Esercizio_S8_L4_Windows_Log

Consegna

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:**

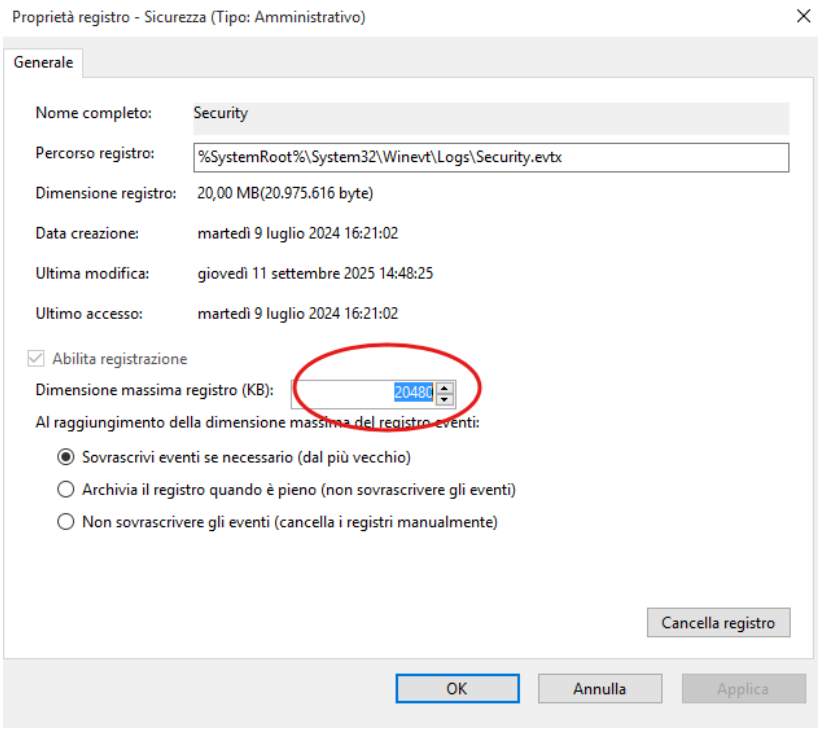
Nel pannello di sinistra, espandi "Registri di Windows" e seleziona "Sicurezza".

Svolgimento

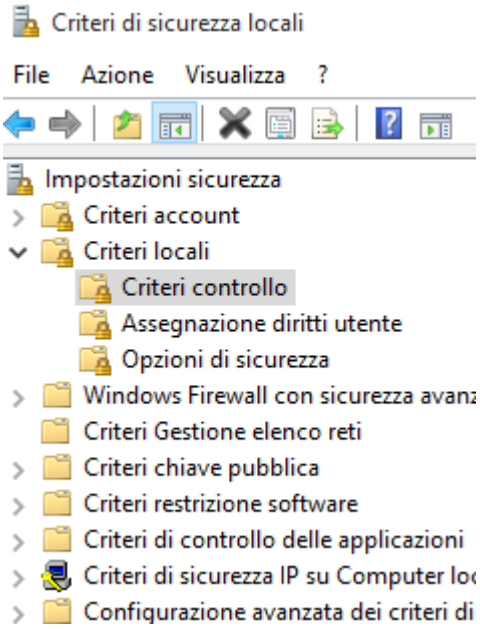
Dopo aver seguito le istruzioni riportate nella consegna ci si ritroverà all'interno del menù dell'event viewer.

Una delle cose opzioni più importanti che è possibile modificare da qui è la **dimensione dei file log**.

