S9-L4
File log di Windows

Emanuele Benedetti | 6 febbraio 2025

Consegna

Obiettivo

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

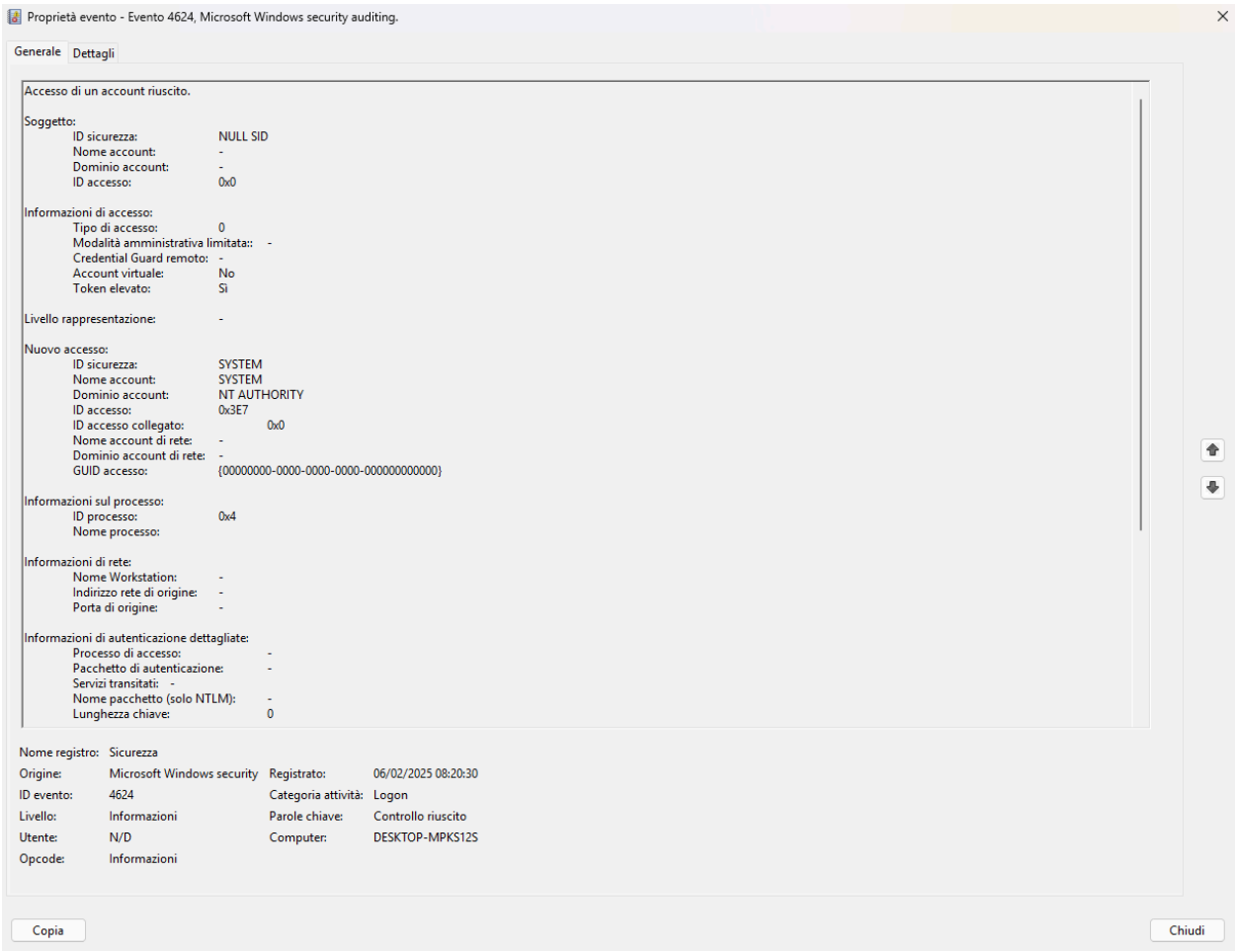
Istruzioni

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".
3. Analizzare gli eventi con Categoria Attività **Logon** e **Special Logon**

Svolgimento

Come richiesto dalla consegna ho avviato il Visualizzatore eventi della mia macchina Windows 11 per analizzare i log di sicurezza generati dal sistema.

