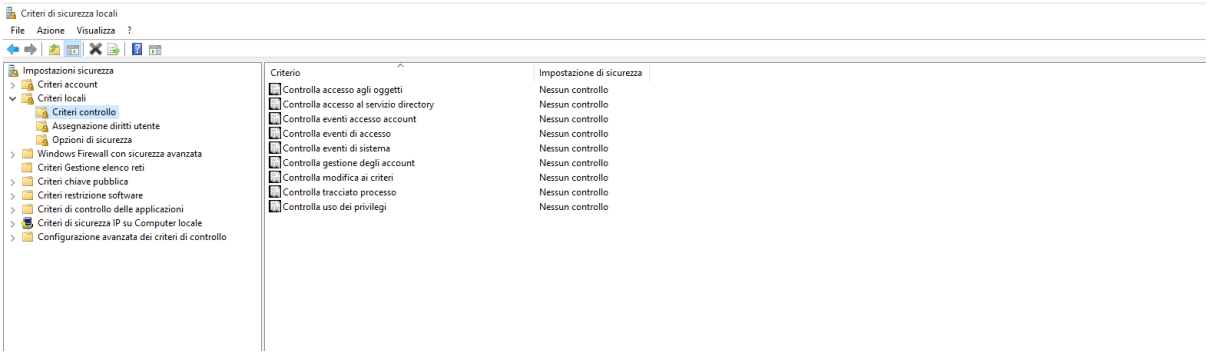
L'attivazione delle Regole (Il passaggio cruciale)

L'esercizio chiede: *"Provate a impostare il log dei Login/Logoff"*. Qui c'è un dettaglio tecnico importante: il Visualizzatore Eventi *legge* i dati, ma non decide *cosa* registrare. Per registrare i login, devo attivare una **Policy di Audit**. Se non lo facessi potrei fare login mille volte e non vedere nulla.

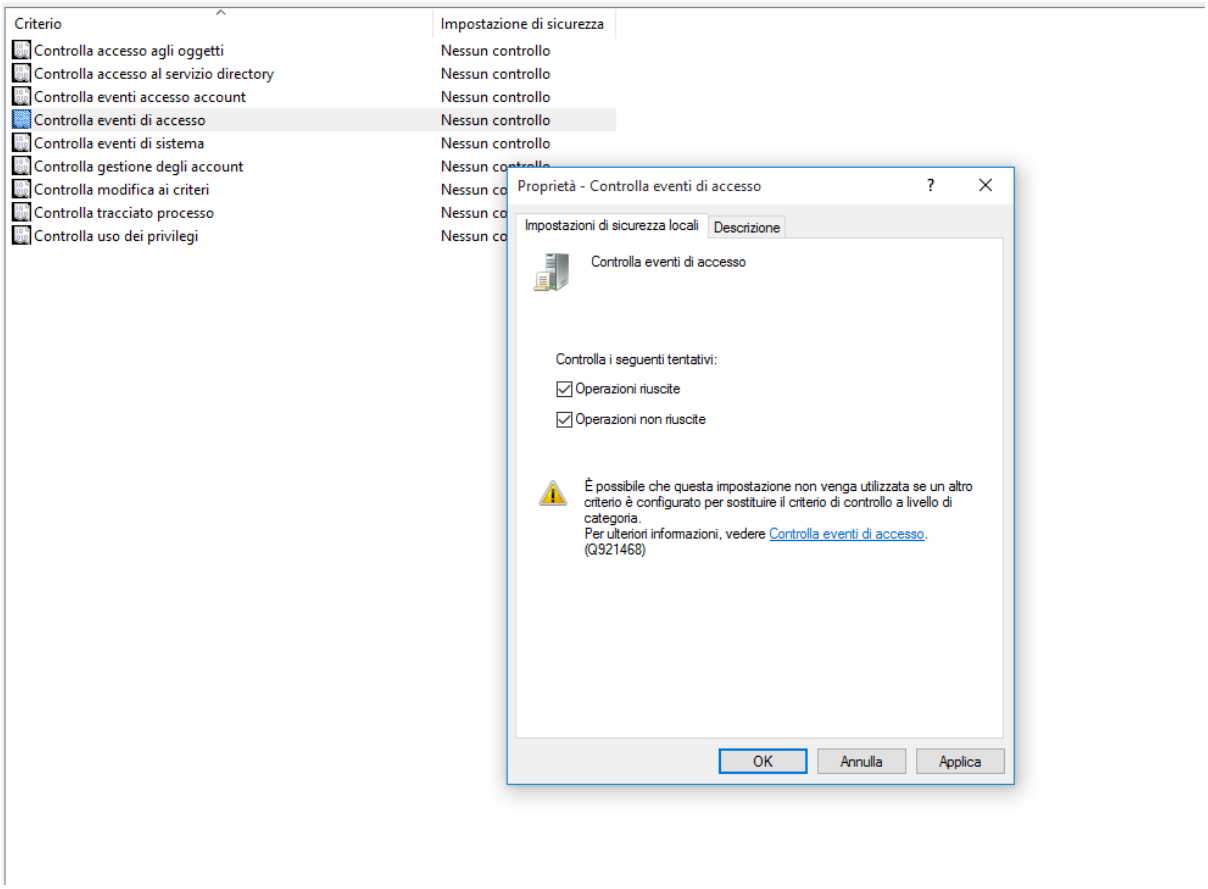
1. Ho aperto nuovamente Win + R.
2. Ho digitato questo comando per aprire le policy di sicurezza locali:



3. Ho navigato in: **Criteri Locali (Local Policies)** -> **Criteri controllo (Audit Policy)**.



4. Nel pannello di destra, ho fatto doppio click su **Controlla eventi di accesso (Audit logon events)**.
5. Ho spuntato entrambe le caselle:



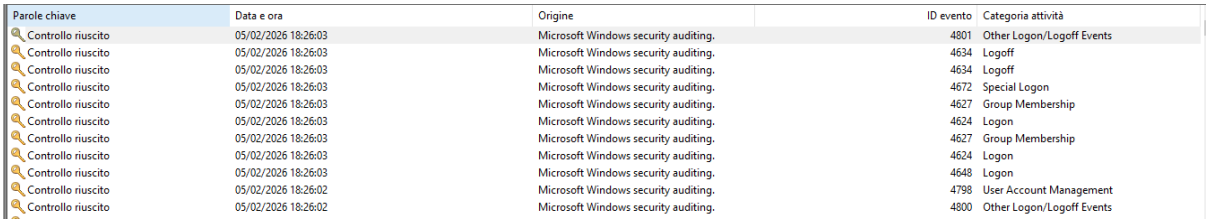
Selezionare quelle non riuscite è vitale per scoprire se qualcuno sta cercando di indovinare la password (attacco Brute Force).

Generazione dei Dati (Test Pratico)

Per verificare che la configurazione funzionasse, non mi sono limitato a guardare lo schermo. Ho "stressato" il sistema per generare dei log reali.

Tentativo 1: Accesso Corretto

1. Ho premuto Win + L per bloccare la macchina virtuale.
2. Ho inserito la password corretta e sono rientrato.



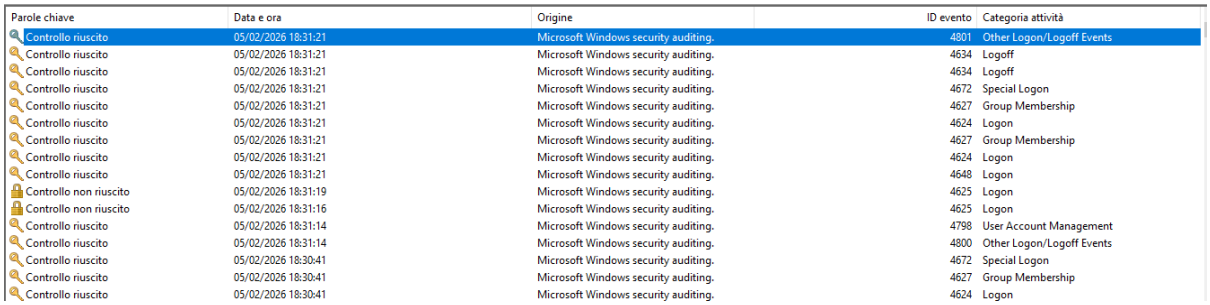
Parole chiave	Data e ora	Origine	ID evento	Categoria attività
Controllo riuscito	05/02/2026 18:26:03	Microsoft Windows security auditing.	4801	Other Logon/Logoff Events
Controllo riuscito	05/02/2026 18:26:03	Microsoft Windows security auditing.	4634	Logoff
Controllo riuscito	05/02/2026 18:26:03	Microsoft Windows security auditing.	4634	Logoff
Controllo riuscito	05/02/2026 18:26:03	Microsoft Windows security auditing.	4672	Special Logon
Controllo riuscito	05/02/2026 18:26:03	Microsoft Windows security auditing.	4627	Group Membership
Controllo riuscito	05/02/2026 18:26:03	Microsoft Windows security auditing.	4624	Logon
Controllo riuscito	05/02/2026 18:26:03	Microsoft Windows security auditing.	4627	Group Membership
Controllo riuscito	05/02/2026 18:26:03	Microsoft Windows security auditing.	4624	Logon
Controllo riuscito	05/02/2026 18:26:03	Microsoft Windows security auditing.	4648	Logon
Controllo riuscito	05/02/2026 18:26:02	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	05/02/2026 18:26:02	Microsoft Windows security auditing.	4800	Other Logon/Logoff Events

