Report Esercizio 06/02/2025

Analisi Visualizzatore Eventi Windows Leonardo Catalano

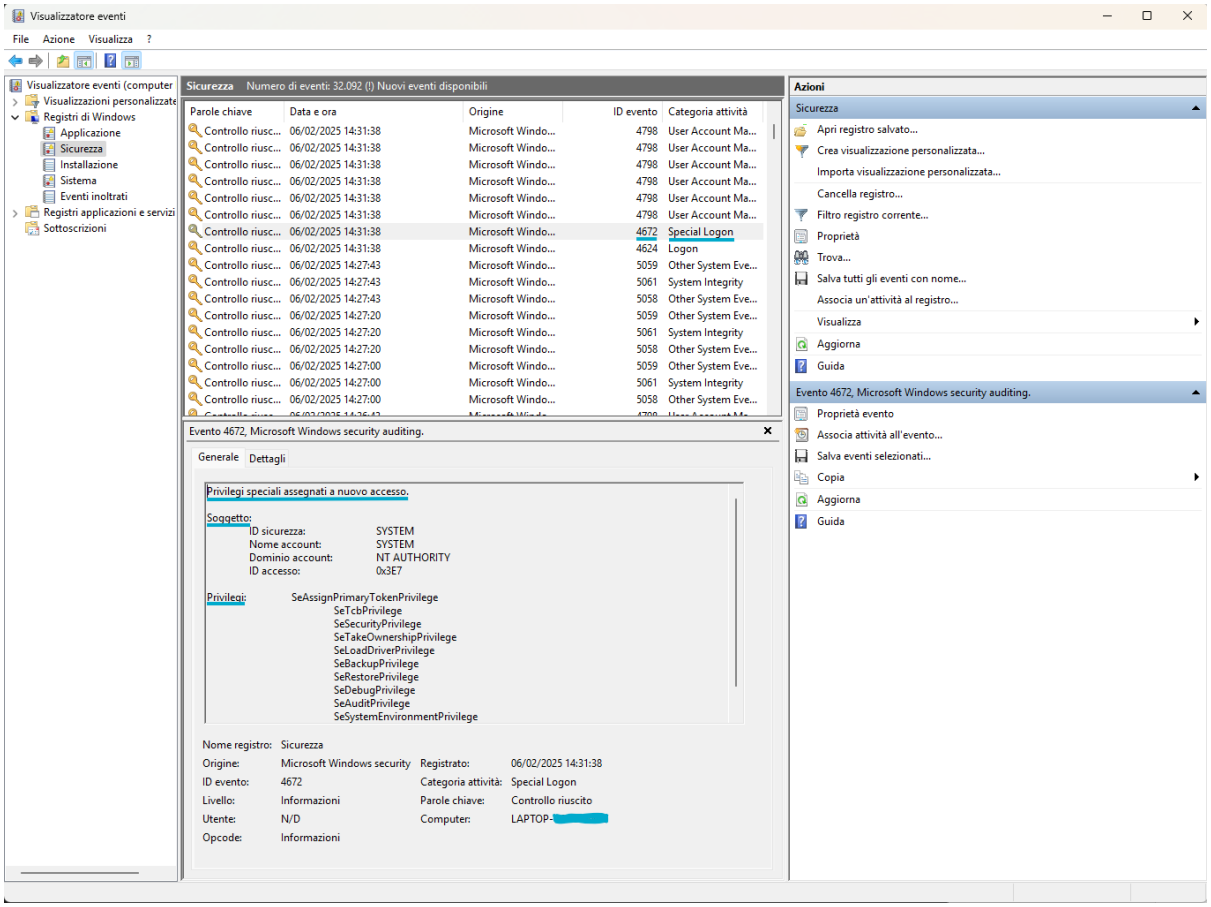
“La traccia di oggi ci chiede di effettuare un’analisi con il Visualizzatore eventi di Windows .”

-Istruzioni:

Nello specifico nel Visualizzatore Eventi dovremmo andare nella sezione “Registri di Windows” e categoria “Sicurezza”.
Gli eventi da analizzare saranno quelli con “Categoria attività” Special Logon e Logon.

