REPORT S9/L4

File di Log di Windows

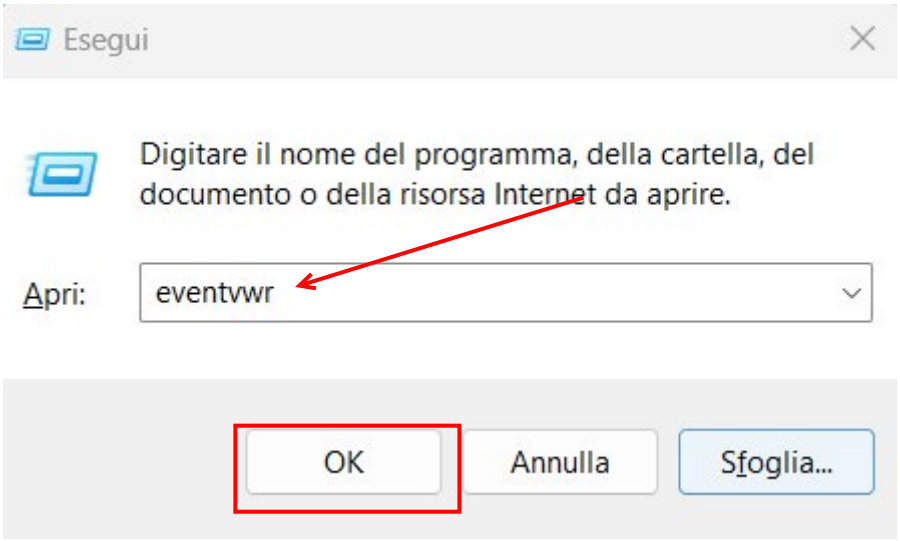
Traccia

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

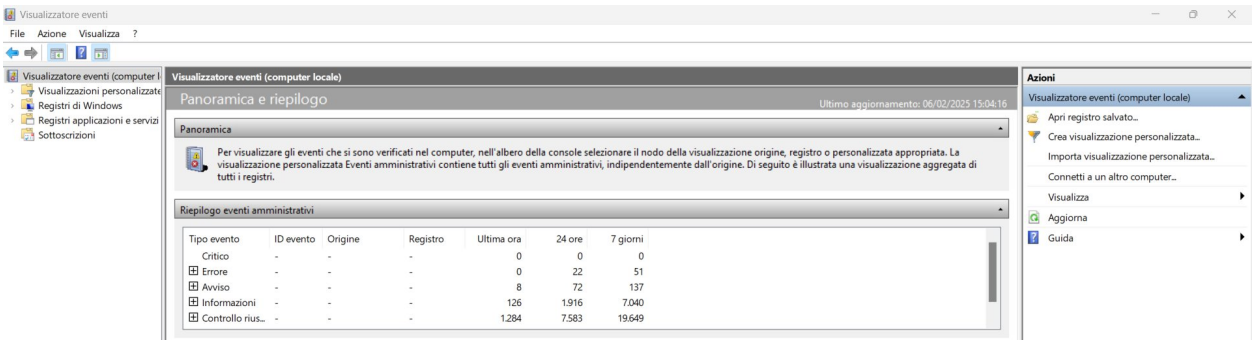
1. Accedere al Visualizzatore Eventi:
   - Apri il Visualizzatore eventi premendo Win + R per aprire la finestra "Esegui".
   - Digita eventvwr e premi Invio.
2. Configurare le Proprietà del Registro di Sicurezza:
   - Nel pannello di sinistra, espandi "Registri di Windows" e seleziona "Sicurezza".
3. Analizzare gli eventi con Categoria Attività Logon e Special Logon

Svolgimento

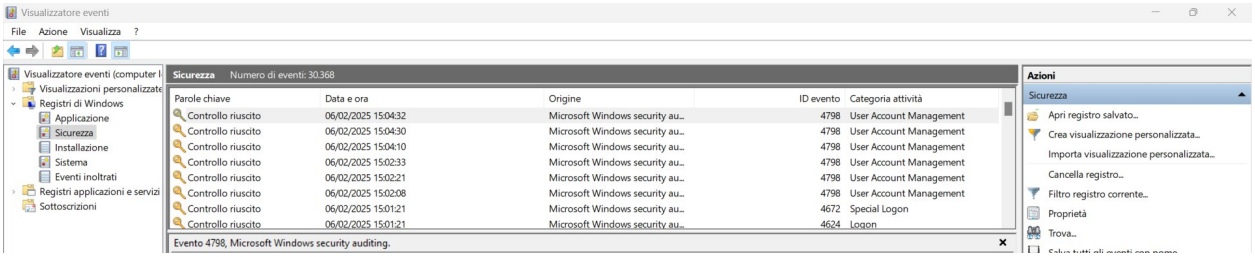
Per svolgere l'esercizio di oggi seguiamo i passaggi scritti nella consegna:



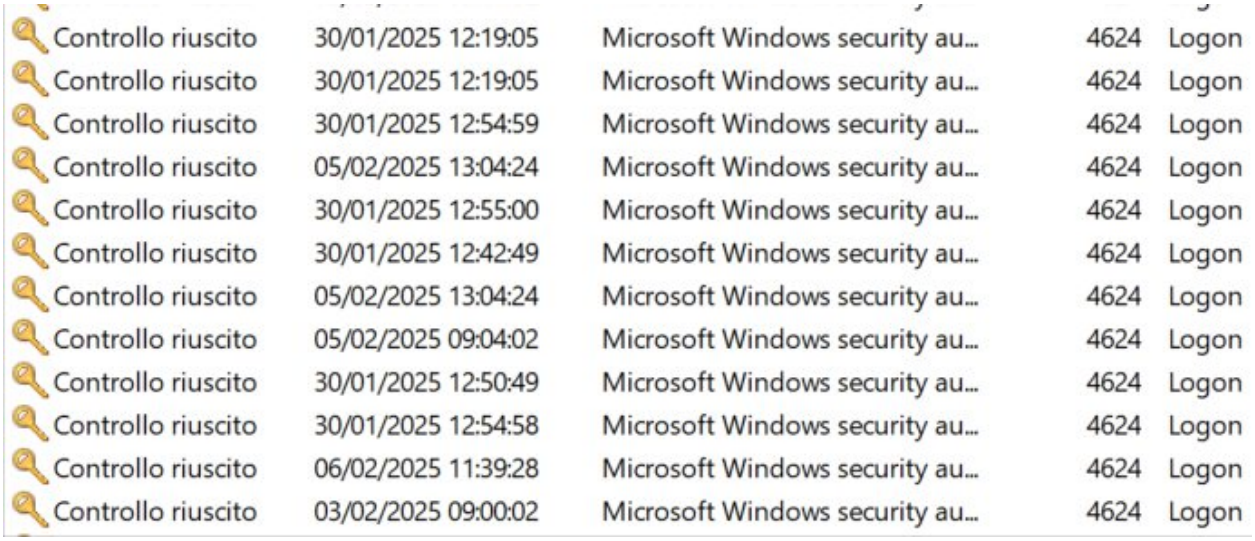
Premendo **Win + R** e digitando **eventvwr** (Event Viewer) otteniamo:

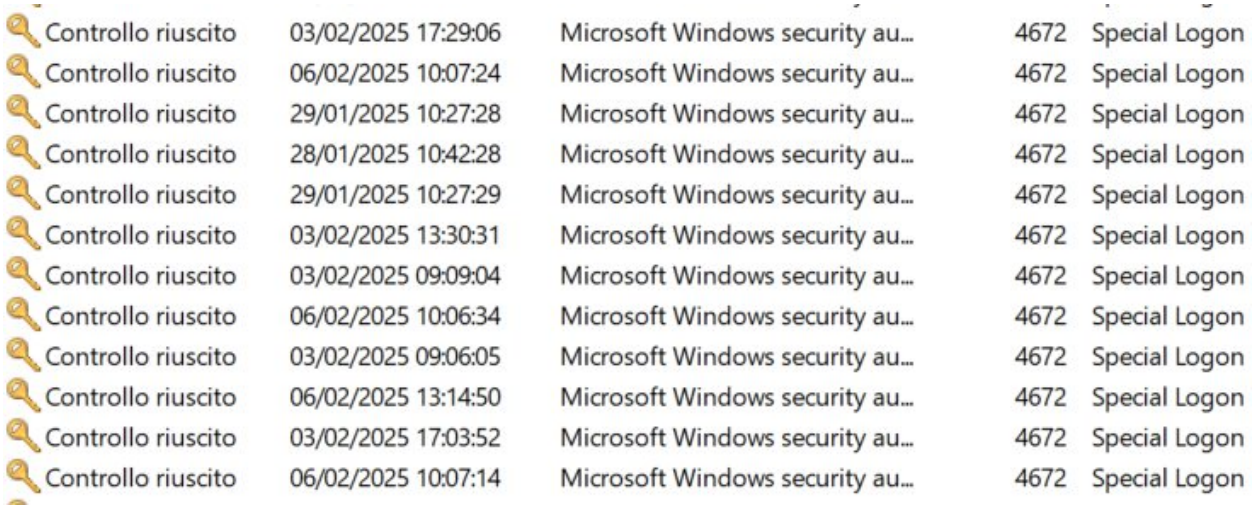


Poi spostandoci su **Registri di Windows, Sicurezza**:



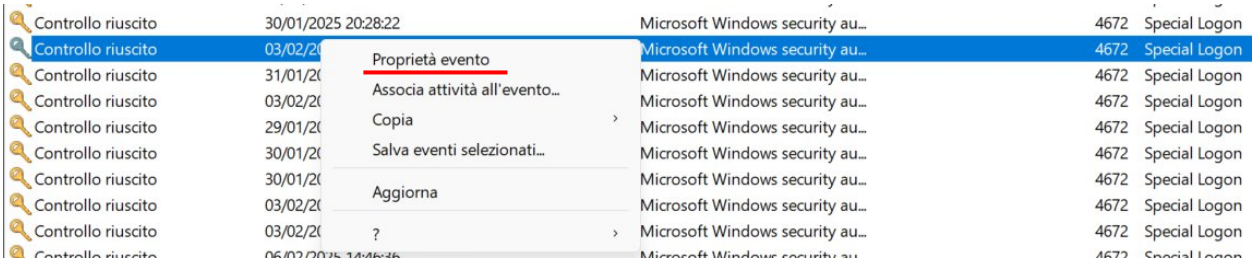
A questo punto possiamo analizzare gli eventi della categoria **Logon** e **Special Logon**:



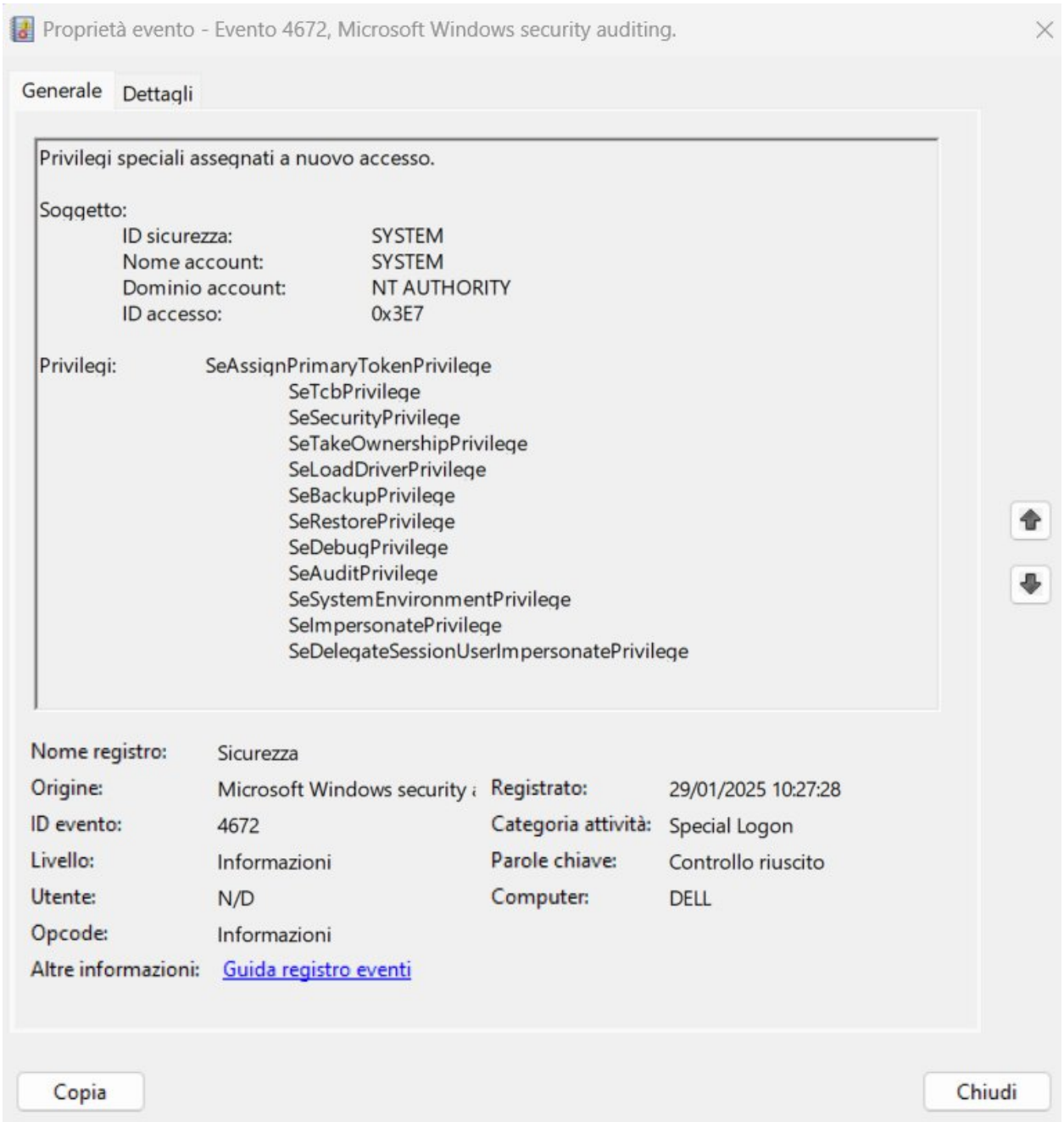


Ricordiamo che la differenza tra "logon" e "special logon" si riferisce al tipo di sessione di accesso in un sistema operativo di Windows. Un logon standard è l'accesso normale a un sistema, mentre un "special logon" è un tipo di logon che ha privilegi di amministratore equivalente e può essere utilizzato per elevare un processo a un livello superiore. **Un logon speciale può essere utile per monitorare eventuali attività sospette, come tentativi di accesso con privilegi elevati o movimenti laterali di un attaccante all'interno di un sistema**.

Per analizzare più precisamente gli eventi basterà cliccare su un evento, premere il tasto destro e cliccare su “proprietà evento” per avere maggiori dettagli:

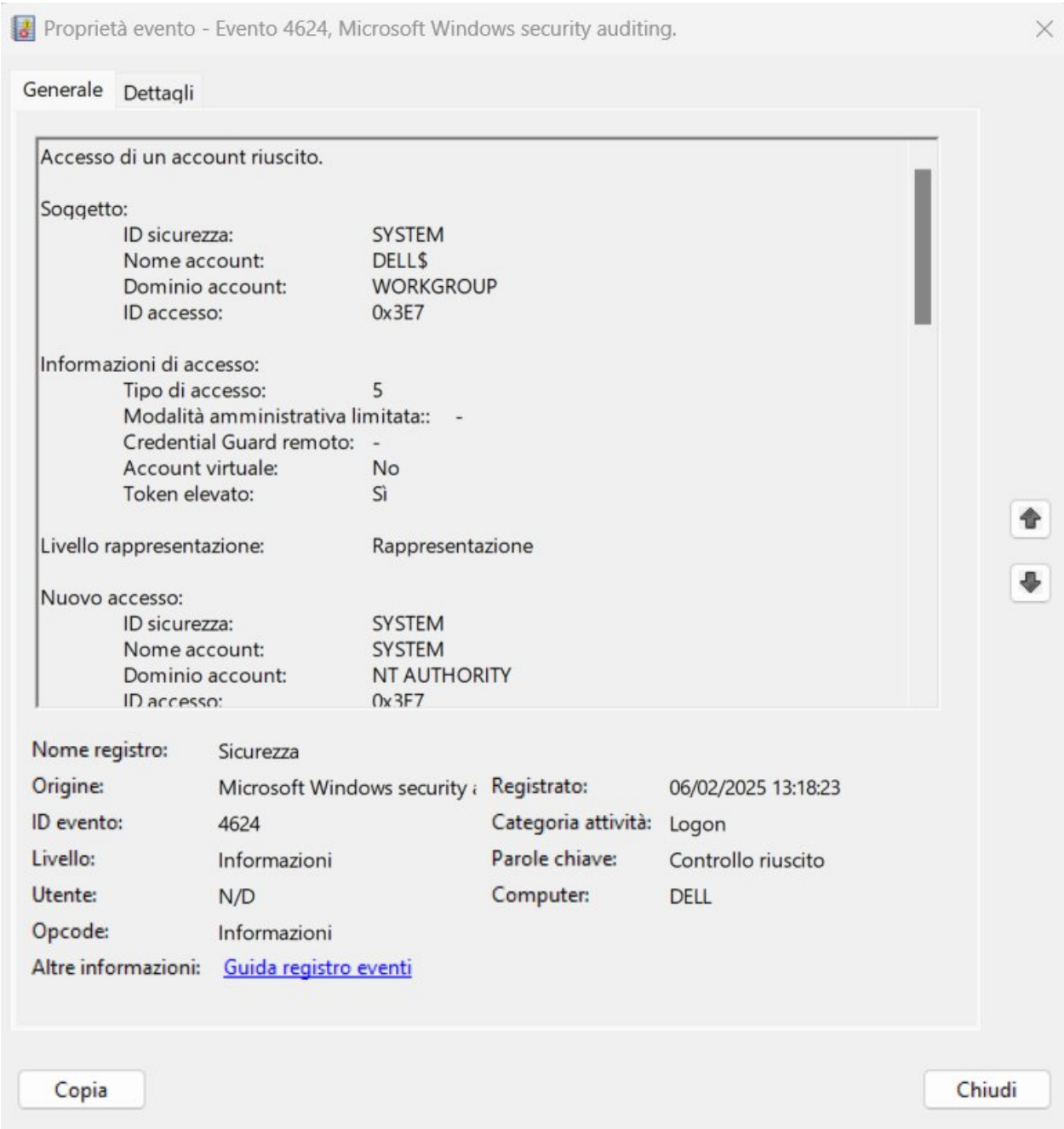


La schermata che ci appare sarà di questo tipo:



L’ID dell’evento ci dice quale evento si è verificato e dalla finestra dei dettagli capiamo cosa analizzare e perchè. Ad esempio:

Eventi di Accesso (ID 4624)



Questo evento viene generato quando viene creata una sessione di accesso.

Il campo **Soggetto** indica l'account nel sistema locale che ha richiesto l'accesso. Generalmente si tratta di un servizio, quale il servizio Server, o di un processo locale, ad esempio Winlogon.exe o Services.exe.

Il campo **Tipo di accesso** indica il tipo di accesso che è stato effettuato. I tipi più comuni sono 2 (interattivo) e 3 (rete).

Il campo **Nuovo accesso** indica l'account per il quale è stato creato il nuovo accesso, vale a dire l'account che ha effettuato l'accesso.

I campi **Informazioni di rete** indicano l'origine della richiesta di accesso remota. Il nome della workstation non è sempre disponibile e può essere vuoto in alcuni casi.

Il campo **Livello rappresentazione** indica la portata della rappresentazione consentita a un processo nella sessione di accesso.

Il campo **Informazioni di autenticazione** fornisce informazioni dettagliate sulla specifica richiesta di accesso.

- GUID è un identificatore univoco che può essere utilizzato per correlare questo evento a un evento KDC (key distribution center è parte di un crittosistema il cui scopo è ridurre i rischi dovuti allo scambio delle chiavi).
- Servizi transitati indica quali servizi intermedi hanno partecipato alla richiesta di accesso.
- Nome pacchetto indica quale sotto-protocollo dei protocolli NTLM (NT LAN Manager è una suite di protocolli di autenticazione sviluppati da Microsoft che fornisce autenticazione, integrità e confidenzialità agli utenti nelle reti Windows) è stato utilizzato.