Ho inizialmente deciso di analizzare il file log di tipo Logon che viene generato all'accensione del computer.



In questo caso il file è di tipo Logon con ID evento 4624, che rappresenta un accesso riuscito al sistema.

Di seguito ho riportato le caratteristiche principali presenti nelle informazioni del file log con delle brevi descrizioni dei campi analizzati.

Informazioni generali

- Nome registro: *Security*
    - Indica che l'evento è stato registrato nel registro di sicurezza di Windows.
- ID evento: *4624*
    - Questo ID rappresenta un accesso riuscito al sistema.
- Livello: *Informazioni*
    - Indica che si tratta di un evento informativo, non critico o di errore.
- Parole chiave: *Controllo riuscito*
    - Significa che l'accesso è stato completato con successo.

Analisi dei campi principali

1. Soggetto
    - ID sicurezza: *NULL SID*
        - L'account che ha richiesto l'accesso non è associato a un utente specifico (potrebbe essere un servizio o un processo di sistema).
    - Nome account: -
        - Nessun nome account associato al soggetto.
    - Dominio account: -
        - Nessun dominio associato al soggetto.
    - ID accesso: *0x0*
        - Identificatore dell'accesso, in questo caso vuoto (0x0).
2. Informazioni di accesso
    - Tipo di accesso: *0*
        - In questo caso, il valore 0 potrebbe indicare un accesso di sistema o un evento speciale.
    - Token elevato: *Sì*
        - Indica che l'account ha ottenuto privilegi elevati durante l'accesso.

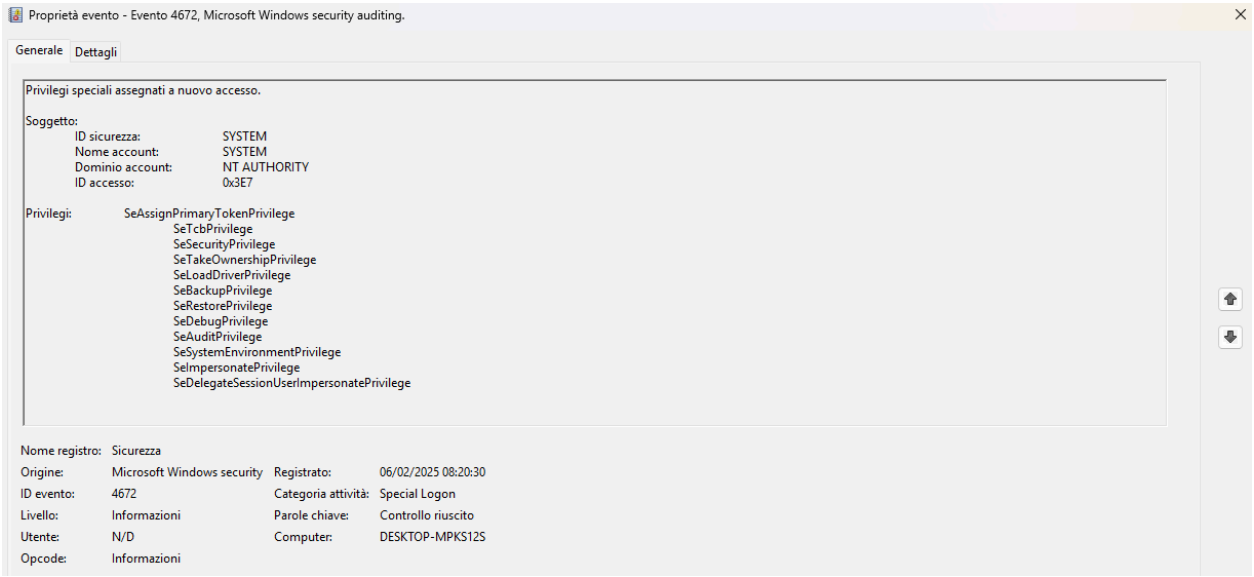
3. Nuovo accesso
    - ID sicurezza: *SYSTEM*
        - L'account che ha effettuato l'accesso è il sistema operativo stesso (SYSTEM).
    - Nome account: *SYSTEM*
        - L'account di sistema è un account privilegiato utilizzato da Windows per eseguire processi critici.
    - Dominio account: *NT AUTHORITY*
        - Indica che l'account appartiene al dominio locale del sistema (NT AUTHORITY).
    - ID accesso: *0x3E7*
        - Identificatore univoco per l'accesso del sistema.