-Visualizzatore eventi:

Evento Special Logon:



Come da screen è riportato il 1* Special Logon in ordine cronologico con ID evento n. 4672, questo ID sta a significare un particolare evento:
“Evento 4672: Accesso speciale per un utente con privilegi elevati (d’amministratore)”.

Sono riportate altre informazioni :

Origine dell'evento: Microsoft Windows security
Il Livello : Informazioni

Il Soggetto:

ID SICUREZZA: SYSTEM
Nome account: SYSTEM
Dominio account NT AUTHORITY
ID accesso: 0x3E7

L'id di Sicurezza SYSTEM, e l'account SYSTEM sono legati e associati al sistema operativo Windows e rappresentano l'utente di sistema. L'evento ci indica che l'accesso è del sistema non dell'utente umano, e che questo processo di sistema ha ottenuto privilegi elevati.

Privilegi assegnati all'utente:

1) SeAssignPrimaryTokenPrivilege: Permesso di assegnare un token di accesso primario ad un altro processo.

2)SeTcbPrivilege: Privilegio che consente di agire come sistema di controllo di sicurezza (Trust Computer Base).

3)SeTakeOwnershipPrivilege: Permesso di prendere possesso di un file o di una risorsa.

4)SeLoadDriverPrivilege: Permesso di caricare un driver di dispositivo.

5)SeBackupPrivilege: Permesso di eseguire il backup di file e cartelle, ignorando le restrizioni di sicurezza.

6)SeRestorePrivilege: Permesso di ripristinare file e cartelle.

7)SeDebugPrivilege: Privilegio di debug dei processi.

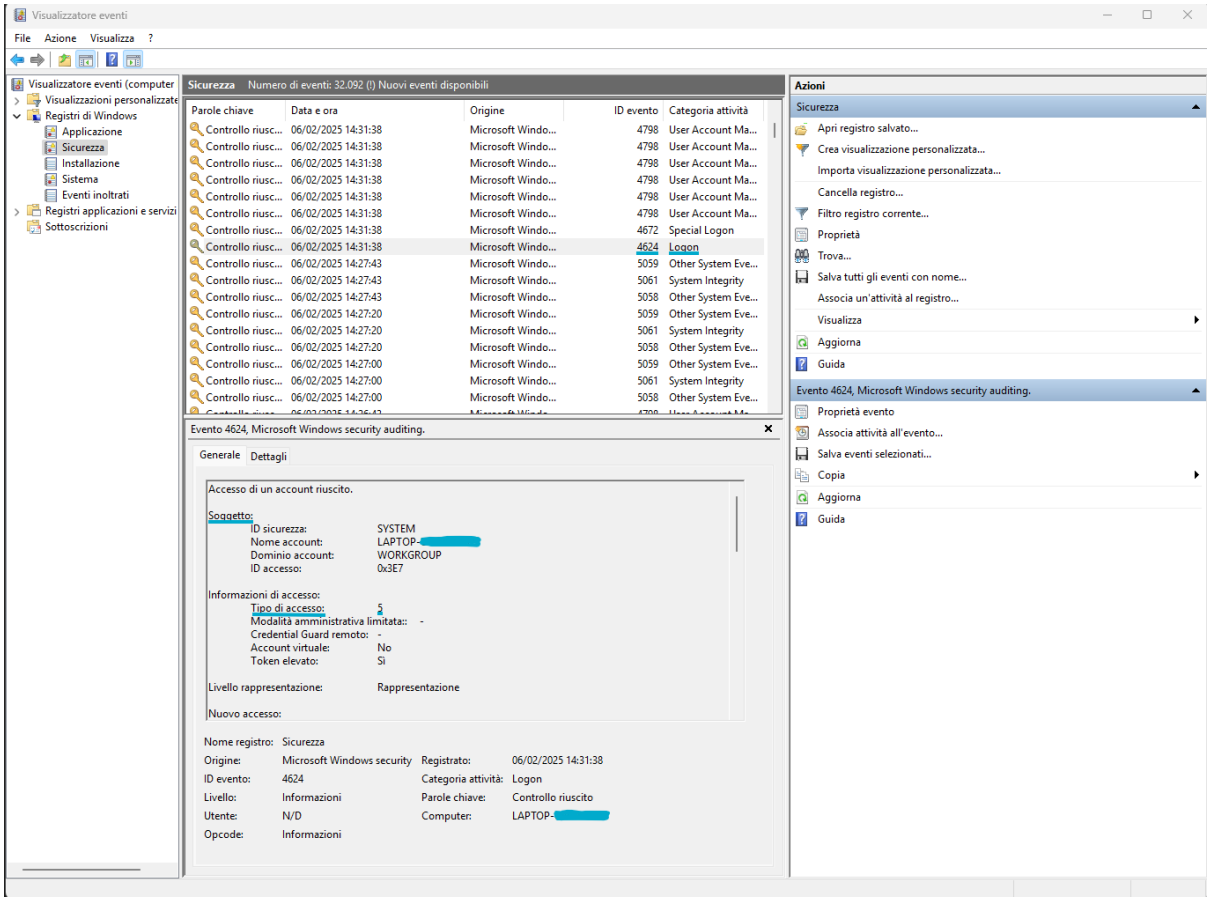
8)seAuditPrivilege: Privilegio di modificare le impostazioni di auditing del sistema.