Analisi Tecnica per il tentativo riuscito

- **Logon:** È presente più volte (alle 18:26:03). Questo è l'evento fondamentale dell'esercizio. Indica che un utente ha effettuato l'accesso al sistema con successo. È la "firma" digitale del tuo login corretto.
- **Special Logon:** Appare subito dopo il login. Indica che l'utente che è entrato ha privilegi amministrativi (o speciali). È tipico quando accedi come Administrator o con un utente che ha poteri elevati.
- **Logoff:** Indica la chiusura di una sessione. È normale vederli insieme ai login, perché Windows apre e chiude diverse "sotto-sessioni" di sistema in background durante l'uso.
- **Group Membership:** Elenca i gruppi di cui fa parte l'utente che ha appena fatto log-in (utile per vedere se è davvero un amministratore).
- **Timestamp:** Vedo che gli eventi sono tutti concentrati nello stesso secondo (18:26:03). Questo dimostra come un singolo "click" per accedere scateni in realtà una cascata di controlli di sicurezza che ora sei in grado di vedere.

Tentativo 2: Accesso Fallito (Simulazione intrusione)

1. Ho bloccato nuovamente la macchina (Win + L).
2. Ho provato a inserire una password *sbagliata* per due volte.
3. Poi ho inserito quella giusta per rientrare.



Parole chiave	Data e ora	Origine	ID evento	Categoria attività
Controllo riuscito	05/02/2026 18:31:21	Microsoft Windows security auditing.	4801	Other Logon/Logoff Events
Controllo riuscito	05/02/2026 18:31:21	Microsoft Windows security auditing.	4634	Logoff
Controllo riuscito	05/02/2026 18:31:21	Microsoft Windows security auditing.	4634	Logoff
Controllo riuscito	05/02/2026 18:31:21	Microsoft Windows security auditing.	4672	Special Logon
Controllo riuscito	05/02/2026 18:31:21	Microsoft Windows security auditing.	4627	Group Membership
Controllo riuscito	05/02/2026 18:31:21	Microsoft Windows security auditing.	4624	Logon
Controllo riuscito	05/02/2026 18:31:21	Microsoft Windows security auditing.	4627	Group Membership
Controllo riuscito	05/02/2026 18:31:21	Microsoft Windows security auditing.	4624	Logon
Controllo riuscito	05/02/2026 18:31:21	Microsoft Windows security auditing.	4648	Logon
Controllo non riuscito	05/02/2026 18:31:19	Microsoft Windows security auditing.	4625	Logon
Controllo non riuscito	05/02/2026 18:31:16	Microsoft Windows security auditing.	4625	Logon
Controllo riuscito	05/02/2026 18:31:14	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	05/02/2026 18:31:14	Microsoft Windows security auditing.	4800	Other Logon/Logoff Events
Controllo riuscito	05/02/2026 18:30:41	Microsoft Windows security auditing.	4672	Special Logon
Controllo riuscito	05/02/2026 18:30:41	Microsoft Windows security auditing.	4627	Group Membership
Controllo riuscito	05/02/2026 18:30:41	Microsoft Windows security auditing.	4624	Logon

Analisi Tecnica per il tentativo fallito

1. **L'Evento "Fumante": ID 4625** Nello screenshot saltano subito all'occhio due righe con l'icona del lucchetto e la dicitura **"Controllo non riuscito"**.
    a. L'ID evento associato è **4625**.

