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

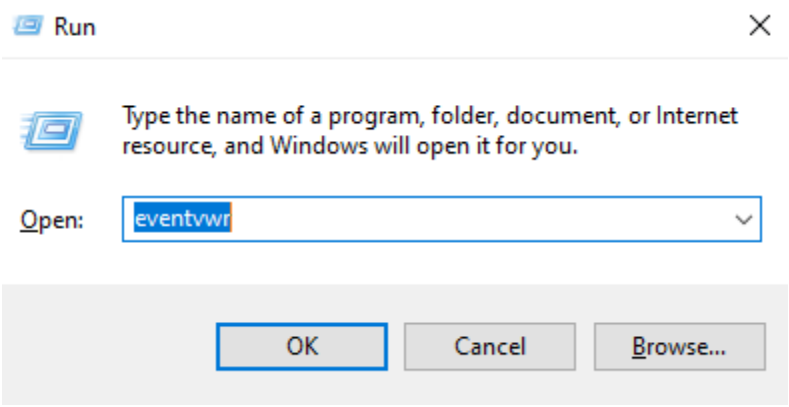
PREFAZIONE

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**.

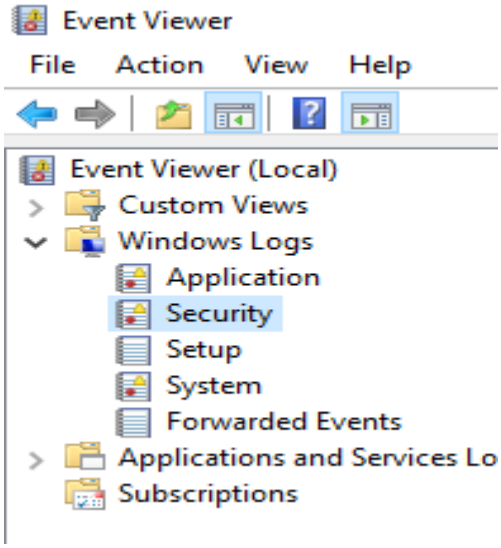
Entrambi i **Log** sono caratterizzati dalla loro tipologia (**Logon Type**).
Verranno presi in esame i **Logon Type 2** (Interazione dell'**Utente**) e i **Logon Type 5** (Interazione dei **Servizi**)

ESECUZIONE

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

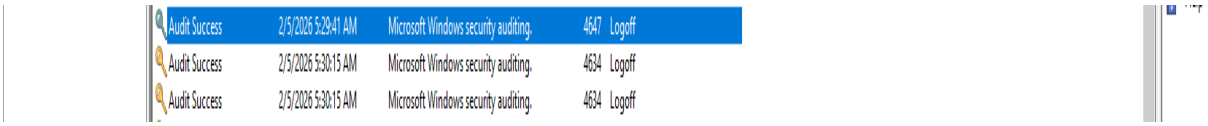


Aperto l'**Event Viewer** (Visualizzatore di Eventi) sul pannello di sinistra si imposta **Windows Log** (Registri di Windows) e **Security** (Sicurezza)



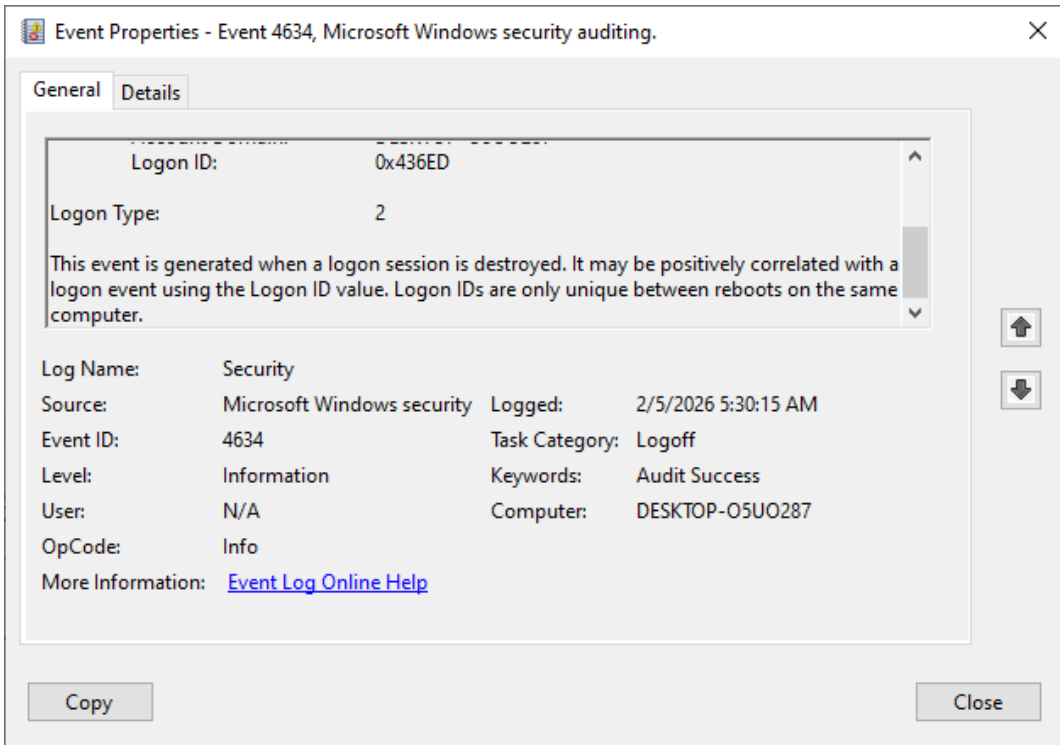
All'accensione la Macchina Virtuale **FlareVM**, si presenta con migliaia di eventi in esecuzione, sul panello di destra **Actions** (Azioni) effettuo un click su **clear log..(**cancella registro..), e riavvio la macchina per avere una visione più dettagliata e pulita dei parametri che voglio cercare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