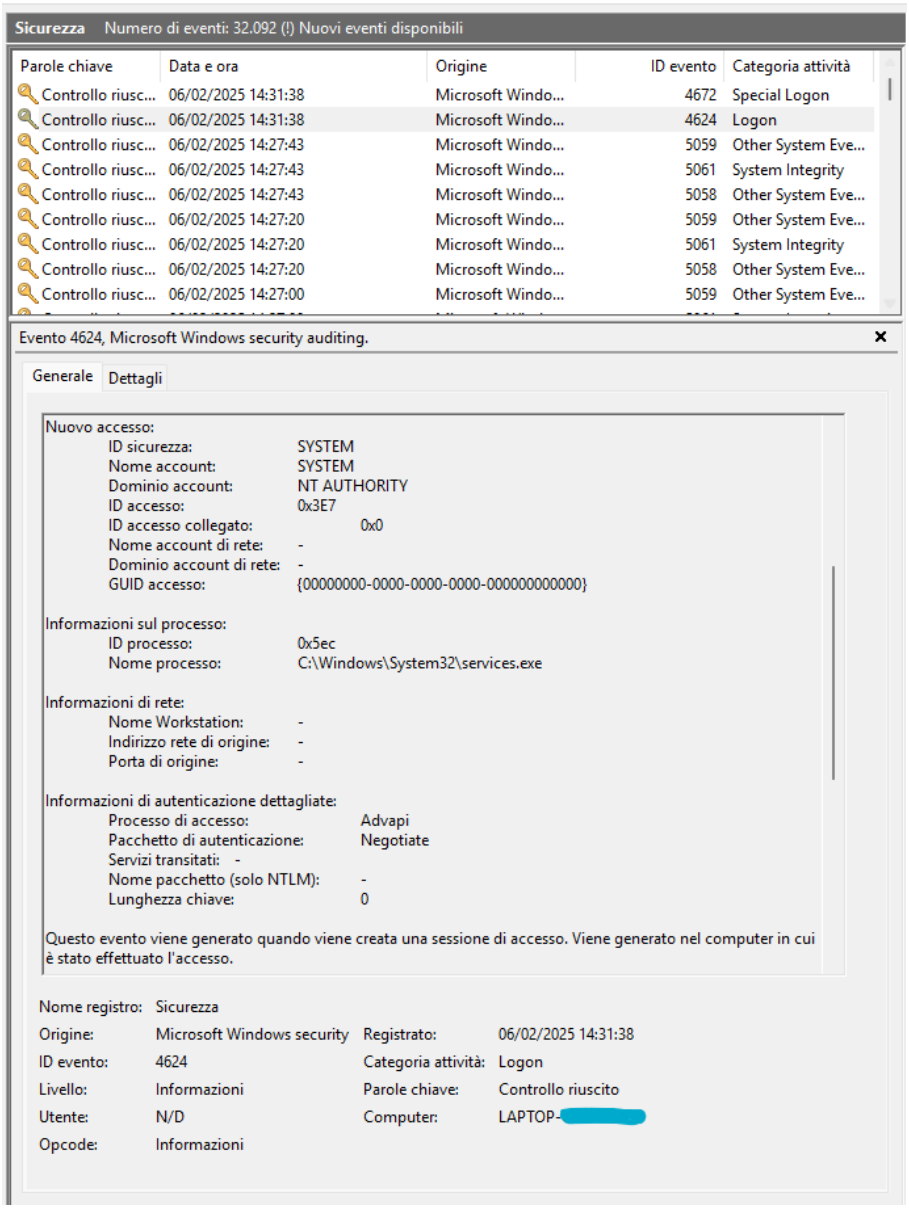
9)seSystemEnvironmentPrivilege: Permesso di modificare variabili di ambiente di sistema.

