S9-L4 FILE DI LOG DI WINDOWS

**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.

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

**Introduzione:** L'obiettivo di questo esercizio è comprendere come configurare e gestire i file di log della sicurezza utilizzando il Visualizzatore eventi di Windows. Questa operazione è cruciale per monitorare le attività di sistema e rilevare eventuali tentativi di accesso non autorizzati o anomalie. Il Visualizzatore eventi rappresenta uno strumento integrato in Windows che consente di raccogliere informazioni dettagliate sui registri di sistema, tra cui quelli relativi alla sicurezza.

**Procedura Svolta:**

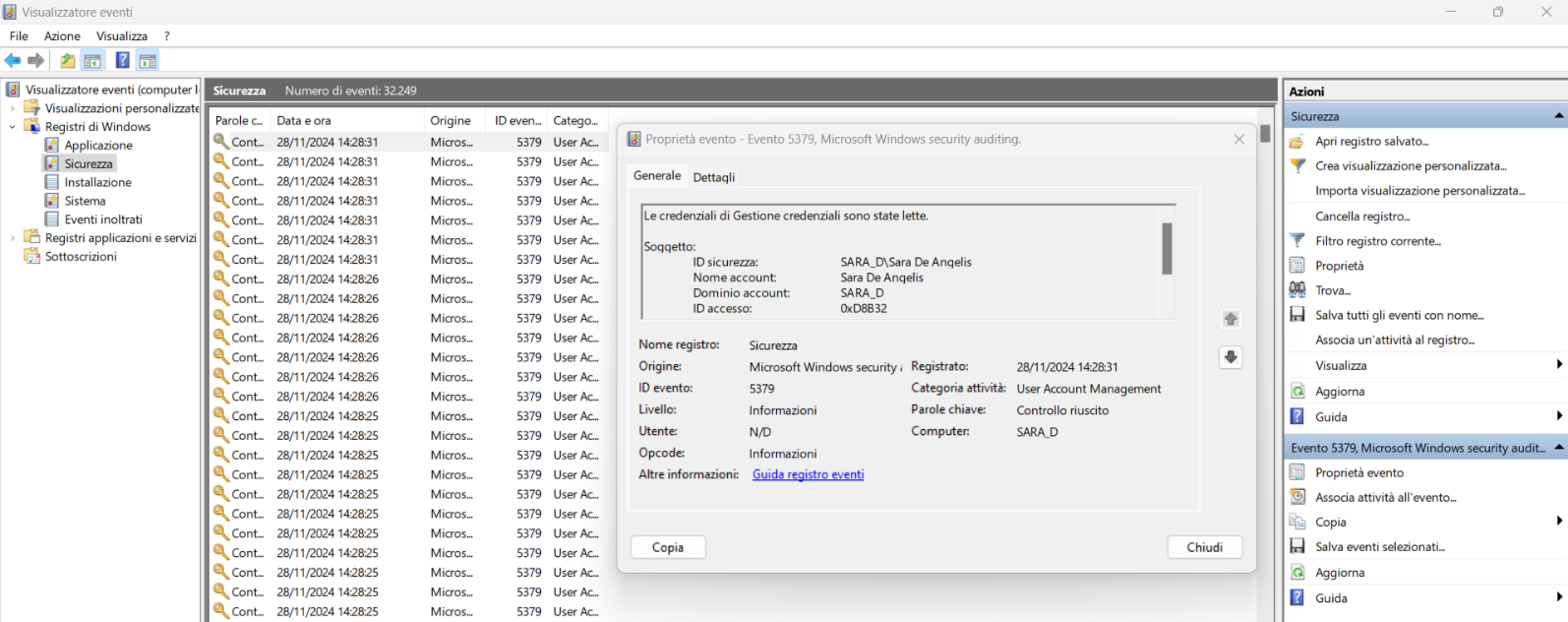
1. **Accesso al Visualizzatore Eventi:**
   * Per aprire il Visualizzatore eventi, ho premuto la combinazione di tasti Win + R per avviare la finestra "Esegui".
   * Ho digitato eventvwr e premuto *Invio*. Questo comando ha avviato l'applicazione "Visualizzatore eventi".
2. **Navigazione e Configurazione:**
   * Nel pannello di sinistra del Visualizzatore eventi, ho espanso la sezione **"Registri di Windows"** e selezionato il registro denominato **"Sicurezza"**.
   * Questa sezione raccoglie eventi relativi alla sicurezza, come tentativi di accesso, modifiche alle policy di sicurezza e altre attività critiche.
3. **Esplorazione delle Proprietà del Registro di Sicurezza:**
   * Facendo clic con il tasto destro su **"Sicurezza"** e selezionando **"Proprietà"**, è stato possibile configurare aspetti importanti del registro:
     + **Dimensione massima del file di registro**: Ho definito un limite per evitare che il file di log occupi troppo spazio.
     + **Gestione del file di log**: Ho scelto l'opzione per sovrascrivere gli eventi più vecchi quando necessario, assicurandomi che i log più recenti vengano sempre salvati.
   * Ho inoltre verificato che il registro sia configurato per tracciare eventi rilevanti, come accessi non riusciti o modifiche alle policy di sicurezza.
4. **Analisi degli Eventi di Sicurezza:**
   * Ho esaminato gli eventi elencati nel registro di sicurezza. Ciascun evento contiene dettagli come l'ID evento, l'utente coinvolto, l'ora e la descrizione dell'evento.
   * Ho utilizzato i filtri del Visualizzatore eventi per individuare specifici tipi di eventi, come quelli relativi al login fallito (ID evento 4625).