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

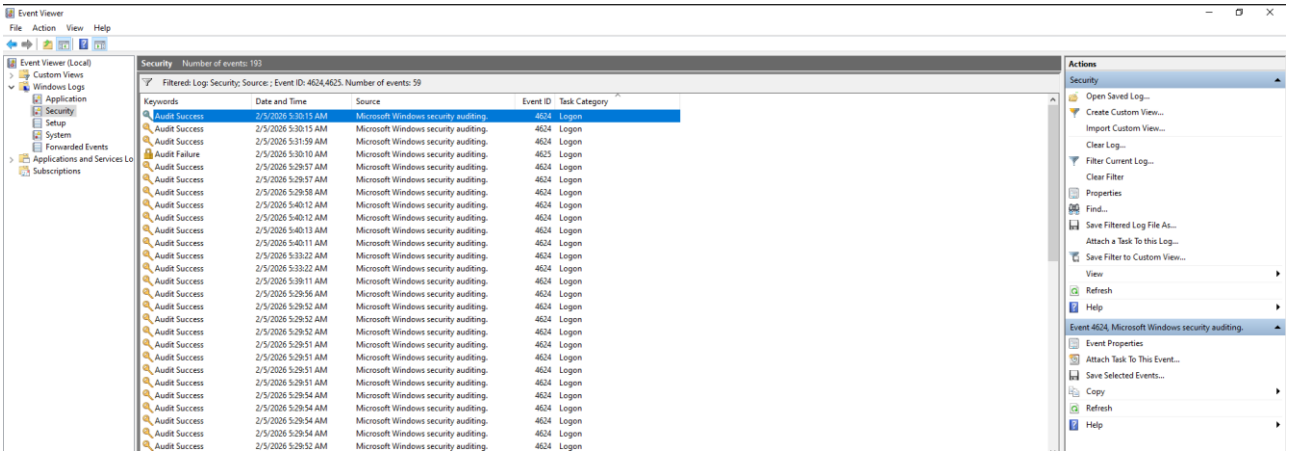
L'**Event ID** si compone di due tipologie**: 4634** e **4647**.
Event ID 4634 sono le interazioni dell'**Utente**. Con il tasto destro del Mouse si apre la finestra **Event Proprieties** (Proprietà dell'evento) e si cerca il tipo di evento o **Logon Type** associato a questo **ID**.
Qui **Logon Type è 2** (Interazione **Utente**)



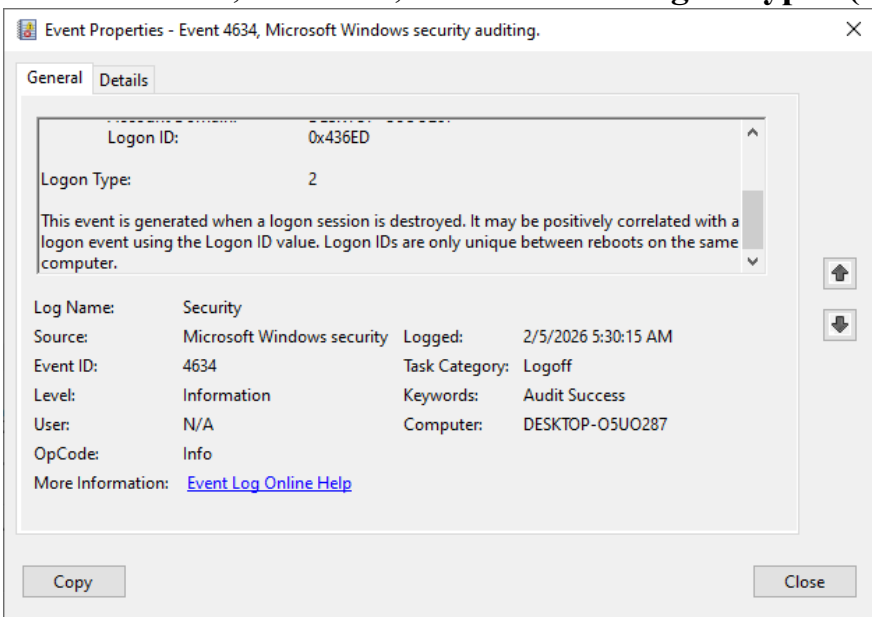
L'Event ID 4647 invece si riferisce **all'interazione del Sistema Operativo** che effettua il riavvio della macchina

