ESERCIZIO S9 L4

EPICODE

Pratica S9/L4 PDF

Cyber Security & Ethical Hacking

Esercizio

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:
   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

SVOLGIMENTO

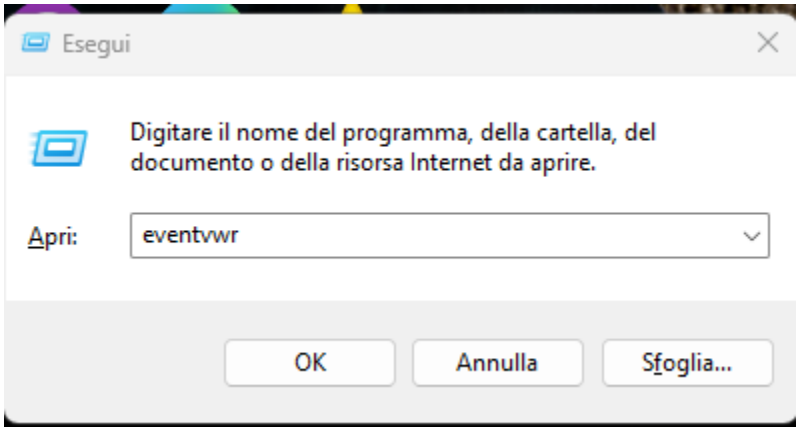
1. Accedere al Visualizzatore eventi

Per prima cosa, apro il Visualizzatore eventi di Windows:

Premo il tasto Win + R sulla tastiera. Questo aprirà la finestra "**Esegui**".

Digito **eventvwr** nel campo di testo.

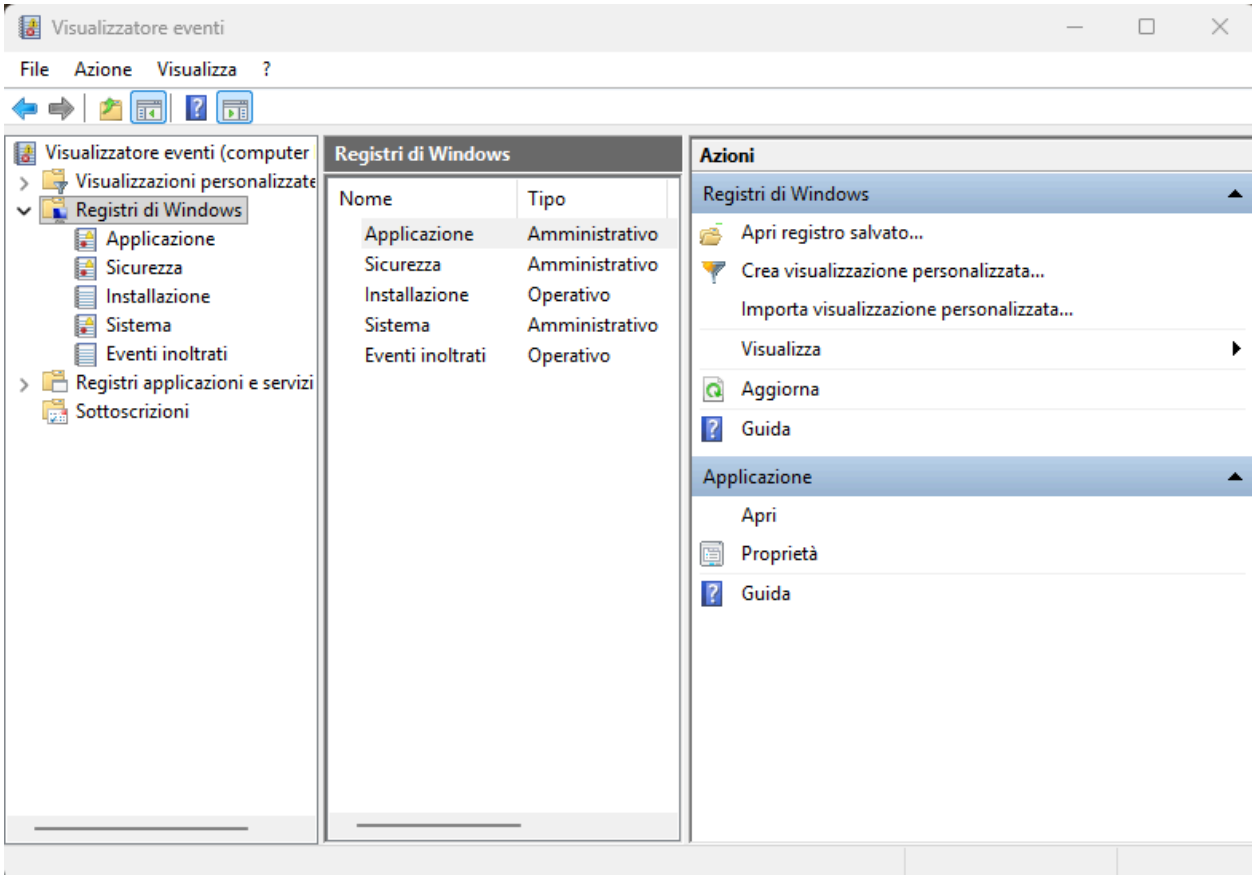
Premo Invio.



