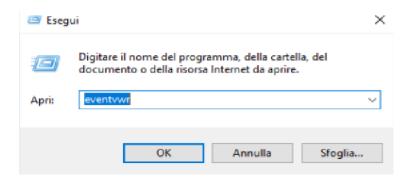
REPORT S9/L4

L' obbiettivo è quello di configurare e gestire i file di log della sicurezza utilizzando il visualizzatore eventi di windows.

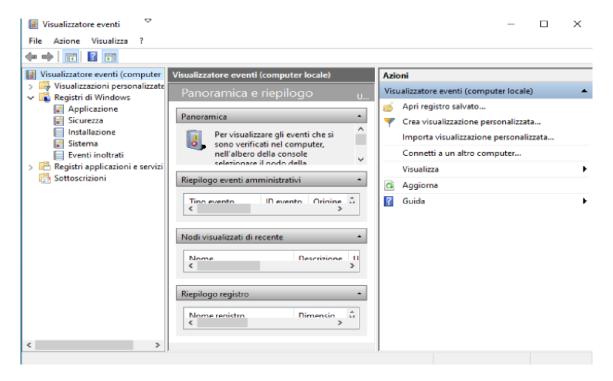
- 1. Accedere al visualizzatore eventi.
- 2. Configurare le Proprietà del Registro di Sicurezza.
- 3. Analizzare gli eventi con Categoria Attività Logon e Special Logon

REPORT S9/L4

Procedo per prima cosa aprendo il Visualizzatore eventi di Windows, **WIN + R** per aprire finestra "Esegui" e digito all' interno **eventvwr**.



Sulla sinistra vado poi ad espandere "Registri di Windows" e poi "Sicurezza".



Vado quindi a selezionare gli eventi di **logon** e ne faccio un analisi manuale prendendo in esame qualche caso.

Prendo in esame uno di questi e faccio doppio click.

Token elevato:

Accesso di un account riuscito. Soggetto: ID sicurezza: SYSTEM Nome account: DESKTOP-V91KR58\$ Dominio account: WORKGROUP ID accesso: 0x3E7 Informazioni di accesso: 5 Tipo di accesso: Modalità amministrativa limitata:: -Credential Guard remoto: -Account virtuale: No

Da qui abbiamo una serie di inofmrazioni, l' *ID*, il *nome* dell' *account*, il *dominio* e il *tipo* di *accesso*.

In questo caso ho *tipo di accesso 5*, che sta a significare che si tratti di accesso ad un servizio.

Sì