

LABORATORIO 6 FEBBRAIO 2025 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.

Istruzioni:

1: Accedere al Visualizzatore Eventi:

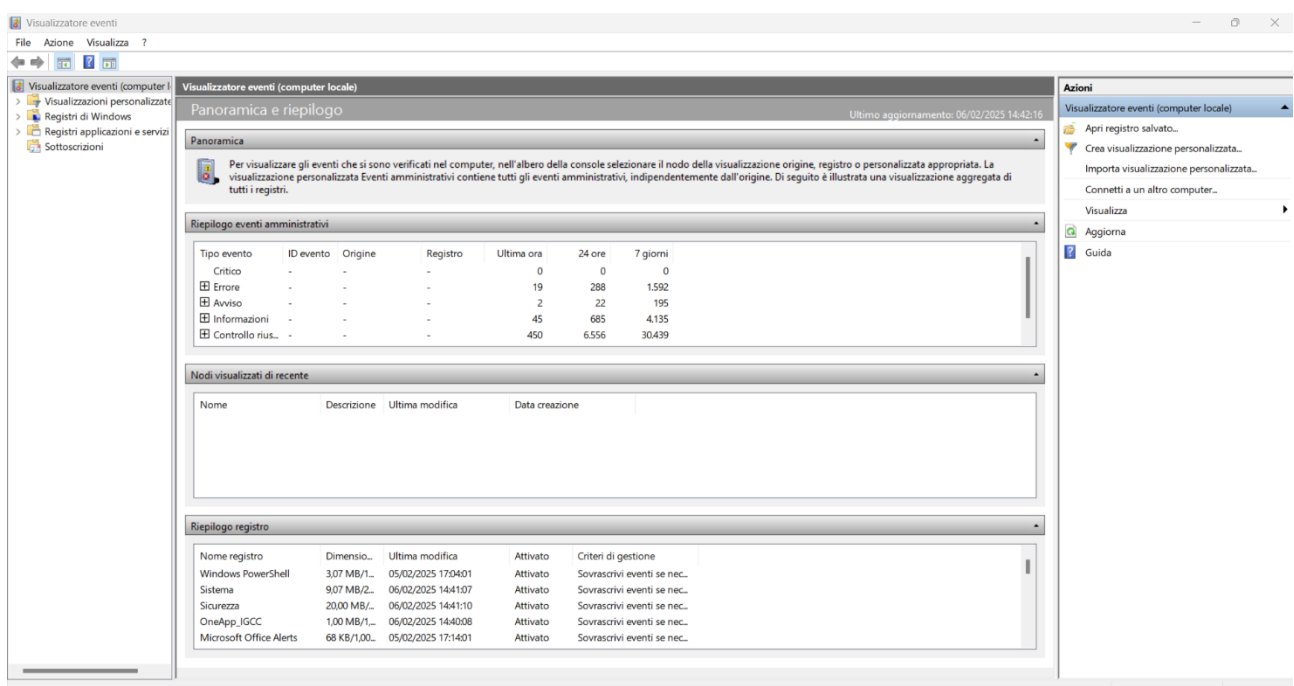
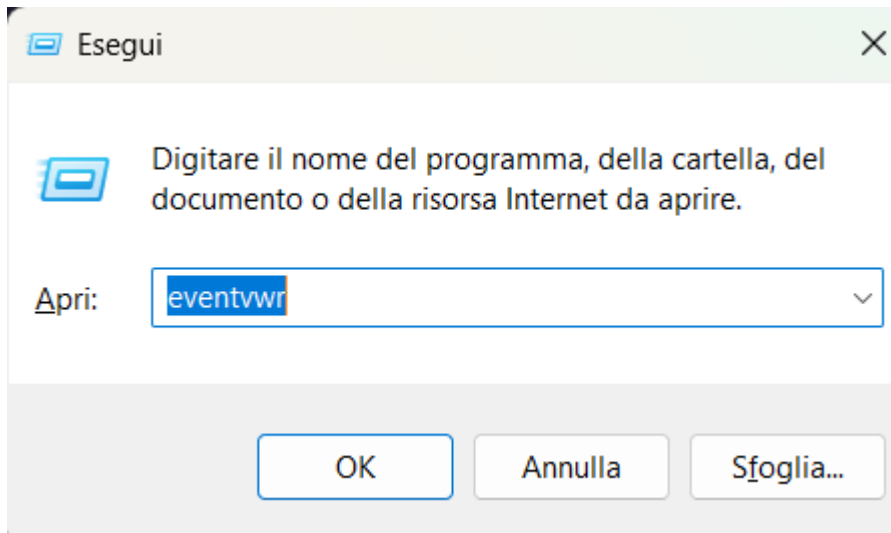
- Apri il Visualizzatore eventi premendo Win + R per aprire la finestra "Esegui".
- Digita eventvwr e premi Invio.

