

Esercizio di Pratica S9L4 - Creazione e Gestione delle Regole per i File di Log della Sicurezza in Windows

Sergio Falcone

INTRODUZIONE

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".

Provate a impostare il log dei Login/Logoff

PREFAZIONE

L'esercizio si svolgerà all'interno della Macchina Virtuale **FlareVM**, Sistema Operativo **Windows10**

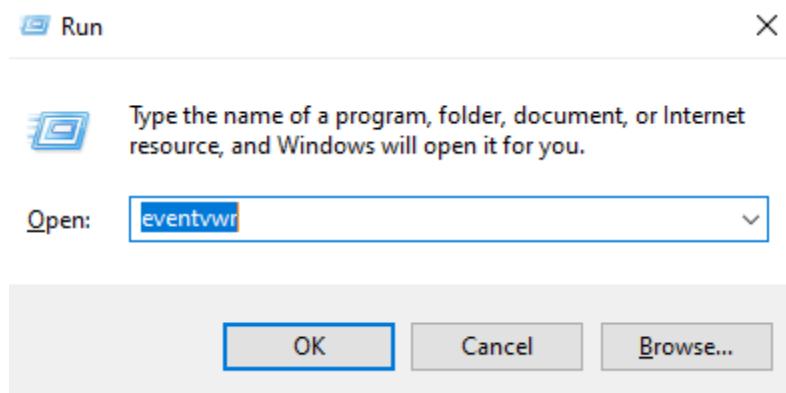
Tratta l'analisi dei **Log** sul **Visualizzatore di eventi di Windows10** (qui **Event Viewer**), in particolare sui **Logon** e **Logoff**.

Entrambi i **Log** sono caratterizzati dalla loro tipologia (**Logon Type**).

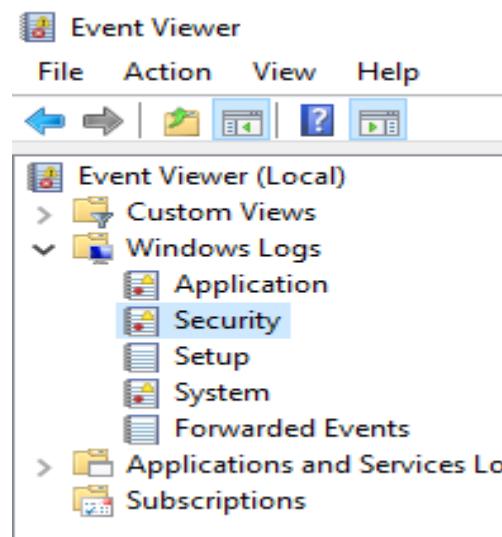
Verranno presi in esame i **Logon Type 2** (Interazione dell'Utente) e i **Logon Type 5** (Interazione dei Servizi)

ESECUZIONE

Come indicato dalle Istruzioni (sezione Introduzione), dalla tastiera si sono premuti i tasti **Win+R** e digitato **eventvwr**.



Aperto l'**Event Viewer** (Visualizzatore di Eventi) sul pannello di sinistra si imposta **Windows Log** (Registri di Windows) e **Security** (Sicurezza)



All'accensione la Macchina Virtuale **FlareVM**, si presenta con migliaia di eventi in esecuzione, sul panello di destra **Actions** (Azioni) effettuo un click su **clear log..**(cancella registro..), e riavvio la macchina per avere una visione più dettagliata e pulita dei parametri che voglio cercare (**Logon** e **Logoff**)

[Clear Log...](#)

[Filter Current Log...](#)

Poiché il sistema è stato riavviato prendiamo in esame i **Logoff**.

