Report Esercitazione: Configurazione e Analisi dei Log di Sicurezza Windows

Studente: Rocco Paolo Caccamo

Data: 05/02/2026

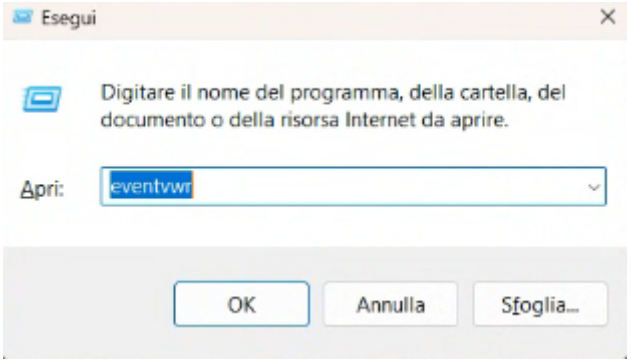
Obiettivo: Configurare le policy di auditing locale e analizzare gli eventi di accesso (Login/Logoff) tramite il Visualizzatore Eventi di Windows per monitorare la sicurezza del sistema.

---

1. Accesso agli Strumenti di Monitoraggio

Per accedere ai log di sistema, è stato utilizzato lo strumento nativo di Windows "Visualizzatore Eventi". **Procedura:**

- Apertura della finestra "Esegui" tramite shortcut `Win + R`.
- Esecuzione del comando `eventvwr`.



(Esecuzione del comando per l'apertura del tool di logging)

---

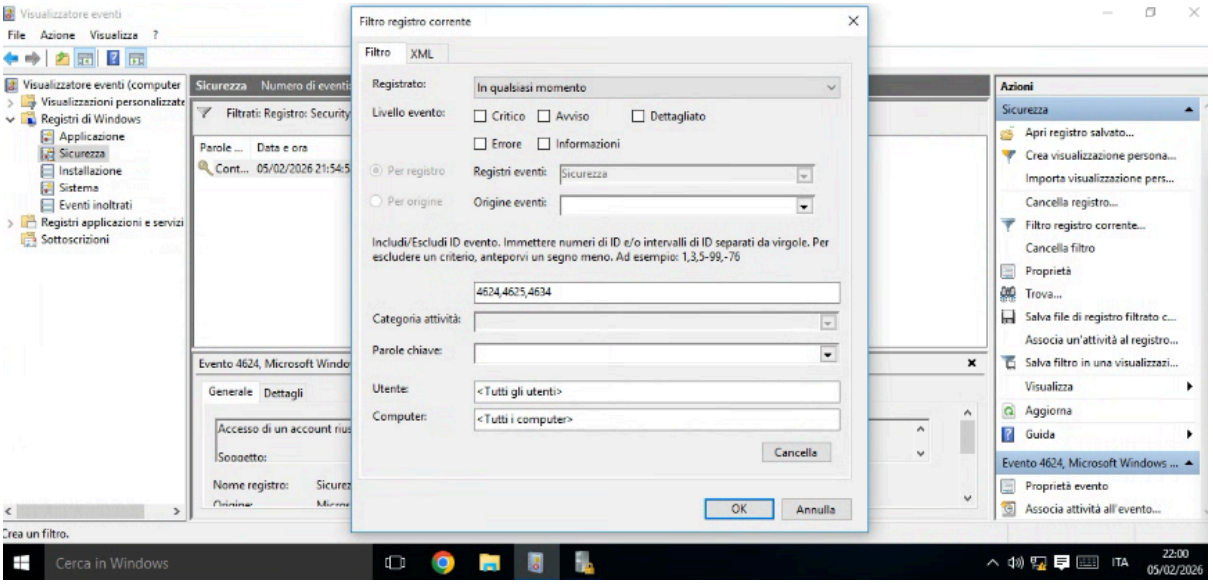
2. Configurazione e Analisi del Registro di Sicurezza

Una volta aperto il Visualizzatore Eventi, è stato selezionato il percorso **Registri di Windows > Sicurezza**. È stato verificato che il sistema stesse tracciando correttamente gli eventi di autenticazione.

Evidenza raccolta:

- È stato individuato l'**Evento ID 4624**, che corrisponde a un "Accesso di un account riuscito".

- Il sistema ha registrato la data, l'ora e l'utente che ha effettuato l'accesso.



(Visualizzazione dell'evento 4624 nel registro Sicurezza)

---

3. Analisi Tecnica dell'Evento

Dall'analisi del log catturato nello screenshot precedente, sono emersi i seguenti dettagli tecnici fondamentali per la sicurezza:

- **ID Evento:** 4624 (Logon Success).
- **Significato:** Conferma che un utente si è autenticato correttamente nel sistema.
- **Importanza per la Security:** Monitorare questi eventi permette di ricostruire la timeline di accesso degli utenti. In combinazione con l'evento **4625 (Logon Failure)**, è possibile rilevare tentativi di intrusione (es. Brute Force).
- **Dettagli aggiuntivi (Logon Type):** Analizzando i dettagli dell'evento, è possibile distinguere tra un accesso locale (Logon Type 2) e un accesso remoto via rete o RDP (Logon Type 3 o 10), cruciale per identificare movimenti laterali o accessi non autorizzati dall'esterno.

---

4. Conclusione

L'esercitazione ha permesso di verificare la corretta configurazione dei **Criteri di Controllo (Audit Policy)**. Il sistema è attualmente in grado di registrare e monitorare gli accessi, fornendo dati essenziali per attività di Forensics e Incident Response.