- Lunghezza chiave indica la lunghezza della chiave di sessione generata. Se non è stata richiesta alcuna chiave di sessione, la lunghezza sarà 0.

Vediamo ora un breve elenco degli ID più comuni.

EventID 528: Un utente si è connesso al computer. Questo evento può essere di tipo interattivo, rete, batch, servizio, sblocco, testo non crittografato in rete, nuove credenziali, remote interactive o cached interactive.

EventID 529: Errore di accesso. È stato effettuato un tentativo di accesso con un nome utente sconosciuto o con un nome utente noto ma password errata.

EventID 530: Errore di accesso. È stato effettuato un tentativo di accesso con un account utente oltre il tempo consentito.

EventID 531: Errore di accesso. È stato effettuato un tentativo di accesso con un account disattivato.

EventID 532: Errore di accesso. È stato effettuato un tentativo di accesso con un account scaduto.

EventID 534: Errore di accesso. L'utente ha tentato di connettersi con un tipo di accesso non consentito.

EventID 4624: Logon riuscito. L'utente si autentica con successo sul sistema. Contiene informazioni sul tipo di logon (interattivo, remoto, ecc.), sull'utente e sul dominio.

EventID 4625: An account failed to log on, fa parte della categoria "Logon/Logoff" e può essere utile per individuare e monitorare tutti i tentativi di logon falliti.

EventID 4672: Special privileges assigned to new logon, fa parte della categoria "Logon/Logoff" e viene registrato a seguito di un evento 4624 (An account was successfully logged on).

EventID 4740: Account bloccato. Registrato quando un account utente viene bloccato, solitamente a causa di troppi tentativi di accesso falliti.