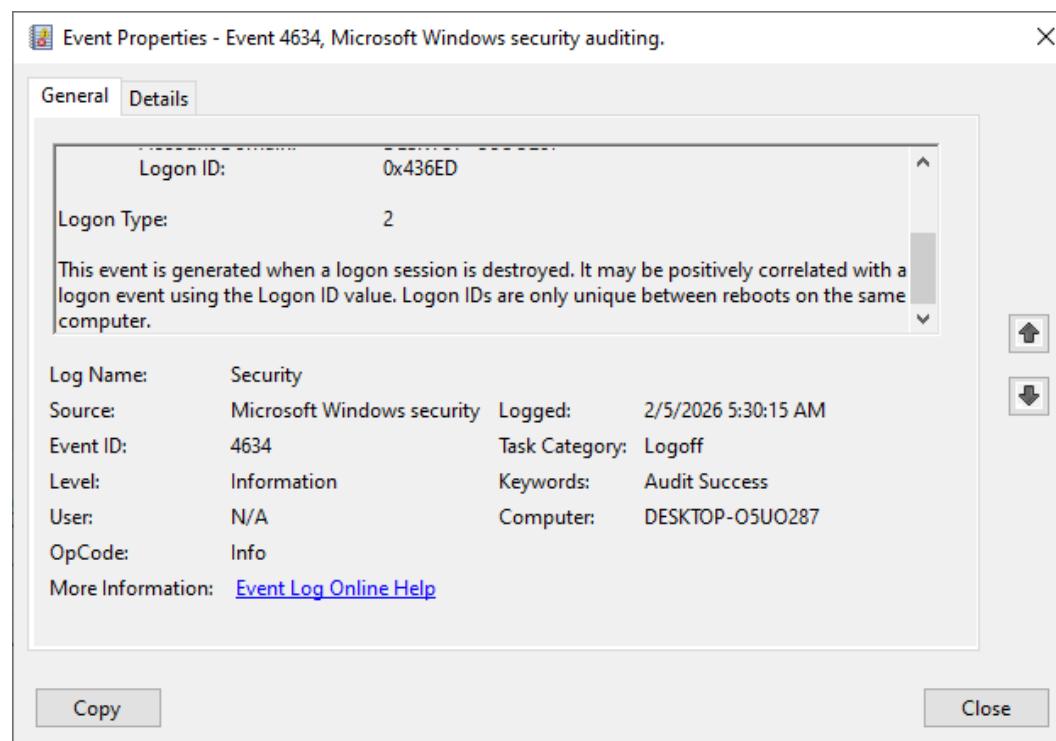
Audit Success	2/5/2026 5:29:41 AM	Microsoft Windows security auditing.	4647 Logoff
Audit Success	2/5/2026 5:30:15 AM	Microsoft Windows security auditing.	4634 Logoff
Audit Success	2/5/2026 5:30:15 AM	Microsoft Windows security auditing.	4634 Logoff

Il registro ci mostra cinque sezioni, **Audit Service**(Servizio di controllo),cioè il sistema che monitora e registra le attività, **data e ora** della registrazione, **Windows Security Auditing** (Controllo sicurezza di Windows) che si riferisce alla capacità del sistema operativo di tenere traccia delle attività, **Event ID**(ID evento), caratterizzato dai numeri e **Task Category**(Categoria attività), in questo caso **Logoff**.

L'**Event ID** si compone di due tipologie: **4634** e **4647**.

Event ID 4634 sono le interazioni dell'**Utente**. Con il tasto destro del Mouse si apre la finestra **Event Properties** (Proprietà dell'evento) e si cerca il tipo di evento o **Logon Type** associato a questo **ID**.

Qui **Logon Type** è **2** (Interazione Utente)



L'Event ID 4647 invece si riferisce all'**interazione del Sistema Operativo** che effettua il riavvio della macchina

Per l'evento di **Logon**, ci sono più registrazioni. Vengono registrati non solo le interazioni dell'**Utente** ma di tutti i **Servizi** in attivazione quando la macchina si avvia.