2: Configurare le Proprietà del Registro di Sicurezza:

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

3: Analizzare gli eventi con Categoria Attività Logon e Special Logon

Apriamo il visualizzatore Windows e apriamo la categoria **eventvwr**



Ci spostiamo nella categoria **registri di windows** e selezioniamo il campo **sicurezza**.



Filtriamo per categoria e troviamo i **Logon**.

Parole chiave	Data e ora	Origine	ID evento	Categoria attività
Controllo riuscito	06/02/2025 12:16:04	Microsoft Windows security au...	4624	Logon
Controllo riuscito	06/02/2025 12:14:04	Microsoft Windows security au...	4624	Logon
Controllo riuscito	06/02/2025 12:14:03	Microsoft Windows security au...	4624	Logon
Controllo riuscito	06/02/2025 12:21:07	Microsoft Windows security au...	4624	Logon
Controllo riuscito	06/02/2025 12:20:30	Microsoft Windows security au...	4624	Logon
Controllo riuscito	06/02/2025 12:19:31	Microsoft Windows security au...	4624	Logon
Controllo riuscito	06/02/2025 12:10:22	Microsoft Windows security au...	4624	Logon
Controllo riuscito	06/02/2025 11:58:20	Microsoft Windows security au...	4624	Logon
Controllo riuscito	06/02/2025 08:47:04	Microsoft Windows security au...	4624	Logon
Controllo riuscito	06/02/2025 09:09:32	Microsoft Windows security au...	4624	Logon
Controllo riuscito	06/02/2025 12:09:51	Microsoft Windows security au...	4624	Logon
Controllo riuscito	06/02/2025 12:09:44	Microsoft Windows security au...	4624	Logon
Controllo riuscito	06/02/2025 12:02:17	Microsoft Windows security au...	4624	Logon
Controllo riuscito	06/02/2025 09:13:04	Microsoft Windows security au...	4624	Logon
Controllo riuscito	06/02/2025 08:56:51	Microsoft Windows security au...	4624	Logon
Controllo riuscito	06/02/2025 08:56:21	Microsoft Windows security au...	4624	Logon
Controllo riuscito	06/02/2025 08:55:26	Microsoft Windows security au...	4624	Logon
Controllo riuscito	06/02/2025 08:56:21	Microsoft Windows security au...	4624	Logon

Possiamo vedere che ce ne sono numerosi e che l'ID evento è sempre lo stesso ovvero **4624**. Nel dettaglio possiamo leggere che si tratta di **accesso di un account riuscito**, l'orario del processo, il nome di quest'ultimo ed altre informazioni sul dispositivo e l'utente.

Evento 4624, Microsoft Windows security auditing.

Generale Dettagli

Accesso di un account riuscito.

Soggetto:
ID sicurezza: SYSTEM

Nome registro: Sicurezza

Origine: Microsoft Windows security : Registrato: 06/02/2025 12:16:04

ID evento: 4624 Categoria attività: Logon

Livello: Informazioni Parole chiave: Controllo riuscito

Utente: N/D Computer: LAPTOP-2JMTUOB7

Opcode: Informazioni

Generale Dettagli

☒ Semplice ☐ XML

+ System

- EventData

 SubjectUserSid S-1-5-18

 SubjectUserName LAPTOP-2JMTUOB7\$

 SubjectDomainName WORKGROUP

 SubjectLogonId 0x3e7

 TargetUserSid S-1-5-18

 TargetUserName SYSTEM

 TargetDomainName NT AUTHORITY

 TargetLogonId 0x3e7

 LogonType 5

 LogonProcessName Advapi

 AuthenticationPackageName Negotiate

 WorkstationName -

 LogonGuid {00000000-0000-0000-0000-000000000000}

 TransmittedServices -

Questo evento viene generato quando viene creata una sessione di accesso. Viene generato nel computer in cui è stato effettuato l'accesso.

Il campo Soggetto indica l'account nel sistema locale che ha richiesto l'accesso. Generalmente si tratta di un servizio, quale il servizio Server, o di un processo locale, ad esempio Winlogon.exe o Services.exe.

Il campo Tipo di accesso indica il tipo di accesso che è stato effettuato. I tipi più comuni sono 2 (interattivo) e 3 (rete).

Il campo Nuovo accesso indica l'account per il quale è stato creato il nuovo accesso, vale a dire l'account che ha effettuato l'accesso.


