FILE DI LOG DI WINDOWS

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

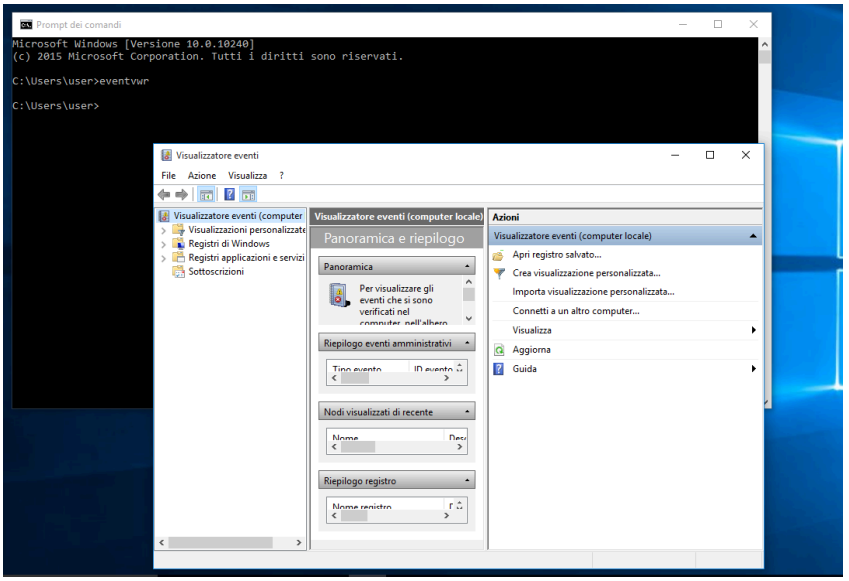
1. Accedere al Visualizzatore Eventi:
    - ○ Apri il Visualizzatore eventi premendo Win + R per aprire la finestra "Esegui".
    - ○ Digita eventvwr e premi Invio.
2. Configurare le Proprietà del Registro di Sicurezza:
    - ○ Nel pannello di sinistra, espandi "Registri di Windows" e seleziona "Sicurezza".

Svolgimento:
In un SOC (Security Operations Center), i file di log svolgono un ruolo cruciale nella protezione della rete, sistemi e applicazioni di una organizzazione. Si tratta di registrazioni dettagliate delle attività e degli eventi che avvengono all'interno di una infrastruttura IT.
Una delle funzioni principali dei file di log in un SOC è quella di monitorare in tempo reale le attività all'interno dell'infrastruttura IT. I dati contenuti nei file di log sono: tentativi di accesso, modifiche ai file di sistema, movimenti di rete (connessioni in ingresso ed uscita), errori di sistema o delle applicazioni.
I file di log possono individuare dati come accessi non autorizzati, anomalie di traffico o modifiche inaspettate. Aiutano nella rilevazione precoce di potenziali minacce e nell'evitamento di incidenti informatici.