Interpretazione dell'evento

Questo evento indica che l'account di sistema (SYSTEM) ha effettuato un accesso con successo. Alcuni punti chiave da notare:

1. Accesso di sistema: l'account SYSTEM è un account privilegiato utilizzato da Windows per eseguire processi critici. Questo tipo di accesso è normale e viene registrato quando il sistema avvia servizi o esegue operazioni interne.
2. Nessuna origine di rete: non ci sono informazioni relative a una connessione di rete, il che suggerisce che l'accesso è avvenuto localmente sul sistema.
3. Privilegi elevati: il campo "Token elevato" è impostato su Sì, il che conferma che l'account ha ottenuto privilegi amministrativi.

Il secondo log di sistema che ho analizzato è il primo **Special Logon** creato dopo l'accensione della macchina.



Il log di tipo Special Logon con ID evento 4672, indica che sono stati assegnati privilegi speciali a un nuovo accesso. Questo tipo di evento è importante perché segnala che un account ha ottenuto permessi avanzati sul sistema.

Informazioni generali

- Nome registro: *Security*
    - Indica che l'evento è stato registrato nel registro di sicurezza di Windows.
- ID evento: *4672*
    - Questo ID rappresenta l'assegnazione di privilegi speciali a un account durante un accesso.
- Livello: *Informazioni*
    - Indica che si tratta di un evento informativo, non critico o di errore.
- Parole chiave: *Controllo riuscito*
    - Significa che l'assegnazione dei privilegi è stata completata con successo.

Analisi dei campi principali

1. Soggetto
    - ID sicurezza: *SYSTEM*
        - L'account che ha ricevuto i privilegi speciali è l'account di sistema (SYSTEM).
    - Nome account: *SYSTEM*
        - L'account di sistema è un account privilegiato utilizzato da Windows per eseguire processi critici.
    - Dominio account: *NT AUTHORITY*
        - Indica che l'account appartiene al dominio locale del sistema (NT AUTHORITY).
    - ID accesso: *0x3E7*
        - Identificatore univoco per l'accesso del sistema.
2. Privilegi assegnati (questo campo elenca i privilegi speciali assegnati all'account durante l'accesso). Per non rendere l'elaborato troppo lungo riporto solamente alcuni dei privilegi.
    - SeTcbPrivilege: consente di agire come parte del Trusted Computing Base (TCB). È un privilegio molto sensibile.
    - SeSecurityPrivilege: permette di gestire la sicurezza del sistema, ad esempio modificando i criteri di sicurezza o accedendo ai log di sicurezza.
    - SeLoadDriverPrivilege: permette di caricare e scaricare driver di sistema.
    - SeBackupPrivilege: consente di eseguire operazioni di backup, bypassando alcune autorizzazioni.
    - SeRestorePrivilege: consente di ripristinare file e directory, bypassando alcune autorizzazioni.
    - SeImpersonatePrivilege: consente di impersonare altri utenti.

Interpretazione dell'evento

Questo evento indica che l'account di sistema (SYSTEM) ha ottenuto una serie di privilegi avanzati durante un accesso. Alcuni punti chiave da notare:

1. Accesso di sistema: l'account SYSTEM è un account privilegiato utilizzato da Windows per eseguire processi critici. Questo tipo di evento è normale e viene registrato quando il sistema avvia servizi o esegue operazioni interne.
2. Privilegi elevati: i privilegi elencati sono tipici per l'account SYSTEM, che richiede autorizzazioni estese per gestire il sistema operativo.
3. Nessuna origine esterna: non ci sono informazioni relative a una connessione di rete, il che suggerisce che l'accesso è avvenuto localmente sul sistema.