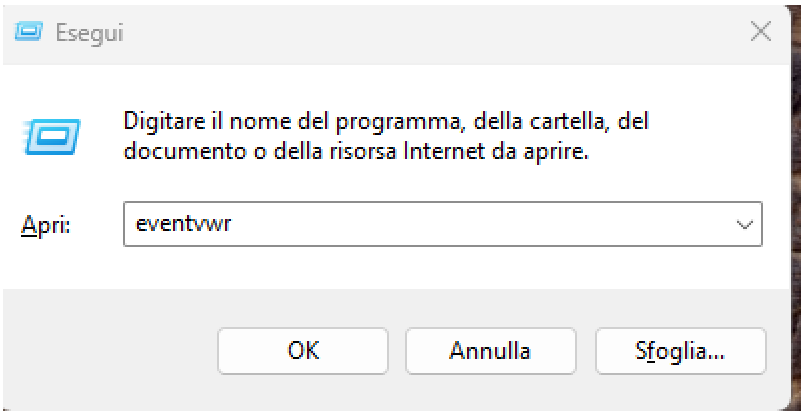
S9/L4

L’esercizio di oggi consiste nel gestire i log di sicurezza di windows.

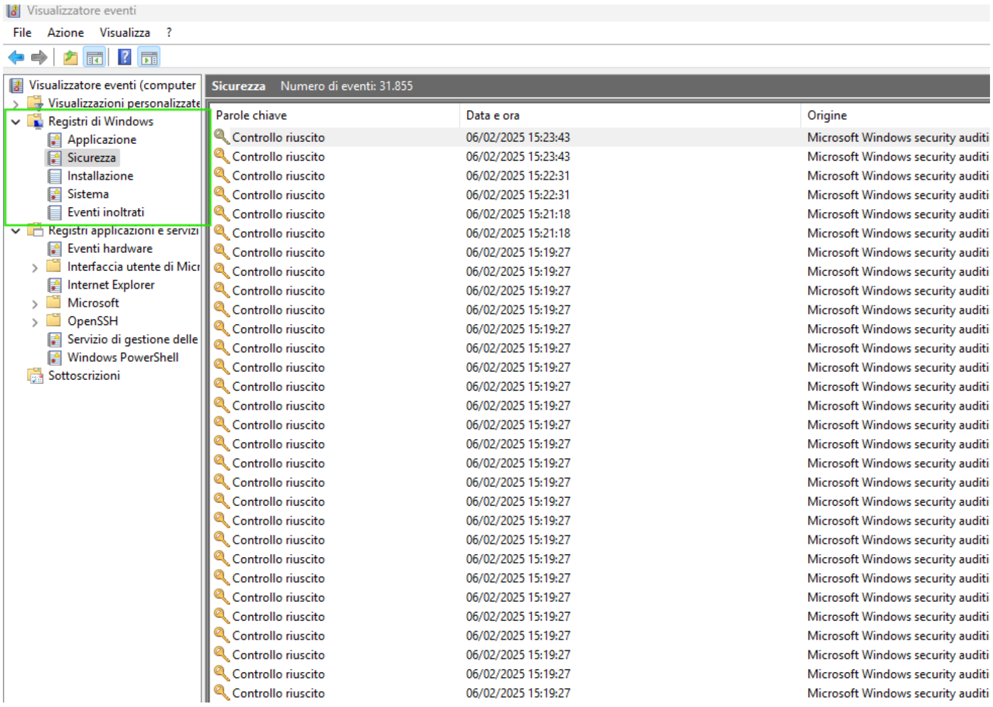
Come prima cosa dobbiamo schiacciare il tasto Windows e poi R, Visualizzeremo un piccolo riquadro chiamato esegui dove all’interno scriviamo **eventvwr**.



Digitare il nome del programma, della cartella, del documento o della risorsa Internet da aprire.

Apri: eventvwr

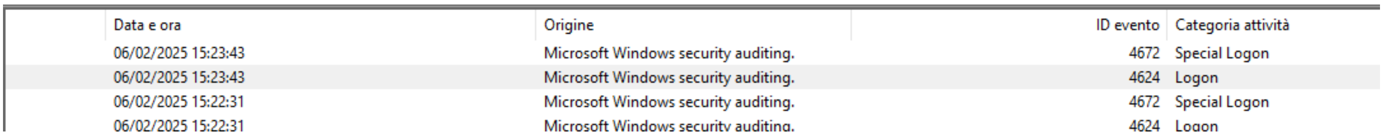
Una volta dentro il visualizzatore eventi dovremo andare nel riquadro di sinistra su registri di windows e poi sicurezza.



Sicurezza Numero di eventi: 31.855

Parole chiave	Data e ora	Origine
Controllo riuscito	06/02/2025 15:23:43	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:23:43	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:22:31	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:22:31	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:21:18	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:21:18	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:19:27	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:19:27	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:19:27	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:19:27	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:19:27	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:19:27	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:19:27	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:19:27	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:19:27	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:19:27	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:19:27	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:19:27	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:19:27	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:19:27	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:19:27	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:19:27	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:19:27	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:19:27	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:19:27	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:19:27	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:19:27	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:19:27	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:19:27	Microsoft Windows security auditi
Controllo riuscito	06/02/2025 15:19:27	Microsoft Windows security auditi

Ora dobbiamo analizzare gli eventi che hanno categoria **logon** e **Special logon**



Data e ora	Origine	ID evento	Categoria attività
06/02/2025 15:23:43	Microsoft Windows security auditing.	4672	Special Logon
06/02/2025 15:23:43	Microsoft Windows security auditing.	4624	Logon
06/02/2025 15:22:31	Microsoft Windows security auditing.	4672	Special Logon
06/02/2025 15:22:31	Microsoft Windows security auditing.	4624	Logon

Come possiamo notare i primi eventi che ci escono sono di nostro interesse.

