**AMATO SARA**

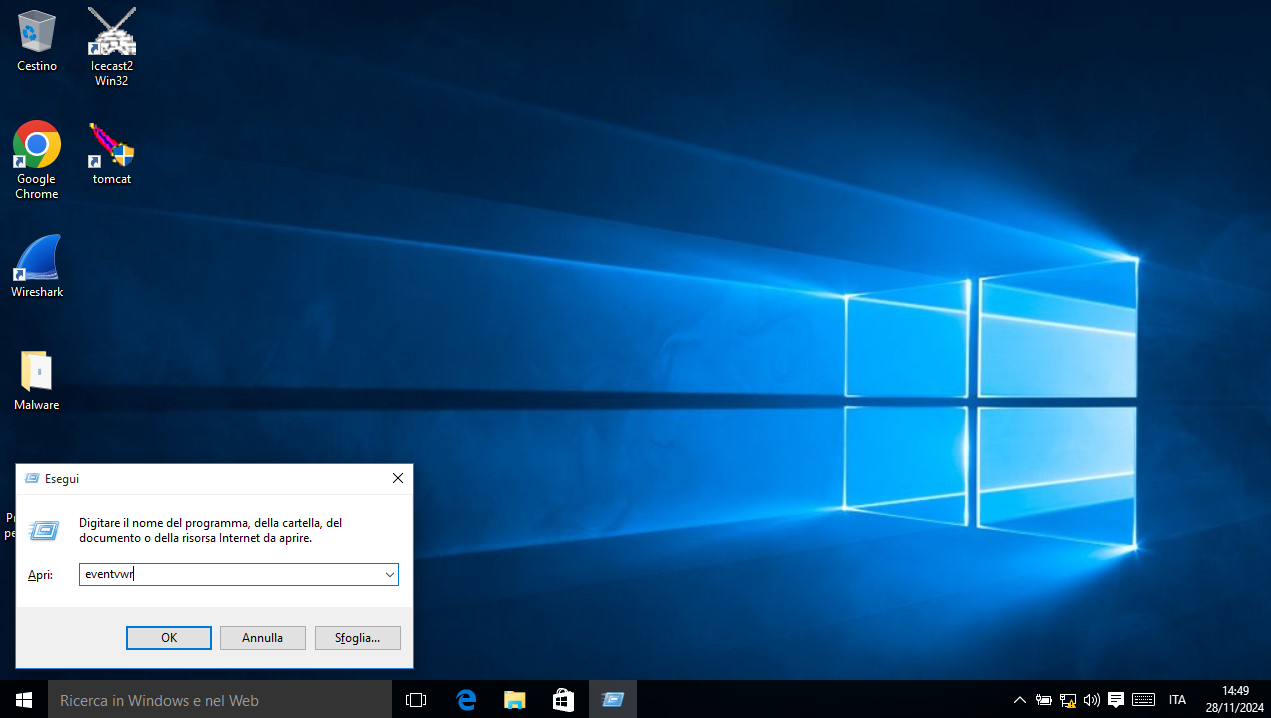
**S9 L4**

**Configurazione e Gestione dei File di Log della Sicurezza in Windows**

L'obiettivo di questa attività è apprendere e applicare i passaggi necessari per configurare e gestire i file di log relativi alla sicurezza utilizzando il Visualizzatore Eventi di Windows. Questa operazione è essenziale per monitorare eventi critici legati alla sicurezza del sistema, identificare potenziali minacce e garantire la tracciabilità delle attività eseguite.

Apertura del Visualizzatore Eventi

Il primo passo consiste nell’accedere al Visualizzatore Eventi, uno strumento integrato in Windows che permette di visualizzare e gestire i log del sistema operativo. Questo è stato realizzato seguendo questi passaggi:



È stata premuta la combinazione di tasti Win + R per aprire la finestra di dialogo Esegui, uno strumento utile per avviare rapidamente applicazioni o comandi di sistema.

All'interno della finestra, è stato digitato il comando eventvwr, che è l'abbreviazione del Visualizzatore Eventi.

