Esercizio di oggi:

Creazione e Gestione delle Regole per i File di Log della Sicurezza in Windows
Obiettivo:

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".

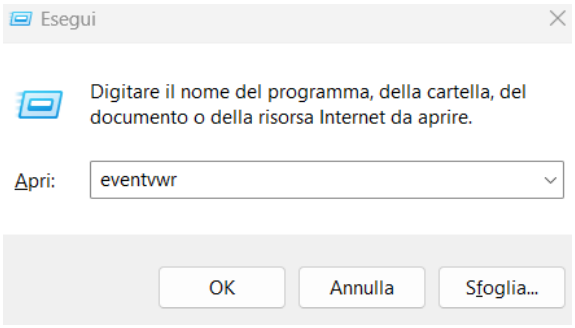
○ Digita eventvwr e premi Invio.

2. Configurare le Proprietà del Registro di Sicurezza:

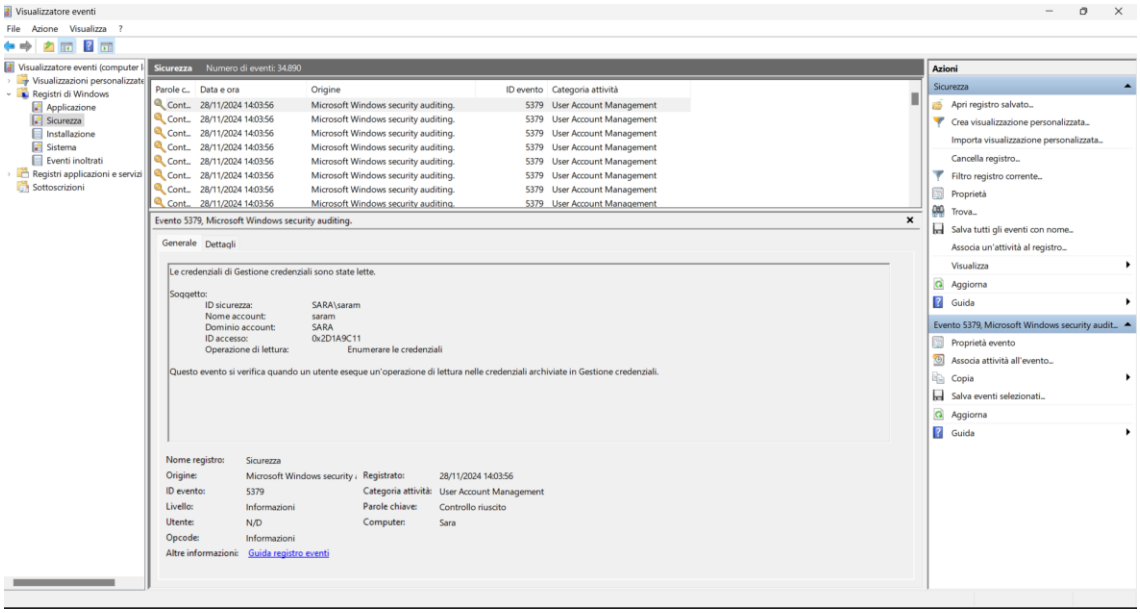
○ Nel pannello di sinistra, espandi "Registri di Windows" e seleziona "Sicurezza".

Esecuzione:

Apriamo il visualizzatore, e inseriamo eventvwr



Successivamente andiamo su Registri di windows e selezioniamo sicurezza:


Visualizzatore eventi
File Azione Visualizza ?
Visualizzatore eventi (computer l
Visualizzazioni personalizzate
Registri di Windows
Applicazione
Sicurezza
Installazione
Sistema
Eventi inoltrati
Registri applicazioni e servizi
Sottoscrizioni
Sicurezza Numero di eventi: 34.890
Parole c... Data e ora Origine ID evento Categoria attività
Cont... 28/11/2024 14:03:56 Microsoft Windows security auditing. 5379 User Account Management
Evento 5379, Microsoft Windows security auditing.
Generale Dettagli
Le credenziali di Gestione credenziali sono state lette.
Soggetto:
ID sicurezza: SARA\saram
Nome account: saram
Dominio account: SARA
ID accesso: 0x2D1A9C11
Operazione di lettura: Enumerare le credenziali
Questo evento si verifica quando un utente eseque un'operazione di lettura nelle credenziali archiviate in Gestione credenziali.
Nome registro: Sicurezza
Origine: Microsoft Windows security
Registrato: 28/11/2024 14:03:56
ID evento: 5379
Categoria attività: User Account Management
Livello: Informazioni
Parole chiave: Controllo riuscito
Utente: N/D
Computer: Sara
Opcode: Informazioni
Altre informazioni: Guida registro eventi
Azioni
Sicurezza
Apri registro salvato...
Crea visualizzazione personalizzata...
Importa visualizzazione personalizzata...
Cancella registro...
Filtro registro corrente...
Proprietà
Trova...
Salva tutti gli eventi con nome...
Associa un'attività al registro...
Visualizza
Aggiorna
Guida
Evento 5379, Microsoft Windows security audit...
Proprietà evento
Associa attività all'evento...
Copia
Salva eventi selezionati...
Aggiorna
Guida