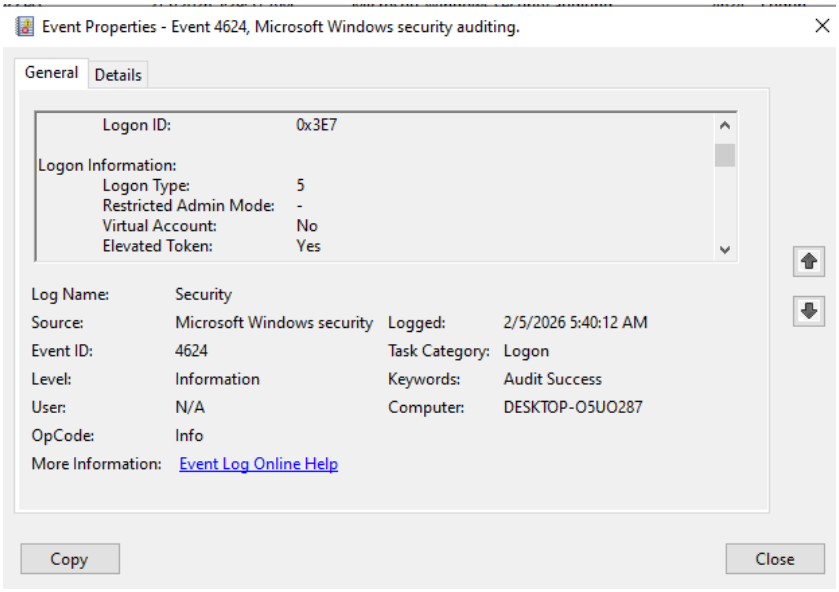
Per l'evento di **Logon,** ci sono più registrazioni. Vengono registrati non solo le interazioni dell'**Utente** ma di tutti i **Servizi** in attivazione quando la macchina si avvia.

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

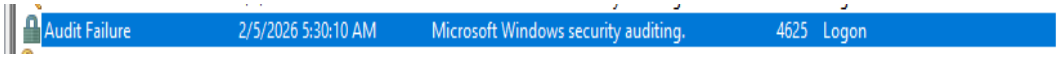


Event ID 4624, analizzati, si dividono in **Logon Type 2(Utente) e 5(Servizi)**

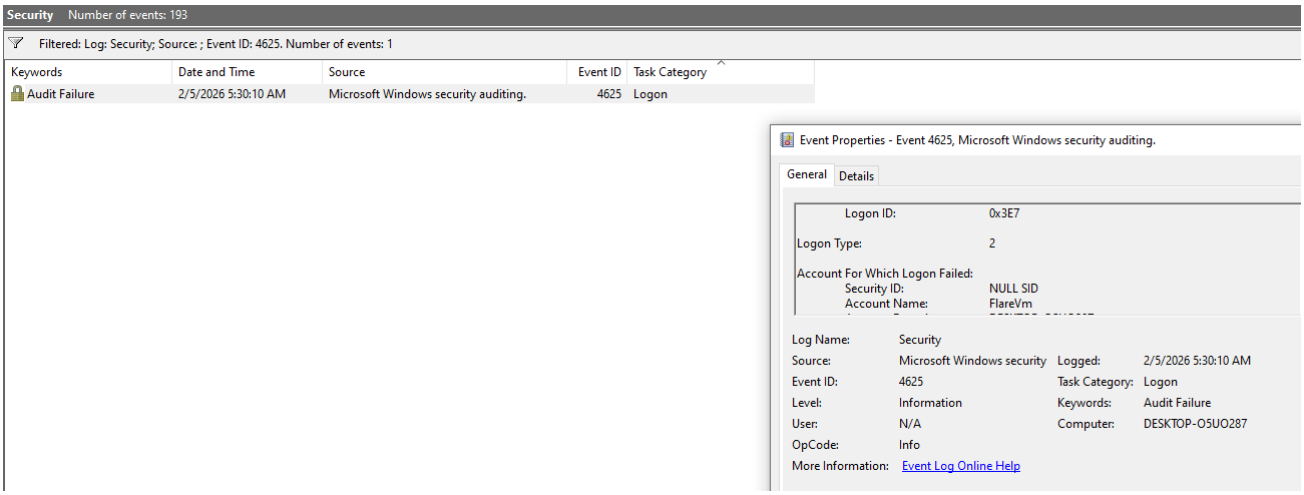




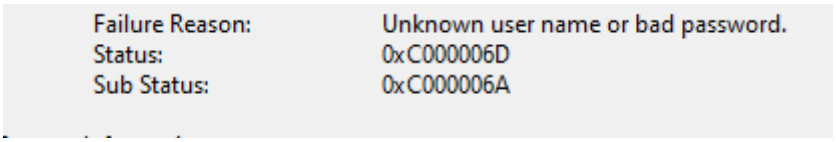
L'Event ID 4625 è stato un tentativo fallito di accesso (password errata)



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



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.



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