Premendo Invio, si è aperto il Visualizzatore Eventi, che si presenta con un'interfaccia strutturata in tre pannelli principali:

Pannello di navigazione a sinistra: consente di accedere alle diverse categorie di log, tra cui Registri di Windows.

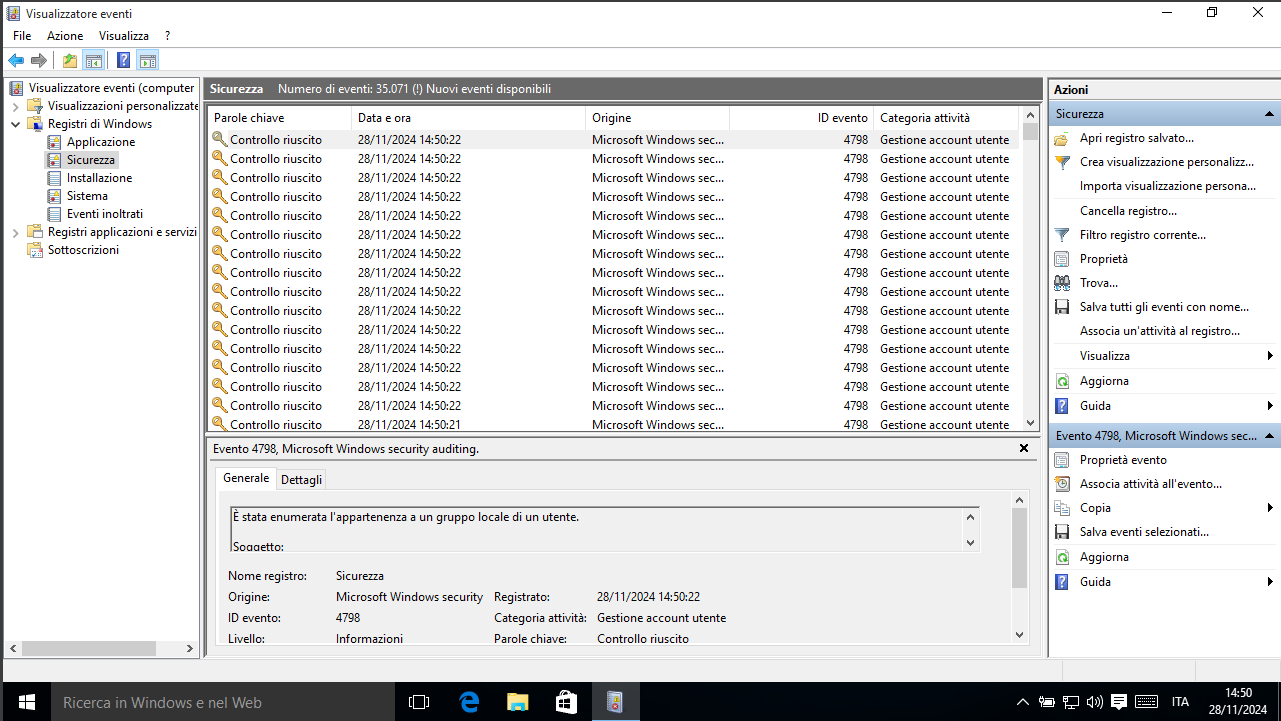
Pannello centrale: mostra gli eventi registrati nella categoria selezionata, elencandoli con informazioni di base (ID evento, data e ora, gravità, ecc.).

Pannello inferiore: fornisce dettagli approfonditi sull'evento selezionato.

Questo strumento è fondamentale per monitorare lo stato del sistema e rilevare attività sospette o problematiche.

Navigazione nel Registro di Sicurezza

Il Registro di Sicurezza è uno dei principali registri presenti nella sezione Registri di Windows. Contiene informazioni relative agli eventi di sicurezza del sistema, come tentativi di accesso, modifiche ai permessi, e attività di audit configurate.



Per accedere a questo registro, dal pannello di navigazione a sinistra, è stata espansa la voce "Registri di Windows".

