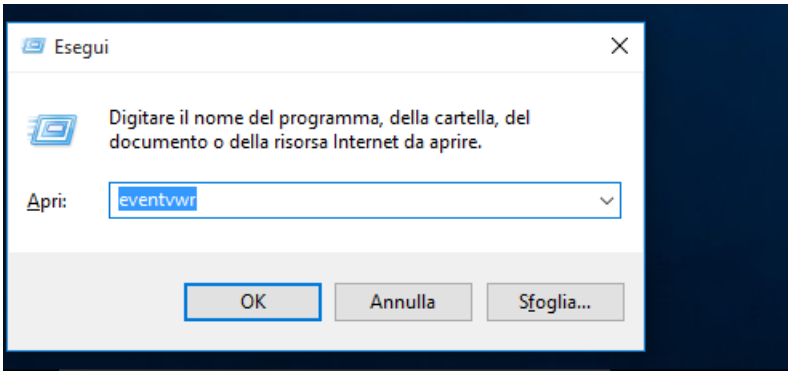
UNIT3 S9/L4 - Creazione e Gestione delle Regole per i File di Log della Sicurezza in Windows

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

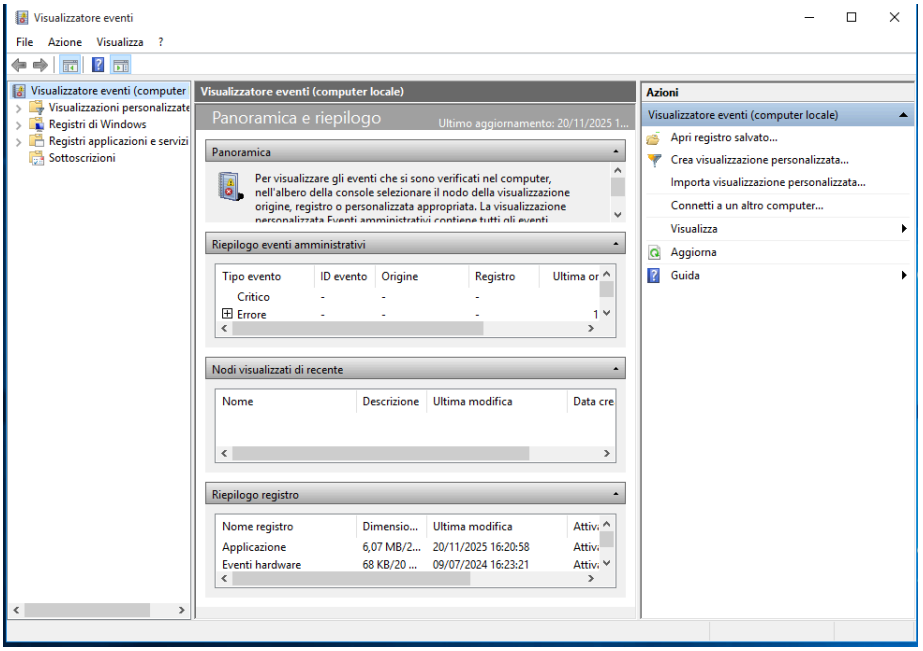
Istruzioni:

1. *Accedere al Visualizzatore Eventi:*
   a) Apri il Visualizzatore eventi premendo Win + R per aprire la finestra "Esegui".
   b) Digita eventvwr e premi Invio.
2. *Configurare le Proprietà del Registro di Sicurezza:*
   a) Nel pannello di sinistra, espandi "Registri di Windows" e seleziona "Sicurezza".
3. *Provate a impostare il log dei Login/Logoff*