**Osservazioni e Conclusioni:**

La gestione dei file di log della sicurezza in Windows è essenziale per garantire la tracciabilità delle attività di sistema e il rilevamento tempestivo di comportamenti sospetti. Questo esercizio mi ha permesso di:

* Comprendere l'importanza dei registri di sicurezza.
* Apprendere come configurare le impostazioni del registro per ottimizzare la conservazione e l'accesso ai log.
* Analizzare eventi specifici per individuare possibili vulnerabilità.

**Applicazione Pratica:** L'analisi dei registri può essere combinata con strumenti di monitoraggio automatico per rilevare e rispondere a incidenti di sicurezza in tempo reale. Questo esercizio è un passo fondamentale per chi aspira a lavorare nel campo della sicurezza informatica, poiché rappresenta una delle basi del monitoraggio proattivo dei sistemi.



IDENTIFICAZIONI ACCESSI ANOMALI

Per capire se ci sono **accessi anomali** nei log della sicurezza di Windows, puoi seguire questi passi:

**1. Identifica gli eventi critici nei registri di sicurezza**

Nel Visualizzatore eventi, concentrati sugli ID evento che riguardano l'autenticazione e l'accesso. Alcuni esempi di ID rilevanti:

* **4624**: Accesso riuscito.
* **4625**: Tentativo di accesso non riuscito.
* **4771**: Errore di autenticazione Kerberos.
* **4768**: Richiesta di ticket Kerberos (TGT).
* **4672**: Accesso con privilegi speciali.

**2. Cerca pattern sospetti**

* **Accessi falliti multipli (ID 4625)**: Un numero elevato di tentativi falliti, specialmente in un breve intervallo di tempo, può indicare un attacco di forza bruta.
* **Accessi da account inattesi**: Verifica se ci sono tentativi di accesso con account sconosciuti o inattivi.
* **Accessi da località insolite**: Controlla l'origine IP degli accessi, se disponibile, e cerca località insolite per la tua rete.
* **Orari inconsueti**: Un accesso da parte di un utente legittimo a orari improbabili (es. tarda notte) potrebbe essere sospetto.

**3. Usa i filtri per analizzare i log**

Nel Visualizzatore eventi:

* Fai clic con il tasto destro su "Sicurezza" e seleziona **"Filtra registro corrente"**.
* Configura i filtri per visualizzare solo gli eventi con specifici ID (es. 4625 per tentativi falliti o 4624 per accessi riusciti).
* Analizza i dettagli degli eventi: nome utente, origine dell'accesso, timestamp, ecc.