2. Configurare le Proprietà del Registro di Sicurezza

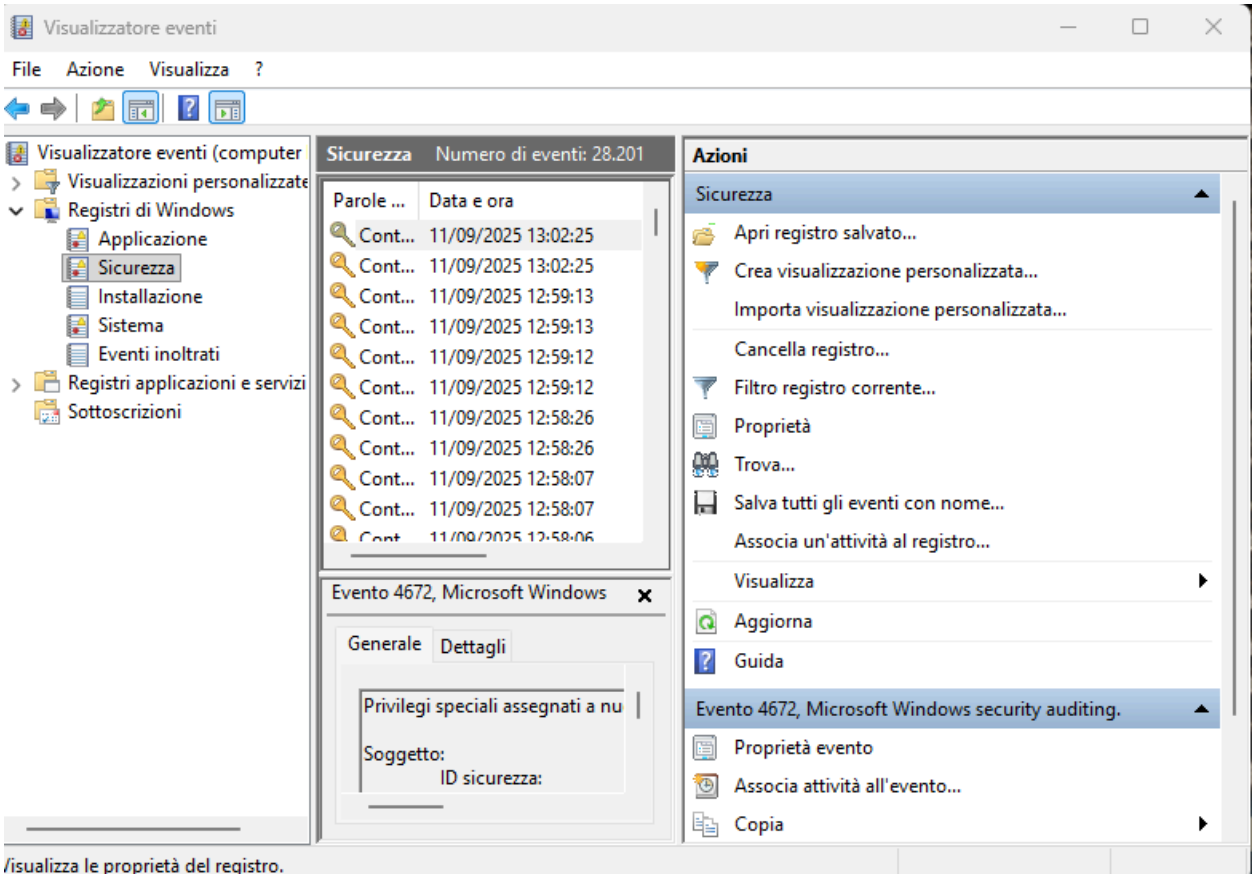
Ora, si può configurare il registro di sicurezza:

Nel pannello di sinistra del visualizzatore eventi, espando **Registri di Windows**

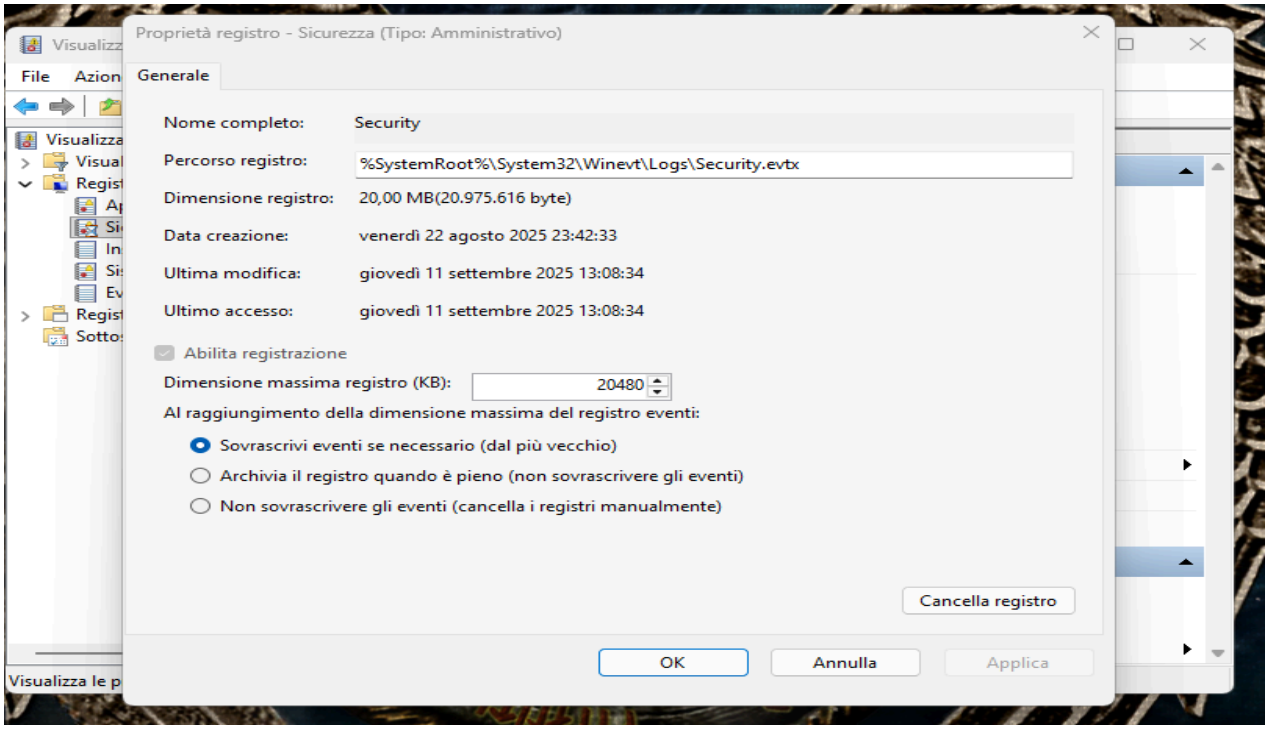


Seleziono il registro **Sicurezza**.

Nel pannello di destra, vado a cliccare su **Proprietà** (o si può anche cliccare con il tasto destro su "Sicurezza" e selezionare **Proprietà**).