Successivamente, è stata selezionata la categoria "Sicurezza". Questa sezione è dedicata esclusivamente agli eventi legati alla sicurezza e presenta un elenco dettagliato di attività rilevanti.

Analizzando gli eventi registrati, è stato possibile osservare informazioni utili, come:

ID evento: un identificatore univoco che consente di classificare e cercare rapidamente eventi specifici (ad esempio, l'ID 4624 rappresenta un accesso riuscito, mentre l'ID 4625 indica un tentativo di accesso fallito).

Data e ora: fondamentale per verificare il momento in cui si sono verificati eventi specifici.

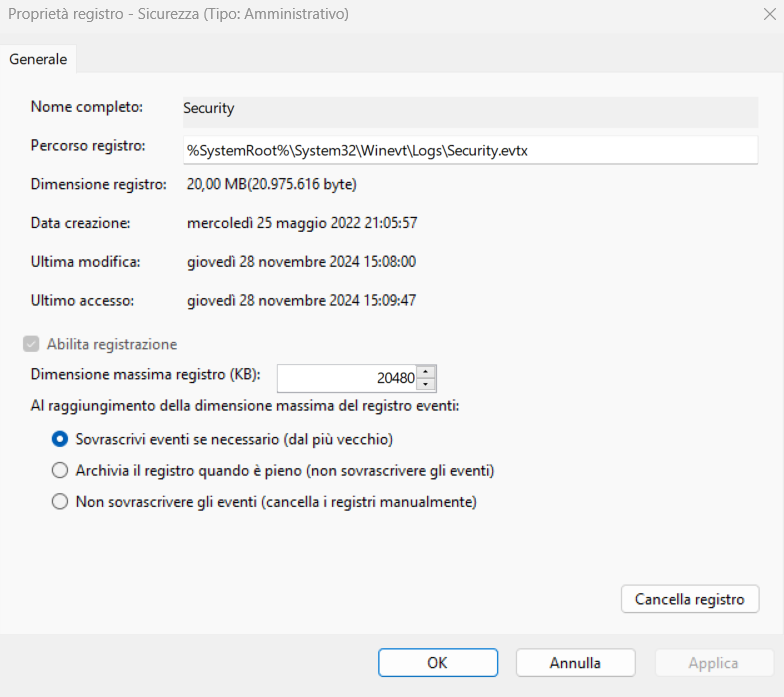
Utente e dominio: indicano chi ha eseguito l'azione registrata.

Descrizione dell’evento: un riepilogo che spiega cosa è accaduto, come un accesso, una modifica ai permessi, o un errore.

Questa fase è stata utile per comprendere come vengono registrati e organizzati i dati relativi alla sicurezza, evidenziando l'importanza di mantenere questi registri aggiornati e facilmente consultabili.

Configurazione delle Proprietà del Registro di Sicurezza

Dopo aver esplorato il registro di sicurezza, è stato necessario configurare le sue proprietà per garantire un'archiviazione efficiente e adeguata alle esigenze del sistema.



Accesso alle proprietà:

Si è fatto clic con il tasto destro sulla voce "Sicurezza" nella sezione Registri di Windows.

Dal menu contestuale, è stata selezionata l’opzione "Proprietà", che consente di personalizzare il comportamento del registro.

Parametri configurati:

Conclusione

I passaggi svolti hanno permesso di:

Familiarizzare con il Visualizzatore Eventi, uno strumento cruciale per il monitoraggio della sicurezza in Windows.

Comprendere l’organizzazione e la funzione del Registro di Sicurezza, evidenziando il ruolo degli eventi registrati per tracciare attività significative e identificare potenziali problemi.

Configurare le proprietà del registro, ottimizzando la gestione dello spazio disco e definendo politiche che bilanciano la necessità di archiviazione e la praticità operativa.

Questa configurazione rappresenta un passo iniziale fondamentale per una gestione avanzata della sicurezza, preparando il sistema per ulteriori miglioramenti come la configurazione di politiche di audit mirate.