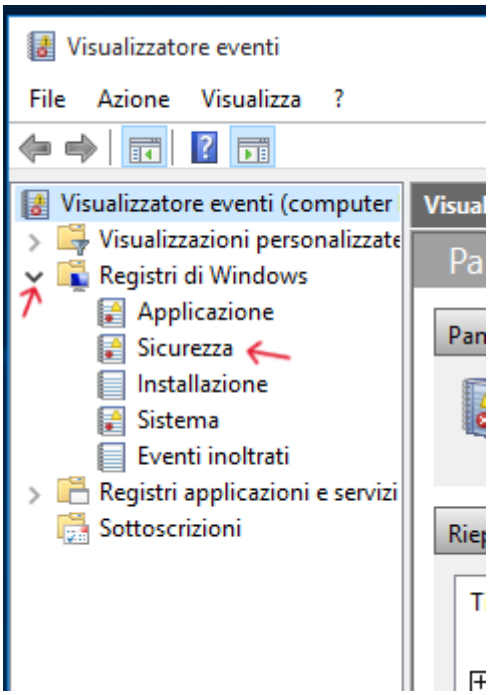
Esercizio:
accendo la VM windows 10 e utilizzo la combo di comandi “Win + R” per aprire la finestra di esegui, dentro la quale cercherò “**eventvwr**”



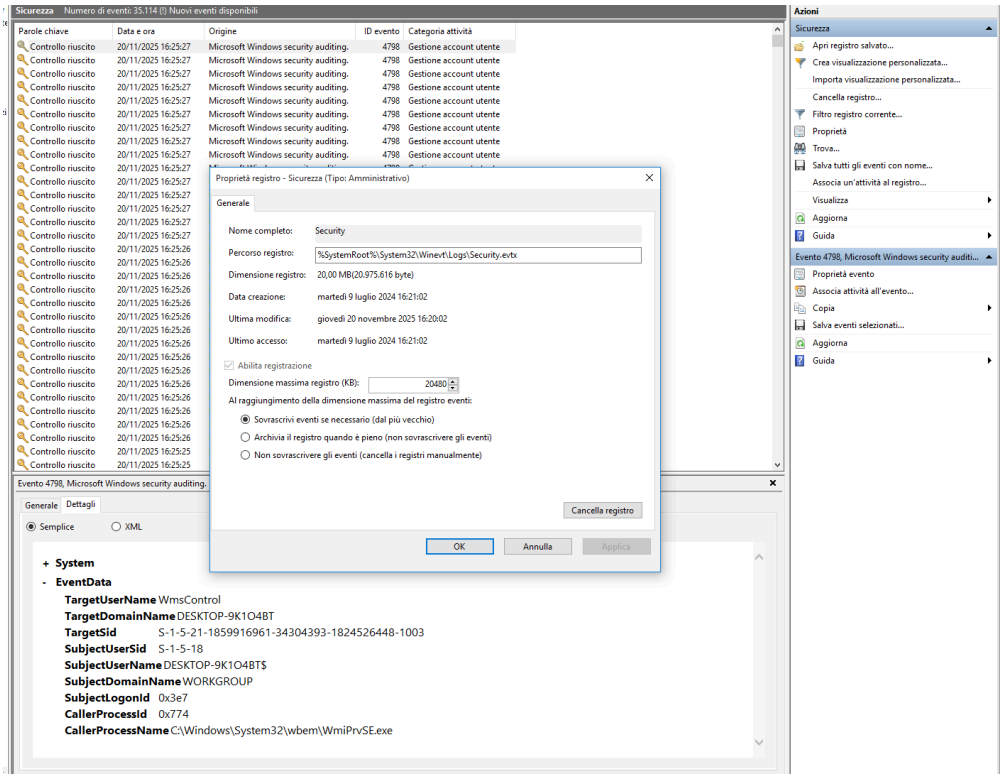
La schermata che si aprirà è la seguente