Si aprirà una nuova finestra con le **proprietà del registro di sicurezza**.



3. Gestione delle Regole di Log

Qui si possono definire le seguenti regole per la gestione del log:

Dimensione massima del registro (KB): Imposta un limite alla dimensione del file di log. Una volta raggiunto questo limite, Windows gestirà i log in base alla tua scelta.

Quando viene raggiunta la dimensione massima del registro >>> sono presenti 3 opzioni principali:

1. Sovrascrivi gli eventi precedenti (il più vecchio per primo):

Quando sceglierla: Questa è l'opzione più comune e pratica per la maggior parte degli utenti e dei sistemi.

Vantaggi:

È un'impostazione che non richiede manutenzione.

Garantisce che il registro di sicurezza non riempia mai il disco, poiché i nuovi eventi sostituiscono automaticamente i più vecchi una volta raggiunto il limite di dimensione.

È adatta per il monitoraggio a breve termine.

Svantaggi:

Si possono perdere dati importanti. Se un evento di sicurezza critico si è verificato più di qualche giorno (o settimana) fa, le informazioni potrebbero essere state già sovrascritte.

2. Archivia il registro quando pieno, non sovrascrivere gli eventi:

Quando sceglierla: Questa è l'opzione migliore se la **sicurezza e la conformità** sono la massima priorità e si vuole conservare una cronologia completa di tutti gli eventi. È l'ideale per server critici o ambienti aziendali.

Vantaggi:

Zero perdita di dati. Ogni evento viene conservato.

Facilita le indagini forensi e gli audit di sicurezza, poiché hai a disposizione tutti i log storici.

Svantaggi:

Richiede più spazio su disco. Nel tempo, verranno creati numerosi file di archivio che possono occupare molto spazio.

Richiede una gestione attiva per la pulizia o il backup dei vecchi archivi.

3. Non sovrascrivere gli eventi (cancella il registro manualmente):

Quando sceglierla: Questa opzione non è generalmente consigliata per i sistemi di produzione.

Vantaggi:

Assoluta garanzia di non perdere nessun dato, poiché la registrazione si ferma quando il log è pieno.

Svantaggi:

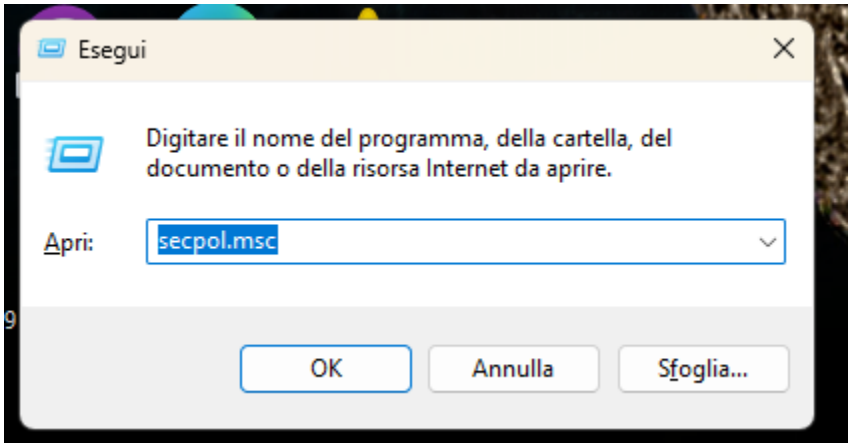
È molto rischiosa. Se il registro si riempie e nessuno lo pulisce manualmente, Windows smette completamente di registrare nuovi eventi di sicurezza. Questo crea una "zona d'ombra" dove non viene registrato nulla, lasciando il sistema vulnerabile.

Applicazione delle modifiche: Dopo aver scelto le opzioni desiderate, si può cliccare su OK per salvare le nuove impostazioni.

