

REPORT S9/L4: Analisi e Gestione dei Log di Sicurezza Windows

Studente: Vincenzo Zarola

Corso: Cybersecurity Specialist

1. Obiettivo dell'Esercitazione

L'obiettivo dell'attività è acquisire familiarità con il **Visualizzatore Eventi (Event Viewer)** di Windows, strumento fondamentale per il monitoraggio della sicurezza. Nello specifico, l'esercizio si concentra sulla configurazione, l'identificazione e l'analisi degli eventi di accesso (Logon/Logoff) per monitorare chi accede al sistema e con quali privilegi.

2. Definizioni Tecniche

Prima di procedere all'analisi pratica, è fondamentale definire le tipologie di eventi monitorati nel registro "Security":

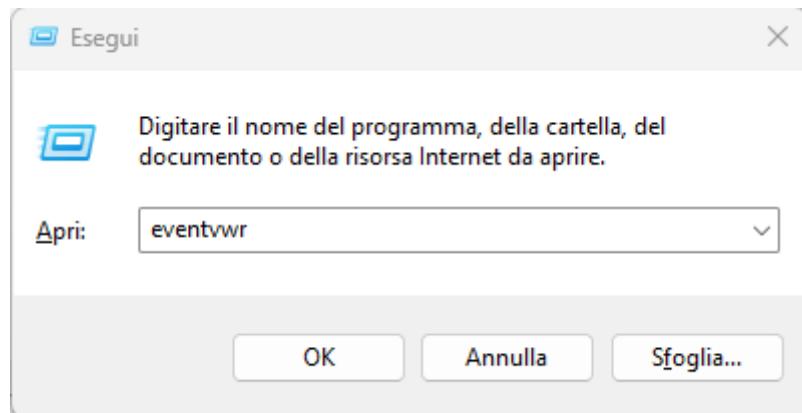
- **Logon (ID Evento 4624):** Indica un **Accesso Riuscito**. Questo evento viene generato ogni volta che un utente (o un servizio) si autentica correttamente nel sistema.
 - *Nota:* Windows distingue vari "Tipi di accesso" (es. Tipo 2 = Tastiera/Schermo, Tipo 3 = Via Rete).
 - **Logoff (ID Evento 4634 / 4647):** Indica la **Disconnessione**.
 - L'evento viene generato quando una sessione di accesso viene terminata. L'ID 4647 è specifico per quando è l'utente a cliccare volontariamente su "Disconnetti" o a riavviare.
 - **Special Logon (ID Evento 4672):** Indica l'assegnazione di **Privilegi Speciali**.
 - Questo è l'evento più critico per la sicurezza. Non indica un nuovo accesso, ma accompagna un normale Logon (4624) quando l'utente che entra ha poteri di **Amministratore** (es. Administrator, SYSTEM). Significa che quell'utente ha il potere di modificare il sistema operativo.
-

3. Procedura Esecutiva

Fase 1: Accesso agli Strumenti di Monitoraggio

Per accedere ai log di sistema, è stato utilizzato lo strumento nativo di Windows.

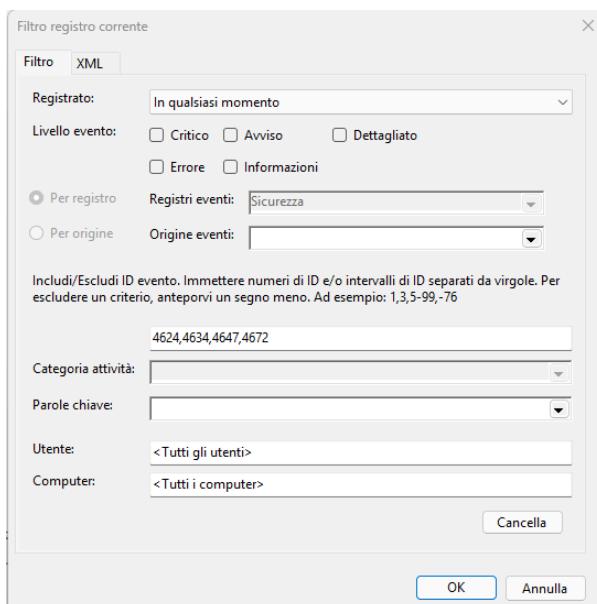
1. Apertura della finestra "Esegui" tramite combinazione tasti **Win + R**.
2. Esecuzione del comando **eventvwr** (Event Viewer).



Fase 2: Configurazione e Filtraggio

Una volta all'interno del Visualizzatore Eventi:

1. È stata selezionata la sezione "**Registri di Windows**" > "**Sicurezza**".
2. È stato verificato che la Policy di Audit fosse attiva (il sistema stava già registrando gli eventi).
3. Per isolare le informazioni rilevanti dal "rumore" di fondo del sistema, è stato applicato un **Filtro** specifico per visualizzare solo le attività di gestione sessione.



Fase 3: Analisi dei Risultati

L'analisi del registro ha evidenziato la presenza delle tre categorie di eventi ricercate.

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: Application, Security, System, and Event logs under the Windows Logs section. The right pane is titled 'Sicurezza' and shows a list of security events. A filter bar at the top indicates 'Filtro: Registro Security; Origine: ID evento: 4624,4634,4647,4672; Numero di eventi: 5,316'. The event list includes columns for Parole..., Data e ora, Origine, ID even..., CATEGORIA ATTIVITÀ, and Dettagli. Most events are categorized as 'Special Logon' (ID 4672) or 'Logon' (ID 4624). The events show a sequence of logons and logoffs occurring between 05/02/2026 14:58:47 and 05/02/2026 14:42:47. The right-hand pane also contains an 'Azioni' (Actions) menu with options like 'Crea visualizzazione personalizzata...' (Create personalized visualization...) and 'Proprietà' (Properties).

Osservazioni sui dati raccolti: Dallo screenshot sopra riportato è possibile notare la sequenza temporale delle azioni:

- Gli eventi **Logon (4624)** mostrano l'ingresso dell'utente nel sistema.
- Gli eventi **Special Logon (4672)** appaiono contemporaneamente ai Logon, confermando che l'utente corrente possiede diritti amministrativi (comportamento tipico dell'utente proprietario su Windows 10/11).
- Gli eventi **Logoff** tracciano la chiusura delle sessioni o dei processi in background.

4. Conclusioni

L'esercizio ha dimostrato come Windows tracci dettagliatamente ogni tentativo di accesso. La capacità di distinguere un "Logon standard" da uno "Special Logon" è cruciale per un analista di sicurezza: un evento **4672 (Special Logon)** generato da un utente che non dovrebbe essere amministratore è un chiaro indicatore di compromissione (**Privilege Escalation**) o di errata configurazione dei permessi.