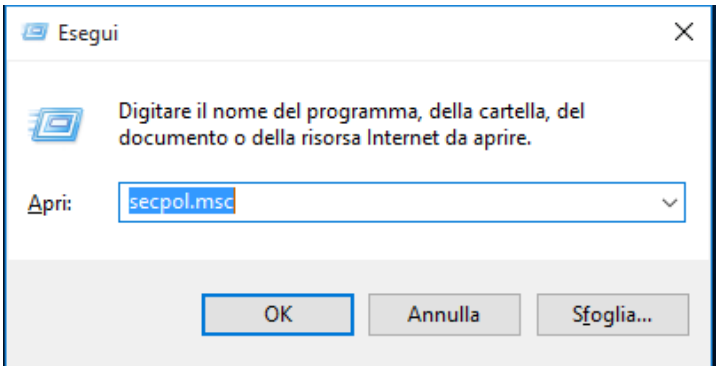
A questo punto andrò su “registri di windows” → “sicurezza”



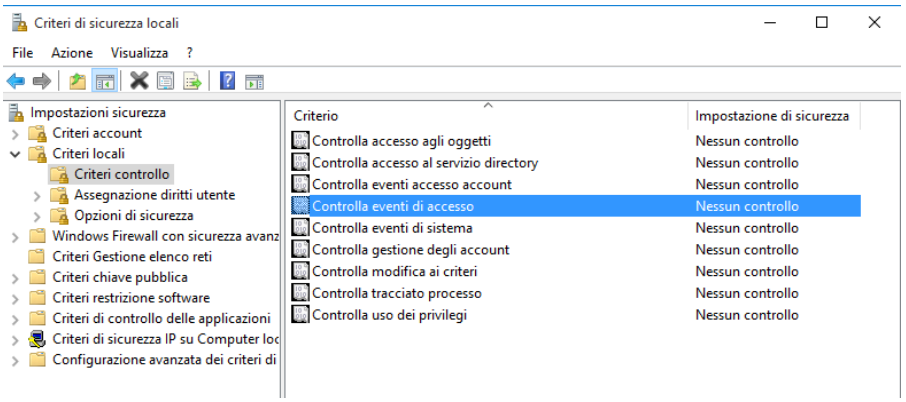
cliccando due volte su uno dei log o con tasto destro e poi → “proprietà evento” posso vedere nello specifico le informazioni del log.
Se invece clicco nel menù in alto a destra su “proprietà” potrò dalla finestra di dialogo “**Proprietà registro: Sicurezza**” gestire le dimensioni massimi del registro (ossia quanto spazio riservare al file di log).



Per l'attivazione degli eventi di login/logoff invece bisogna sempre aprire la finestra dell'esegui tramite Win + R, digitare "**secpol.msc**".



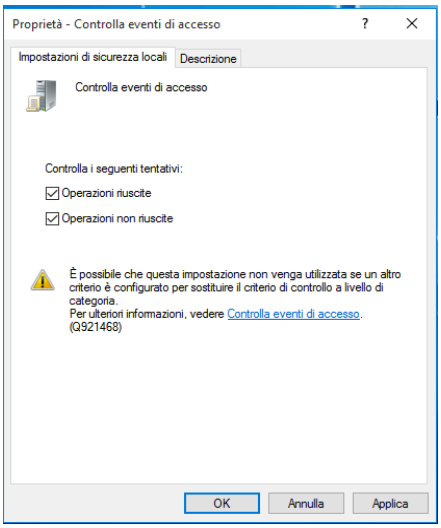
A questo punto ci si aprirà la schermata dei criteri di sicurezza locali.
cliccando su "criteri locali" → "criteri di controllo" → "controlla eventi di accesso"



Il pannello che si aprirà sarà quello appunto del controllo degli eventi di accesso. Spuntando le due opzioni

- operazioni riuscite
- operazioni non riuscite

e selezionando OK, Windows a questo punto sarà in grado di registrare gli eventi di accesso e disconnessione nel **Registro di Sicurezza**.



Gli eventi con ID 4623 dovrebbero corrispondere all'**accesso riuscito** mentre quelli con ID 4625 dovrebbero corrispondere all'**accesso fallito.**