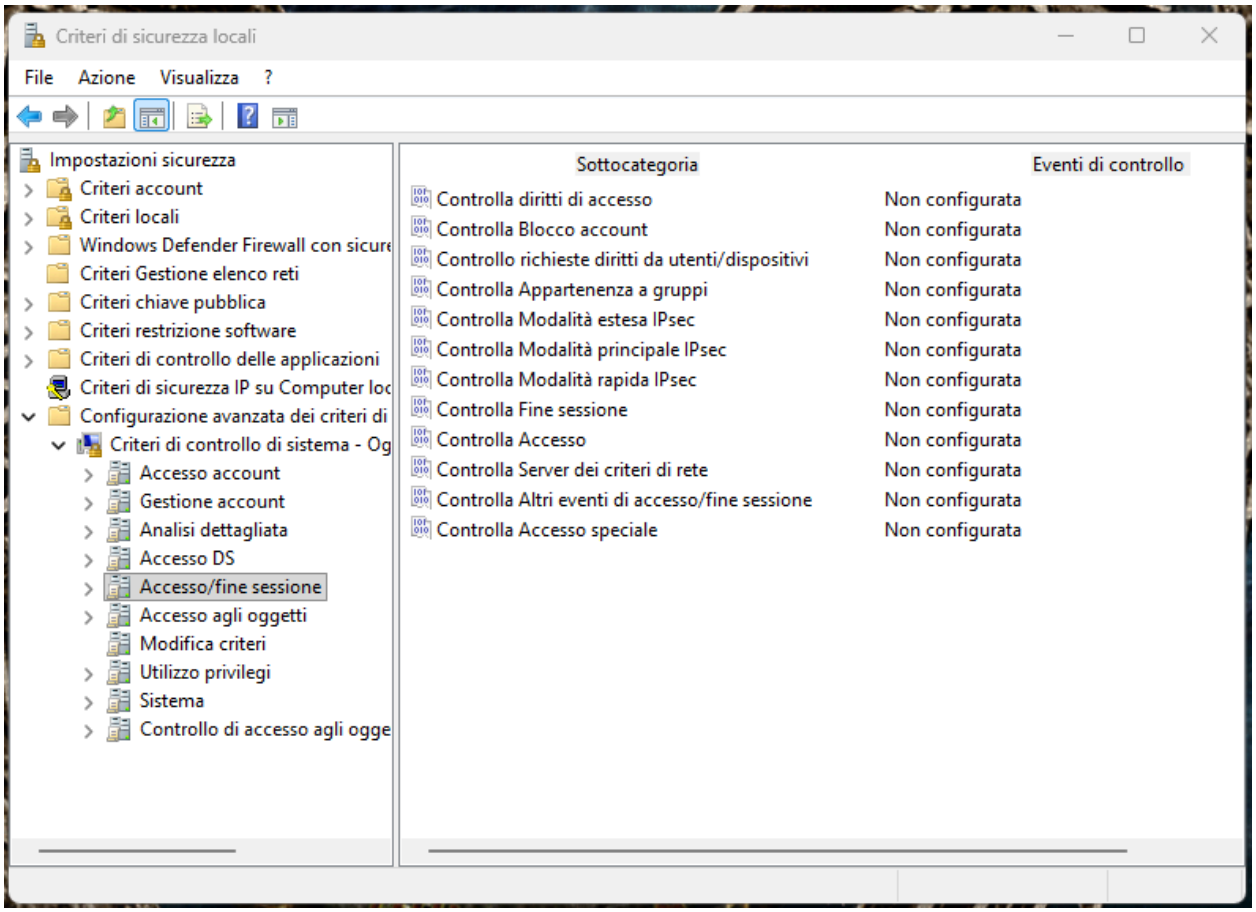
In questo modo, si possono configurare le regole per la gestione del log di sicurezza, garantendo che Windows registri gli eventi di sicurezza secondo le tue esigenze.

IMPOSTAZIONE log del **Logon/Logoff**

Utilizzo il comando Win + R e digito secpol.msc >>> Invio



Navigo nella sezione **Configurazione avanzata dei criteri di controllo**



Seleziono “**Controlla accesso**” e abilito i criteri di login (accesso) e logoff (fine sessione), con esito positivo e negativo.