Gli Event ID per il Logon sono quindi: **4624, 4625**

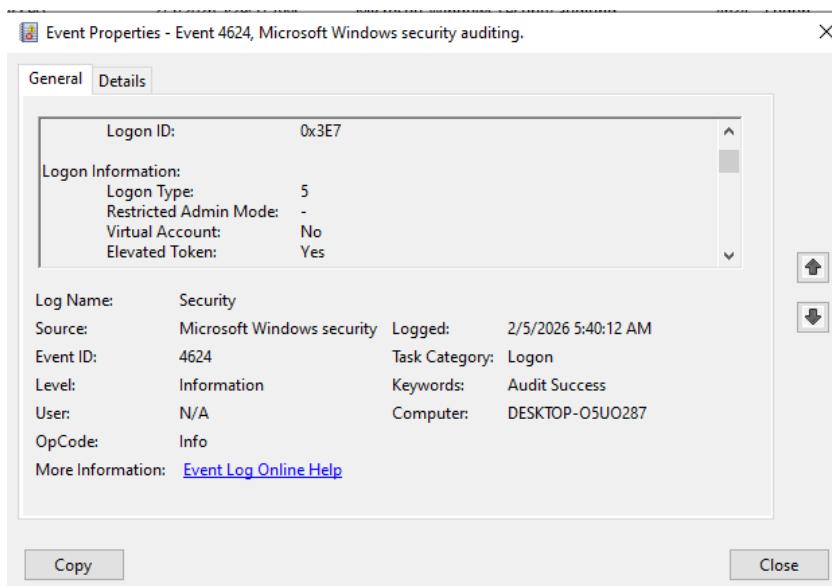
The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: Application, Security, System, Forwarded Events, Subscriptions, and Applications and Services. The main pane is titled 'Security' and shows 'Number of events: 193'. A filter bar at the top indicates 'Filtered Log: Security; Source: ; Event ID: 4624,4625. Number of events: 59'. The list of events includes various audit types like Audit Success, Audit Failure, and Audit Logon, all under the Microsoft Windows security auditing source and categorized as Logon. The right pane contains an 'Actions' menu with options such as Open Saved Log..., Create Custom View..., Import Custom View..., Clear Log..., Filter Current Log..., Find..., Properties, Save Filtered Log File As..., Attach a Task To This Log..., Save Filter to Custom View..., View, Refresh, Copy, and Help. A specific event entry for 'Event 4624, Microsoft Windows security auditing' is highlighted in the list.

Event ID 4624, analizzati, si dividono in **Logon Type 2(Utente)** e **5(Servizi)**

The screenshot shows the 'Event Properties - Event 4634, Microsoft Windows security auditing.' dialog. The 'General' tab is selected. Key details shown include:

- Logon ID: 0x436ED
- Logon Type: 2
- Source: Microsoft Windows security
- Event ID: 4634
- Task Category: Logoff
- Level: Information
- Keywords: Audit Success
- User: N/A
- Computer: DESKTOP-O5UO287
- OpCode: Info
- More Information: [Event Log Online Help](#)

At the bottom of the dialog are 'Copy' and 'Close' buttons.



L'Event ID 4625 è stato un tentativo fallito di accesso (password errata)



Quindi abbiamo **Audit Failure** con l'immagine del lucchetto.

Security Number of events: 193				
Filtered: Log: Security; Source: ; Event ID: 4625. Number of events: 1				
Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	2/5/2026 5:30:10 AM	Microsoft Windows security auditing.	4625	Logon

Nell'**Event Properties**(Proprietà Evento) abbiamo **Logon Type 2(Utente)** e a seguire la spiegazione **Failure Reason** che indica che l'user name sconosciuto o password sbagliata.

Failure Reason:	Unknown user name or bad password.
Status:	0xC000006D
Sub Status:	0xC000006A

Ora, come già accennato in precedenza, vengono registrate migliaia di eventi, Conoscendo gli **ID** degli **Eventi** si possono filtrare nella sezione **Actions(Azioni)** e **Filter Current Log(Filtro registro corrente)** inserendo i numeri dell'**ID** da analizzare