Vediamo che viene registrata la data, l'origine, l'ID evento e la categoria attività

Essendo questi registri di windows precisamente di sicurezza vengono tutti fatti dal programma di sicurezza di windows.

Se andiamo a schiacciare su uno ci vengono fornite ulteriori informazioni.

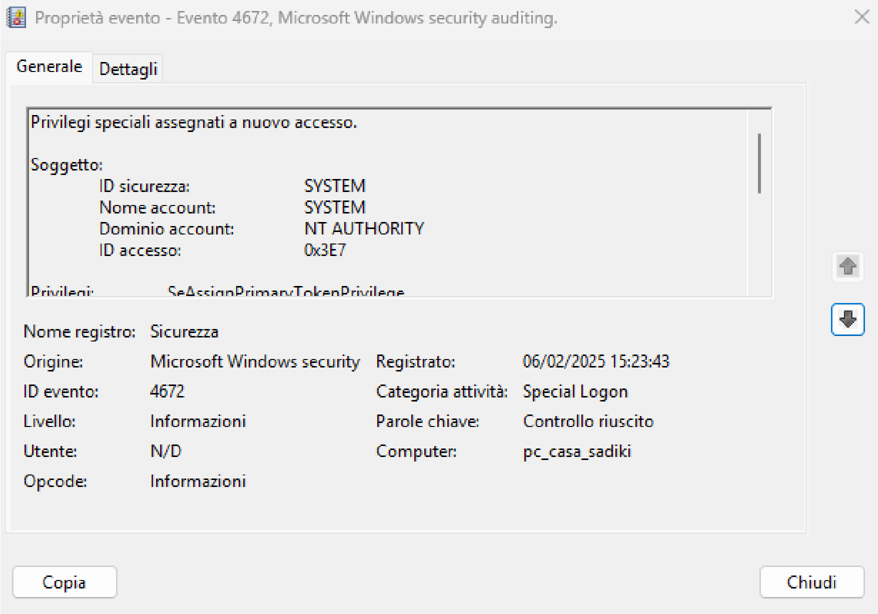
Logon

```
Accesso di un account riuscito.

Soggetto:
          ID sicurezza:            SYSTEM
          Nome account:            PC_CASA_SADIKI$
          Dominio account:         WORKGROUP
          ID accesso:              0x3E7

Informazioni di accesso:
```

Nome registro: Sicurezza
Origine: Microsoft Windows security
Registrato: 06/02/2025 15:23:43
ID evento: 4624
Categoria attività: Logon
Livello: Informazioni
Parole chiave: Controllo riuscito
Utente: N/D
Computer: pc_casa_sadiki
Opcode: Informazioni

Ci vengono fornite tutte le informazioni, in questo caso viene registrato l'accesso all'host (PC_CASA_SADIKI).

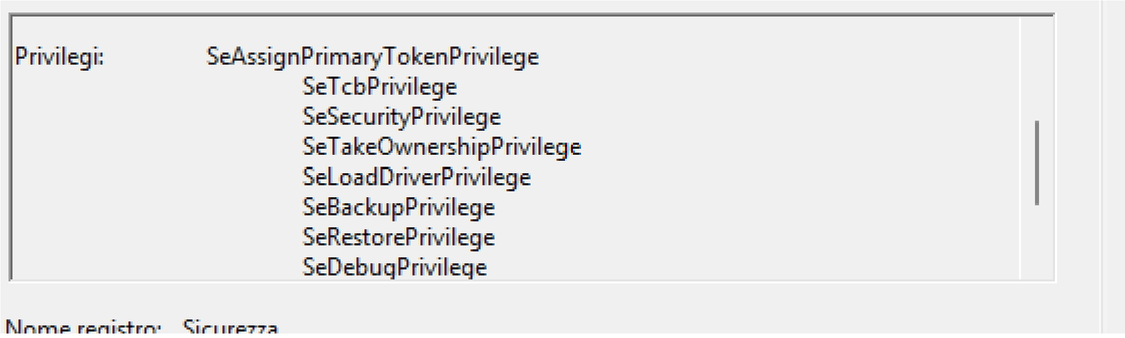
Special Logon



```
Privilegi speciali assegnati a nuovo accesso.

Soggetto:
          ID sicurezza:            SYSTEM
          Nome account:            SYSTEM
          Dominio account:         NT AUTHORITY
          ID accesso:              0x3E7

Privilegi:          SeAssignPrimaryTokenPrivilege
```

Nome registro: Sicurezza
Origine: Microsoft Windows security
Registrato: 06/02/2025 15:23:43
ID evento: 4672
Categoria attività: Special Logon
Livello: Informazioni
Parole chiave: Controllo riuscito
Utente: N/D
Computer: pc_casa_sadiki
Opcode: Informazioni

Come possiamo notare invece non è solo un semplice accesso ma un accesso con privilegi (root), vediamo anche che questi privilegi vengono assegnati all’account di sistema di windows.



```
Privilegi:          SeAssignPrimaryTokenPrivilege
                              SeTcbPrivilege
                              SeSecurityPrivilege
                              SeTakeOwnershipPrivilege
                              SeLoadDriverPrivilege
                              SeBackupPrivilege
                              SeRestorePrivilege
                              SeDebugPrivilege

Nome registro:    Sicurezza
```

Se scendiamo un po' giù possiamo vedere anche tutti i privilegi concessi.

Questi registri sono molto utili da controllare per capire se siamo stati compromessi dato che troveremmo degli accessi non eseguiti da noi, in orari strani o con dettagli anomali.