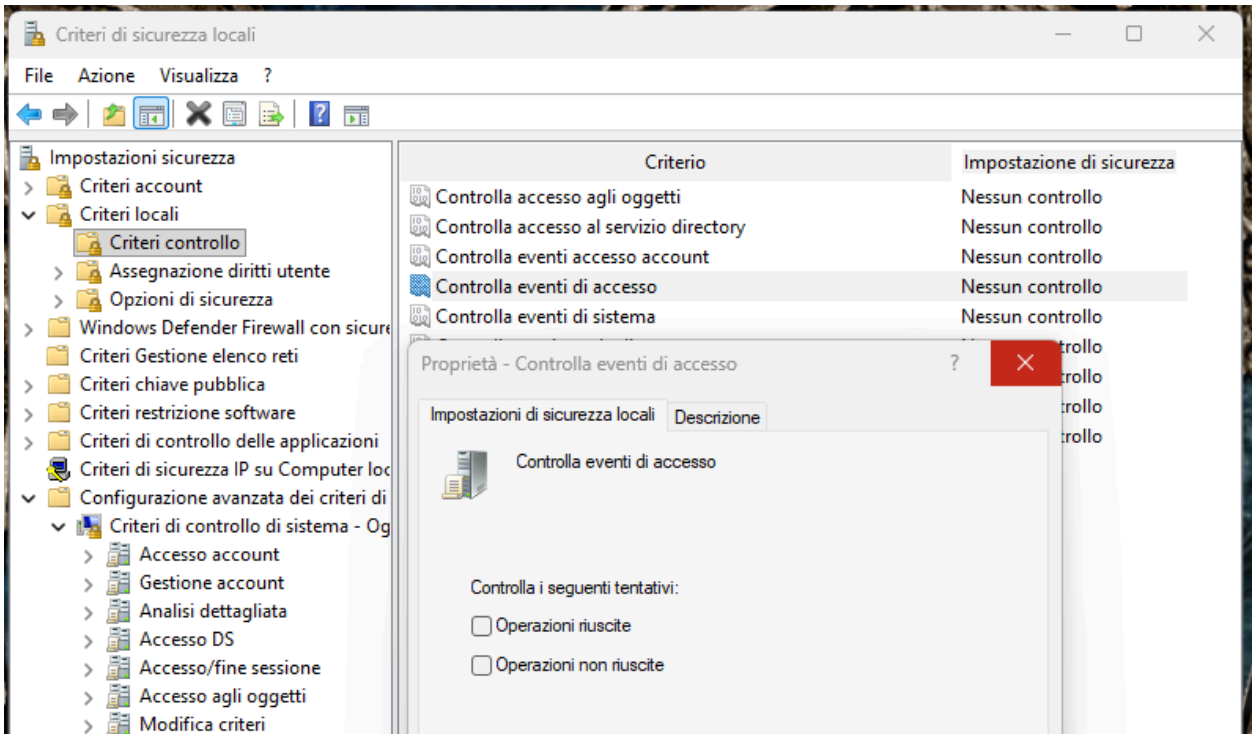
Sottocategoria	Eventi di controllo
Controlla Blocco account	Non configurata
Controllo richieste diritti da utenti/dispositivi	Non configurata
Controlla Appartenenza a gruppi	Non configurata
Controlla Modalità estesa IPsec	Non configurata
Controlla Modalità principale IPsec	Non configurata
Controlla Modalità rapida IPsec	Non configurata
Controlla Fine sessione	Esito positivo e negativo
Controlla Accesso	Esito positivo e negativo

Successivamente, nel pannello di sinistra della finestra >>> **Criteri Locali**, seguo questo percorso:

Espando **Criteri Locali**.

Seleziono la cartella **Criteri di Controllo**.

Doppio clic su **Controlla eventi di accesso**



Si aprirà una nuova finestra. Spunto le caselle per **Operazioni riuscite** e **Operazioni non riuscite**.

Clicco su **Applica** e poi su **OK** per salvare le modifiche.

Per verificare l'effettivo funzionamento riavvio la macchina e una volta effettuato di nuovo l'accesso controllo i log. Gli eventi generati sono:

"**Accesso riuscito**" >>> **Logon** (**ID 4624 =** indica che il logon è riuscito)

"Disconnessione" >>> **Logoff** (**ID 4647 =** Indica che la sessione si è chiusa correttamente)