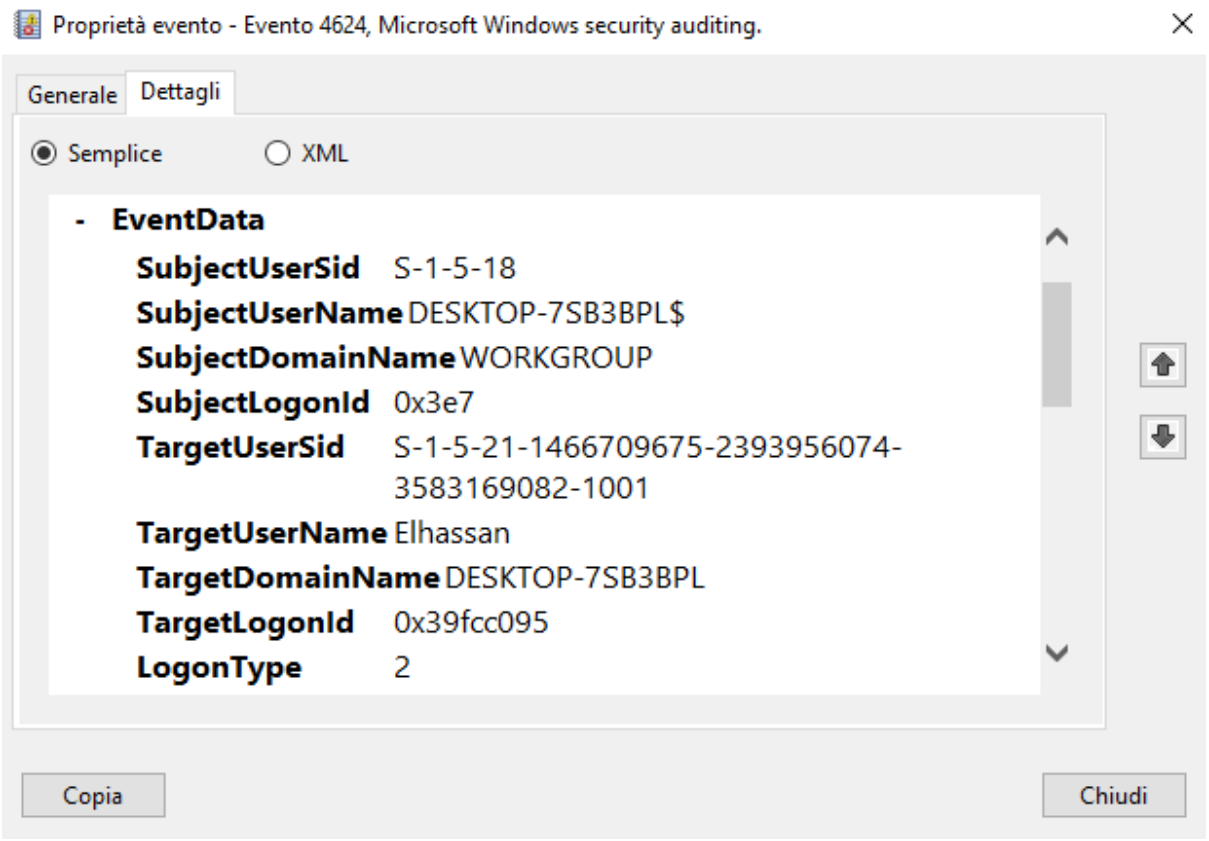
    b. Questo è il codice specifico per "An account failed to log on". È la prova che il sistema ha rilevato un tentativo di intrusione o un errore di digitazione della password.
2. **La Sequenza Temporale (Lo "Storytelling" del Log)** Guardando le date e gli orari (colonna "Data e ora"), si può ricostruire esattamente cosa è successo:
    a. **18:31:16:** Primo errore (Controllo non riuscito, ID 4625).
    b. **18:31:19:** Secondo errore (Controllo non riuscito, ID 4625).
    c. **18:31:21:** Successo (Controllo riuscito, ID 4624 e 4648).
    d. *Interpretazione:* L'utente ha sbagliato la password due volte in rapida successione (a distanza di 3 secondi) e infine è riuscito ad entrare correttamente due secondi dopo l'ultimo errore.
3. **Conferma della Policy "Failure"** La presenza di queste righe conferma che nel passaggio precedente (dentro secpol.msc) hai spuntato correttamente la casella **"Operazione non riuscita" (Failure)**. Se non l'avessi fatto, avresti visto solo l'accesso finale delle 18:31:21, perdendo completamente traccia dei tentativi errati precedenti.