**4. Automatizza il rilevamento di anomalie**

Se gestisci una rete più complessa:

* Utilizza strumenti come **Splunk**, **ELK Stack**, o **Windows Defender for Endpoint** per monitorare e analizzare i log in tempo reale.
* Configura alert automatici per segnalare accessi falliti ripetuti, IP sospetti o account bloccati.

**5. Confronta con la baseline**

Per identificare accessi anomali, confronta gli eventi correnti con il comportamento abituale degli utenti. Crea una baseline che includa:

* Orari e giorni tipici di lavoro.
* Dispositivi e indirizzi IP utilizzati.
* Frequenza degli accessi.

**6. Segnali di compromissione**

Alcuni segnali di compromissione nei log di sicurezza includono:

* Modifica di privilegi utente (es. un utente normale diventa amministratore).
* Creazione o eliminazione improvvisa di account.
* Accessi simultanei allo stesso account da diverse località.

**Esempio pratico:**

Supponiamo di trovare un evento **4625** con nome utente "Admin" proveniente da un IP esterno non riconosciuto alle 3:00 AM. Questo è chiaramente un comportamento anomalo se il sistema è utilizzato solo durante le ore di lavoro.

Analizzando i dettagli degli eventi e incrociando queste informazioni con le policy di accesso aziendali, puoi rilevare anomalie e adottare le contromisure necessarie.

Oltre agli eventi che ti ho già indicato (4624, 4625, 4672), ce ne sono altri molto rilevanti per il monitoraggio degli accessi anomali e di possibili compromissioni in Windows. Di seguito una lista aggiuntiva:

**Eventi relativi all'accesso e autenticazione**

1. **4634**: **Chiusura sessione**  
   Segnala la fine di una sessione utente. Può essere utile verificare se una sessione è terminata correttamente o in modo anomalo.
2. **4648**: **Accesso con credenziali esplicite**  
   Indica un tentativo di autenticazione usando credenziali diverse da quelle correnti, spesso sintomo di attacco da script o di compromissione.
3. **4769**: **Ticket Service (TGS) richiesto**  
   Questo evento è legato al protocollo Kerberos. Richieste insolite di TGS possono suggerire attacchi pass-the-ticket.
4. **4776**: **Tentativo di autenticazione NTLM fallito**  
   Indica un problema con l'autenticazione NTLM, spesso correlato a tentativi di forza bruta o account errati.

**Eventi relativi a modifiche di sistema e account**

1. **4720**: **Creazione di un nuovo account utente**  
   La creazione di nuovi account, soprattutto da parte di utenti non autorizzati, è un chiaro segnale di allarme.
2. **4738**: **Modifica delle proprietà di un account utente**  
   Qualsiasi modifica agli account esistenti (es. cambio password) dovrebbe essere analizzata.
3. **4740**: **Blocco di un account utente**  
   Può indicare tentativi ripetuti di accesso falliti, spesso associati ad attacchi di forza bruta.
4. **4670**: **Modifica dei permessi su un oggetto**  
   Indica cambiamenti nei permessi di file, cartelle o oggetti critici.

**Eventi relativi al controllo amministrativo**

1. **4674**: **Operazione con privilegi speciali tentata**  
   Segnala l'uso di privilegi amministrativi da parte di un utente o di un'applicazione.
2. **4907**: **Modifica della policy di auditing**  
   Modifiche improvvise nelle politiche di auditing possono indicare tentativi di nascondere attività malevole.

**Eventi relativi a rete e connessioni**

1. **5156**: **Connessione rete consentita**  
   Indica che una connessione in entrata o in uscita è stata consentita. È utile per monitorare connessioni sospette da/verso IP non autorizzati.
2. **4771**: **Errore autenticazione Kerberos (Pre-auth)**  
   Può segnalare attacchi di tipo brute force su Kerberos.

**Suggerimenti pratici:**

* Utilizza strumenti di analisi come **Splunk** o **SIEM** per correlare questi eventi e creare avvisi in tempo reale.
* Integra regole di filtraggio per eventi specifici che combaciano con il tuo contesto di rete.

Questi eventi, se monitorati regolarmente, ti permetteranno di identificare accessi anomali e attività sospette nel tuo ambiente Windows.