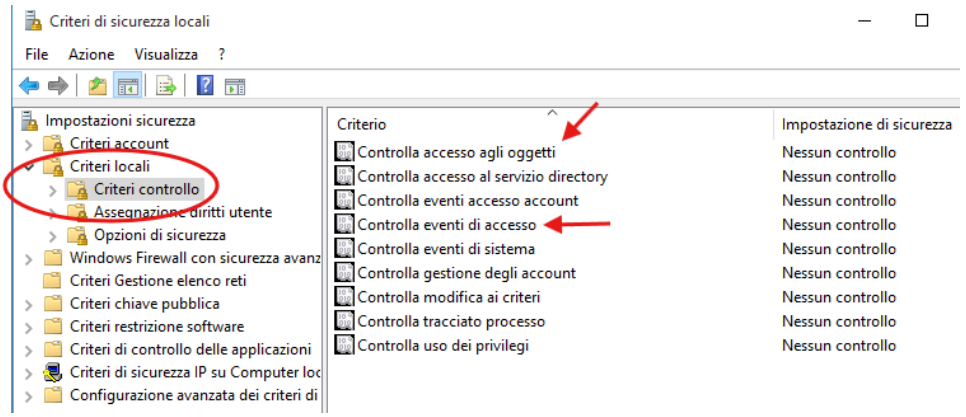
Spostandoci sul menù di destra alla voce proprietà troviamo infatti l'opzione per modificare la **dimensione massima** del registro eventi assieme alla possibilità di **sovrascrivere gli eventi** o meno.



Possiamo ora passare ad attivare alcune impostazioni in modo da registrare determinate categorie di eventi; navigando infatti verso Pannello di controllo > Strumenti di amministrazione > Criteri di sicurezza locali possiamo andare ad attivare i log a seconda di cosa siamo interessati a monitorare all'interno della macchina:



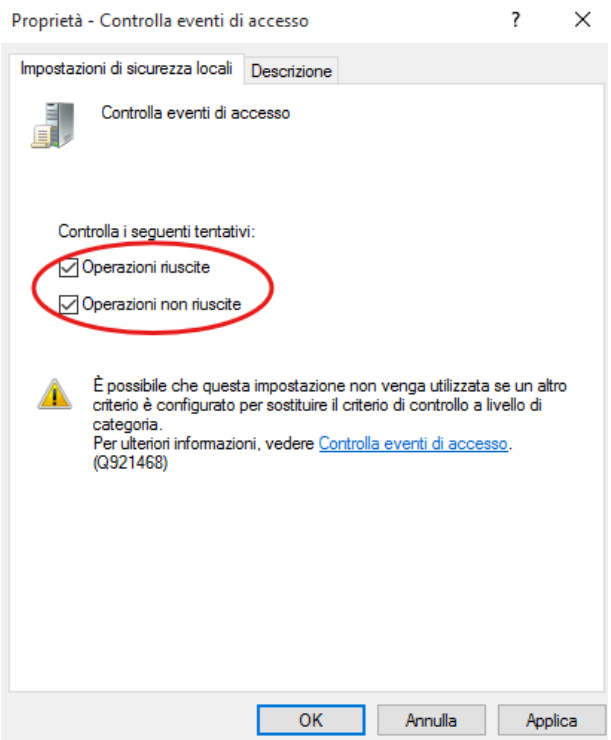
Al fine di questo test andremo semplicemente ad attivare i log per tre voci sotto alla voce criteri di controllo:



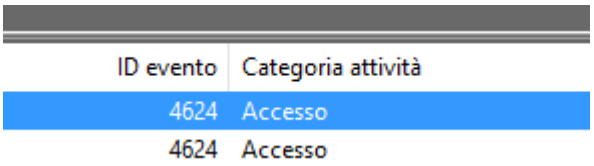
Le voci che attiveremo saranno quelle relative a:

- Controllo di eventi di accesso
- Controllo uso dei privilegi
- Controllo tracciato processo

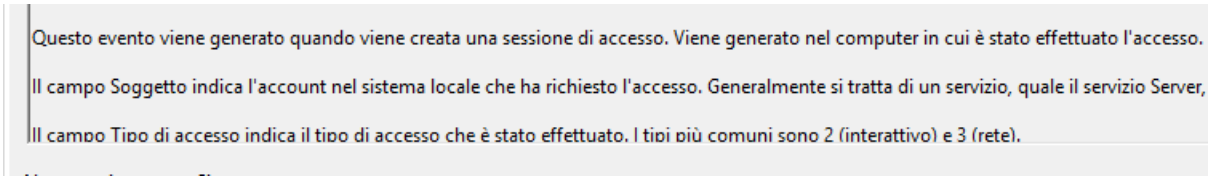
Procediamo dunque con la prima voce ed una volta aperta possiamo spuntare le opzioni per il controllo delle operazioni riuscite e di quelle non riuscite in modo che il sistema registri entrambe le tipologie di eventi:



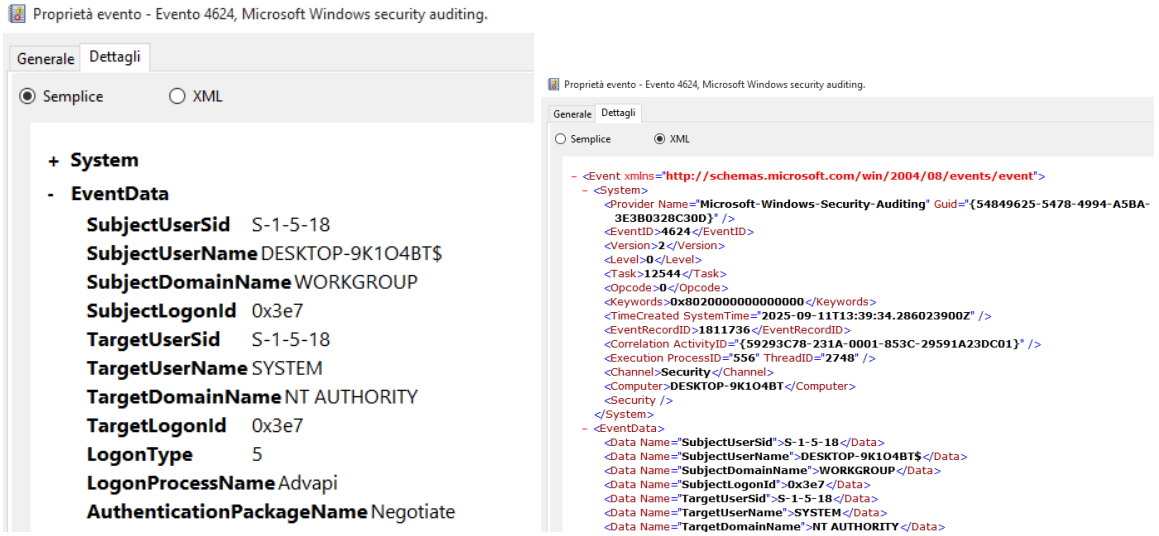
Eseguendo poi un semplice cambio di utente possiamo tornare all'interno dell'event viewer e notare la creazione di un log con ID 4624:



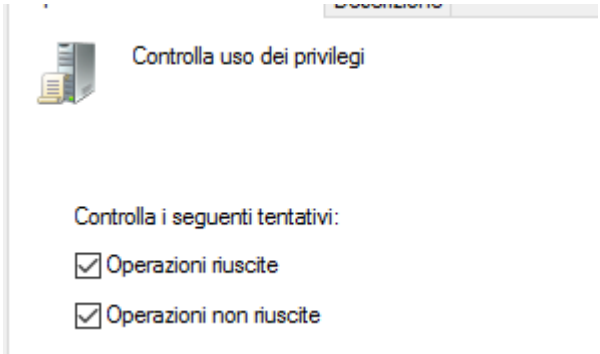
4624 → login riuscito al sistema.



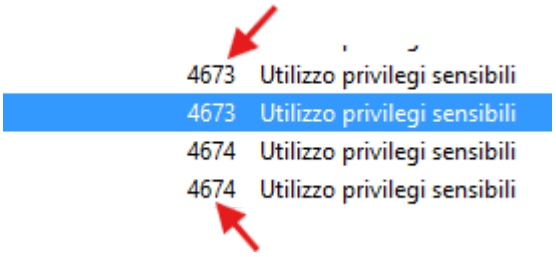
Entrando nel dettaglio dell'evento è possibile trovare un'intera sessione rappresentate i suoi dati sia in **formato semplice/leggibile** che in formato **XML**:



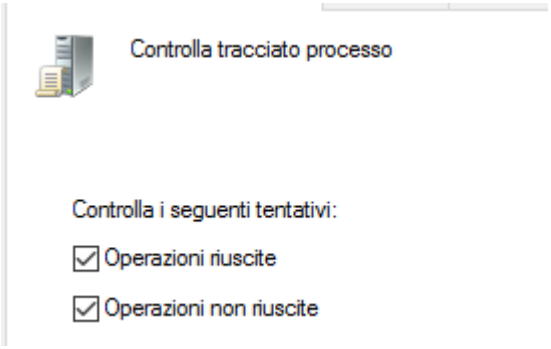
Lo stesso procedimento possiamo effettuarlo per il controllo dei privilegi:



I log creati in questo caso a seguito dell'avvio di un software o di accesso a servizi/oggetti saranno con ID 4672, 4673 e 4674 a seconda dei privilegi utilizzati/richiesti.



Possiamo infine notare che configurando i log per i processi:



All'avvio e al termine di un determinato programma otterremo i seguenti log:

4688 → creazione di nuovi processi.

4689 → terminazione dei processi precedentemente avviati.

Log ID Windows

Possiamo di seguito trovare un riassunto dei principali Log ID che potremmo dover analizzare durante operazioni di auditing, analisi forense e sicurezza:

🔐 *Eventi di accesso (logon / logoff)*

- ***4624*** *→ Account connesso con successo (Login riuscito)*
- ***4625*** *→ Tentativo di accesso non riuscito (Login fallito)*
- ***4634*** *→ Account disconnesso (Logoff)*
- ***4647*** *→ Logout iniziato dall'utente*
- ***4672*** *→ Privilegi speciali assegnati a un nuovo login (es. admin)*

🛠️ *Processi e oggetti*

- ***4688*** *→ Creazione di un nuovo processo*
- ***4689*** *→ Terminazione di un processo*
- ***4697*** *→ Installazione di un nuovo servizio di sistema*
- ***4657*** *→ Modifica di un valore nel Registro di sistema*

👤 *Gestione account e gruppi*

- ***4720*** *→ Creato un nuovo account utente*
- ***4722*** *→ Account utente abilitato*
- ***4723*** *→ Tentativo di cambio password*
- ***4724*** *→ Tentativo di reset password da parte di un admin*
- ***4725*** *→ Account utente disabilitato*
- ***4726*** *→ Account utente eliminato*
- ***4732*** *→ Utente aggiunto a un gruppo locale di sicurezza*
- ***4733*** *→ Utente rimosso da un gruppo locale di sicurezza*

🔒 *Oggetti e accesso a risorse*

- ***4663*** *→ Accesso a un oggetto (file/cartella)*
- ***4656*** *→ Una richiesta di accesso a un oggetto è stata fatta*
- ***4658*** *→ Handle a un oggetto chiuso*

🌐 *Rete e autenticazioni particolari*

- *4776 → Tentativo di autenticazione NTLM*
- *4768 → Richiesta Ticket Kerberos (TGT)*
- *4769 → Richiesta Ticket Service Kerberos*
- *4771 → Errore di autenticazione Kerberos*

⚠️ *Attività sospette o privilegiate*

- *4673 → È stato invocato un servizio che richiede privilegi speciali*
- *4674 → Tentativo di accesso a un oggetto privilegiato*
- *4719 → Modificata la configurazione di auditing di sistema*
- *1102 → Cancellati i log di audit di sicurezza*

Conclusioni

Con questo esercizio abbiamo imparato a configurare e gestire i log di sicurezza in Windows utilizzando sia il **Visualizzatore Eventi** che i **Criteri di sicurezza locali**.
Attivando categorie specifiche di auditing (accessi, privilegi, processi) è stato possibile osservare in pratica la generazione di eventi distinti:

- **4624** per login riusciti.
- **4672/4673/4674** per l'uso di privilegi speciali.
- **4688/4689** per la creazione e la terminazione di processi.

Questo dimostra come Windows metta a disposizione strumenti di monitoraggio potenti, che permettono all'amministratore di sistema di **rilevare comportamenti sospetti** (es. esecuzione di programmi non autorizzati o tentativi di accesso anomali) e di mantenere una traccia utile in ottica di **sicurezza e auditing forense**.