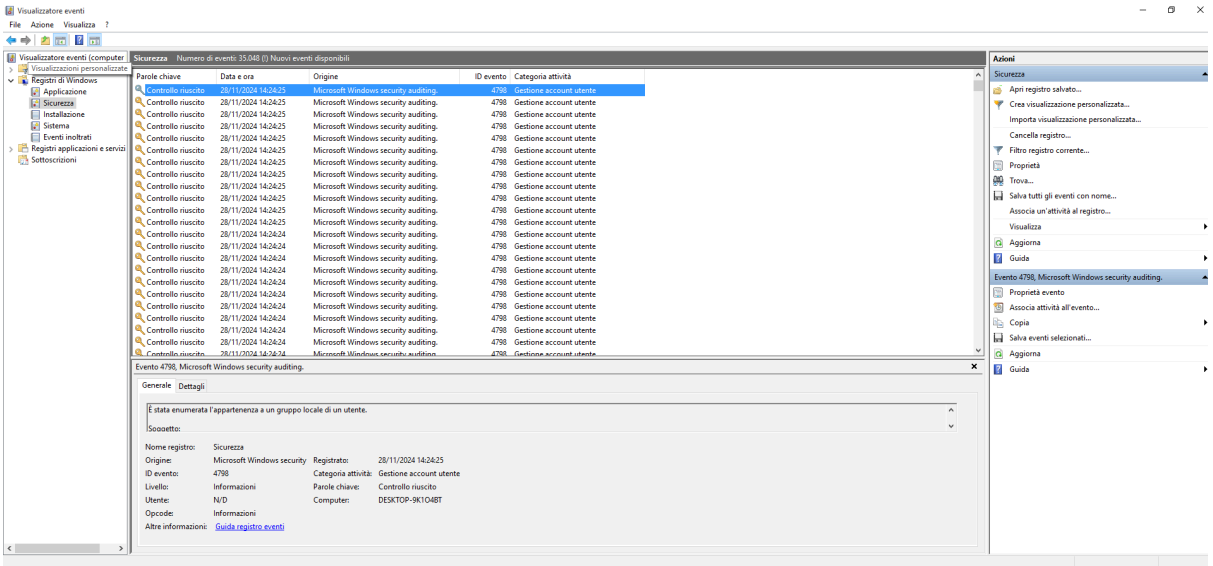
Accesso ai file di log di Windows

Per accedere al file di log di Windows sarà necessario utilizzare il prompt di comando digitando: *eventvwr*.

Così facendo avremo accesso al visualizzatore di eventi, uno strumento essenziale per monitorare e gestire gli eventi di sistema, in questo caso quelli legati alla sicurezza.

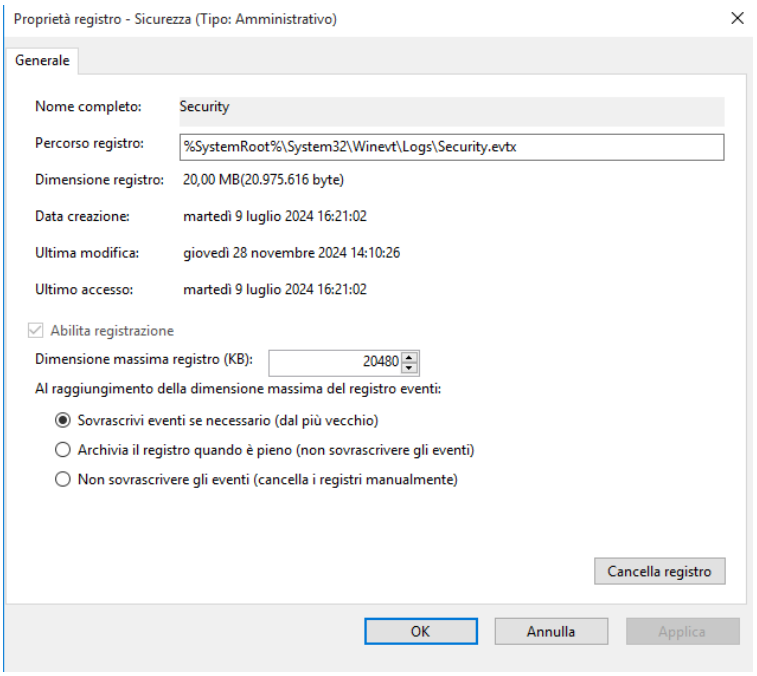


Si è andata ad aprire la sezione relativa alla sicurezza col seguente risultato, ovvero l'apertura dei registri di sicurezza:



Se volessimo impostare delle specifiche configurazioni, andremo ad aprire le proprietà del registro, nelle quali potremo decidere la dimensione del registro ed suo

percorso, ma anche la politica di gestione dei log (sovrascrivere o meno gli eventi, oppure archiviarli).



Andando ad analizzare il registro, potremo avere accesso a dati come l'ID dell'evento, se l'accesso è riuscito o fallito, la categoria, il livello di gravità.
Cliccando sul singolo eventi si ottiene una descrizione più dettagliata, in cui sono specificati ulteriori dati specifici, nome dell'utente coinvolto, l'ora esatta e l'azione eseguita.
Sui file di log è possibile anche filtrare e ricercare eventi specifici allo scopo di ottenere un risultato più rapido.
I file di log possono anche essere esportati per analisi successive o per la conservazione di prove in caso di audit o indagini,

Conclusioni

Il visualizzatore eventi di Windows è uno strumento potente per gestire i file di log di sicurezza, essenziale per monitorare, analizzare e rispondere a eventi critici di sicurezza in un sistema Windows. Configurare correttamente le proprietà del registro, filtrare e salvare gli eventi sono tutte operazioni che migliorano la capacità di risposta a potenziali minacce e facilitano le attività di auditing e di investigazione. La gestione adeguata dei log è dunque un aspetto chiave per la protezione e l'integrità di un ambiente Windows.

Progetto a cura di
Sonia Laterza