Analisi dei Risultati

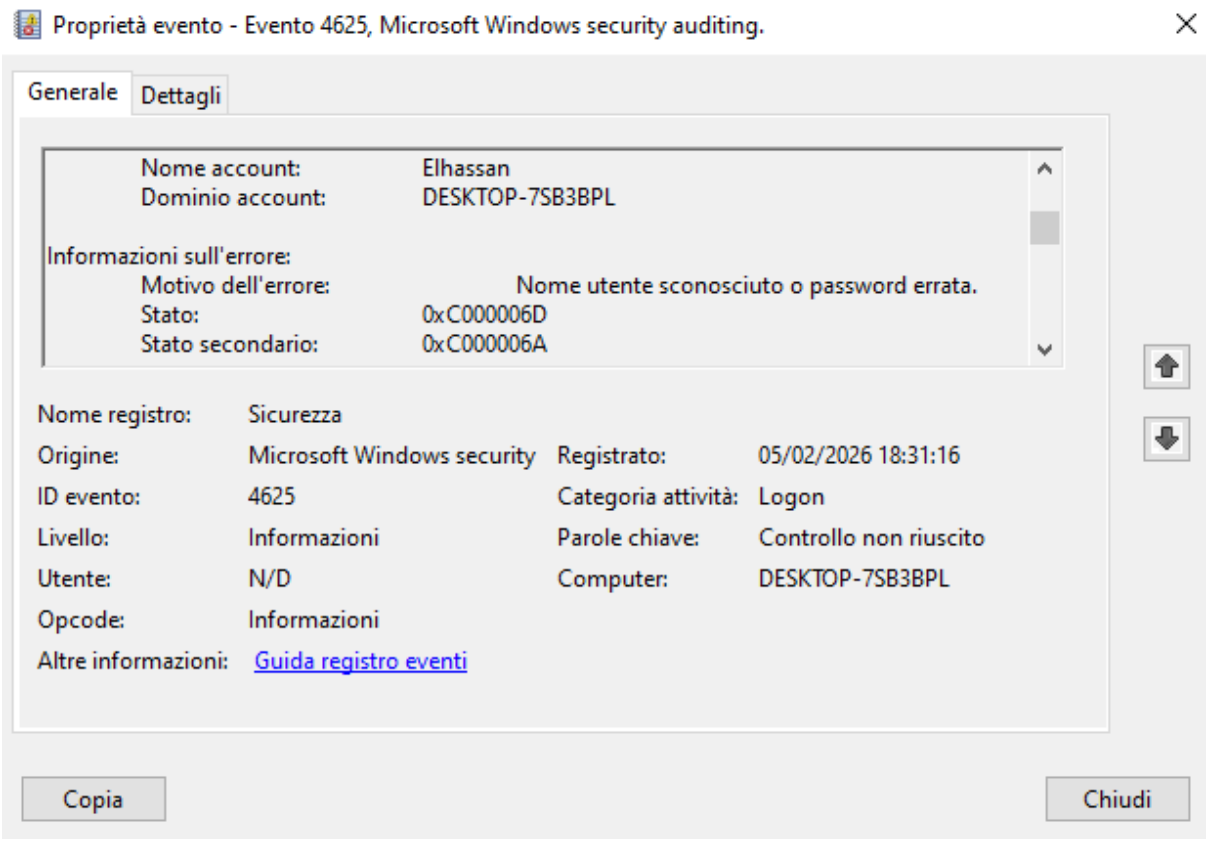
Sono tornato sul **Visualizzatore Eventi** (eventvwr). Ho cliccato su **Sicurezza** e ho premuto F5 per aggiornare la lista (i log non compaiono in tempo reale se non si aggiorna).

Ecco cosa ho trovato analizzando i codici evento (Event ID):

- **Analisi Evento 4624 (Logon Success):** Ho cercato l'ID **4624**. Cliccandoci sopra, nel pannello in basso (proprio come nell'immagine 2 fornita traccia), ho letto i dettagli.
    - *Cosa mi dice:* Conferma che l'utente (io) ha effettuato l'accesso con successo.
    - *Dettaglio chiave:* "Tipo di accesso". Se vedo 2 o 7, è un utente fisico. Se vedo 3, è un accesso via rete.



- **Analisi Evento 4625 (Logon Failure - Il più interessante):** Ho cercato l'ID **4625**. Questo è il risultato del mio "Tentativo 2".
    - *Analisi:* Il log mi mostrava chiaramente che c'è stato un tentativo fallito. Leggendo i dettagli, Windows riportava "Unknown user name or bad password".
    - *Riflessione:* Se vedessi 100 di questi eventi in un minuto, saprei di essere sotto attacco.



4. Conclusione

Attraverso questo esercizio ho compreso che il **Visualizzatore Eventi** è solo la "vetrina" dei dati. La vera configurazione di sicurezza avviene a monte, tramite le **Local Security Policies (secpol.msc)**. Impostare il log di Login/Logoff (Success/Failure) è la prima linea di difesa per capire cosa accade nel sistema. Senza aver attivato manualmente l'auditing nella Fase B, il visualizzatore eventi sarebbe rimasto parzialmente cieco sui tentativi di intrusione. L'esercizio ha confermato che ogni azione (blocco schermo, errore password, accesso) lascia una traccia digitale precisa (ID 4624, 4625) che può essere analizzata.