10)seImpersonatePrivilege: Permesso di impersonare un altro utente.

11)seDelegateSessionUserImpersonatePrivilege: Permesso di impersonare un altro utente in sessioni di delega.

Evento Logon:





Come da screen ho riportato il 1* evento Logon in ordine cronologico con ID evento n. 4624, questo ID sta a significare un particolare evento:
“Evento 4624: Logon riuscito (l’utente ha effettuato l’accesso con successo al sistema)
Evento 4625: Tentativo di Logon fallito (c’è stato un tentativo di accesso ed è fallito) ”.

Sono riportate altre informazioni:

Origine dell’evento: Microsoft Windows security
Il Livello : Informazioni

Il Soggetto:

ID SICUREZZA: SYSTEM
Nome account: LAPTOP-
Dominio account WORKGROUP
ID accesso: 0x3E7

L’evento 4624 ci segnala che c’è stato un accesso riuscito con delle determinate caratteristiche:

1)Tipo di accesso: 5 (Servizio), questo tipo di accesso si verifica quando un servizio di sistema di Windows viene avviato.

2)Account Virtuale: No (L’accesso non riguarda un account virtuale)

3)Token elevato: Si (Indica che l’accesso è avvenuto con privilegi elevati, tipicamente d’amministratore)

Sezione Nuovo Accesso:

In questa sezione troviamo lo stesso SYSTEM di prima, ossia un account di sistema windows che viene usato per le operazioni internet al sistema operativo, quindi non un account utente, ma di un account interno dell’OS.

Informazioni sul processo:
ID processo: 0x5ec
Nome processo: C:\Windows\System32\services.exe
Questo processo è critico perchè gestisce i servizi del sistema operativo Windows, vuol dire quindi che un servizio di sistema ha richiesto l’accesso a questo particolare servizio “services.exe”.

-Tipi di accesso (LOGON Type):
Una cosa molto importante per gli eventi Logon sono i vari Tipi di accesso che possono esserci:

Tipo di Accesso	Descrizione
2	**Interattivo:** Accesso effettuato direttamente tramite dall’utente fisico sulla macchina con tastiera e mouse.
3	**Rete:** Accesso tramite connessione ad una cartella condivisa o altre risorse di rete da un altro computer sulla stessa rete.
4	**Batch:** Accesso tramite attività pianificata (eseguito da un processo pianificato, come un lavoro di cronologia).
5	**Servizio:** Accesso avviato da un servizio di sistema, ad esempio quando un servizio viene avviato automaticamente.
7	**Unlock:** Accesso effettuato quando una workstation con sreen saver, protetta da password viene sbloccata.

8	**NetworkClearText:** Accesso in cui le credenziali sono inviate in chiaro (ad esempio, login su IIS con “autenticazione di base”).
9	**Nuove Credenziali:** Accesso con credenziali alternative, come nel caso di RunAs o mappatura di un’unita di rete con credenziali diverse. Questo tipo di accesso non appare frequentemente negli eventi, ma è utile per tracciare gli accessi con credenziali diverse.
10	**RemoteInteractive:** Accesso remoto al sistema (tramite Terminal Services, Desktop remoto o Assistenza Remota).
11	**CachedInteractive:** Accesso effettuato con credenziali di dominio memorizzate nella cache, ad esempio quando un utente si connette a un laptop in modalità offline (senza connessione alla rete).