Ti campi Informazioni di rete indicano l'origine della richiesta di accesso remoto. Il nome della workstation non è sempre disponibile e può essere vuoto in alcuni casi.

Il campo del livello di rappresentazione indica la portata della rappresentazione consentita a un processo nella sessione di accesso.

Il campo Informazioni di autenticazione fornisce informazioni dettagliate sulla specifica richiesta di accesso.

- GUID accesso è un identificatore univoco che può essere utilizzato per correlare questo evento a un evento KDC.
- Servizi transitati indica quali servizi intermedi hanno partecipato alla richiesta di accesso.
- Nome pacchetto indica quale sottoprotocollo dei protocolli NTLM è stato utilizzato.
- Lunghezza chiave indica la lunghezza della chiave di sessione generata. Se non è stata richiesta alcuna chiave di sessione, la lunghezza sarà 0.

Ci sono delle eccezioni come in questo caso. Abbiamo trovato un **controllo non riuscito** con codice **4625**.

 Controllo non riuscito 06/02/2025 10:26:47 Microsoft Windows security au... 4625 Logon

Questo evento viene generato quando una richiesta di accesso non ha esito positivo. Viene generato nel computer in cui è stato tentato l'accesso.

Per quanto riguarda la categoria attività **special logon** troviamo sempre numerosi processi, tutti con il codice ID evento **4672**.

Si tratta di privilegi speciali assegnati ad un nuovo accesso.

Anche in questo caso possiamo osservare varie informazioni come data e ora, dispositivo, privilegi ed altro.

Parole chiave	Data e ora	Origine	ID evento	Categoria attività
Controllo riuscito	06/02/2025 12:09:51	Microsoft Windows security au...	4672	Special Logon
Controllo riuscito	06/02/2025 10:24:44	Microsoft Windows security au...	4672	Special Logon
Controllo riuscito	06/02/2025 11:55:27	Microsoft Windows security au...	4672	Special Logon
Controllo riuscito	06/02/2025 09:53:27	Microsoft Windows security au...	4672	Special Logon
Controllo riuscito	06/02/2025 11:54:51	Microsoft Windows security au...	4672	Special Logon
Controllo riuscito	06/02/2025 10:25:32	Microsoft Windows security au...	4672	Special Logon
Controllo riuscito	06/02/2025 11:58:20	Microsoft Windows security au...	4672	Special Logon
Controllo riuscito	06/02/2025 12:09:44	Microsoft Windows security au...	4672	Special Logon
Controllo riuscito	06/02/2025 10:24:51	Microsoft Windows security au...	4672	Special Logon
Controllo riuscito	06/02/2025 10:25:31	Microsoft Windows security au...	4672	Special Logon
Controllo riuscito	06/02/2025 12:02:17	Microsoft Windows security au...	4672	Special Logon
Controllo riuscito	06/02/2025 10:13:02	Microsoft Windows security au...	4672	Special Logon
Controllo riuscito	06/02/2025 09:09:44	Microsoft Windows security au...	4672	Special Logon
Controllo riuscito	06/02/2025 09:54:11	Microsoft Windows security au...	4672	Special Logon
Controllo riuscito	06/02/2025 09:16:04	Microsoft Windows security au...	4672	Special Logon
Controllo riuscito	06/02/2025 09:09:51	Microsoft Windows security au...	4672	Special Logon
Controllo riuscito	06/02/2025 09:09:14	Microsoft Windows security au...	4672	Special Logon
Controllo riuscito	06/02/2025 09:01:07	Microsoft Windows securitv au...	4672	Special Logon

Evento 4672, Microsoft Windows security auditing.

Generale

Dettagli

Privilegi speciali assegnati a nuovo accesso.

Sogetto:

ID sicurezza:SYSTEM

Nome account:SYSTEM

Dominio account:NT AUTHORITY

ID accesso:0x3E7

Privilegi:

SeAssignPrimaryTokenPrivilege

SeTcbPrivilege

SeSecurityPrivilege

SeTakeOwnershipPrivilege

SeLoadDriverPrivilege

SeBackupPrivilege

SeRestorePrivilege

SeDebugPrivilege

SeAuditPrivilege

SeSystemEnvironmentPrivilege

Nome registro: Sicurezza

Origine:Microsoft Windows security ; Registrato:06/02/2025 12:09:51

ID evento:4672 Categoria attività:Special Logon

Livello:Informazioni Parole chiave:Controllo riuscito

Utente:N/D Computer:LAPTOP-2JMTUOB7

Opcode:Informazioni

