

S9 – L4

Titolo:

Analisi e configurazione dei log di sicurezza su Windows

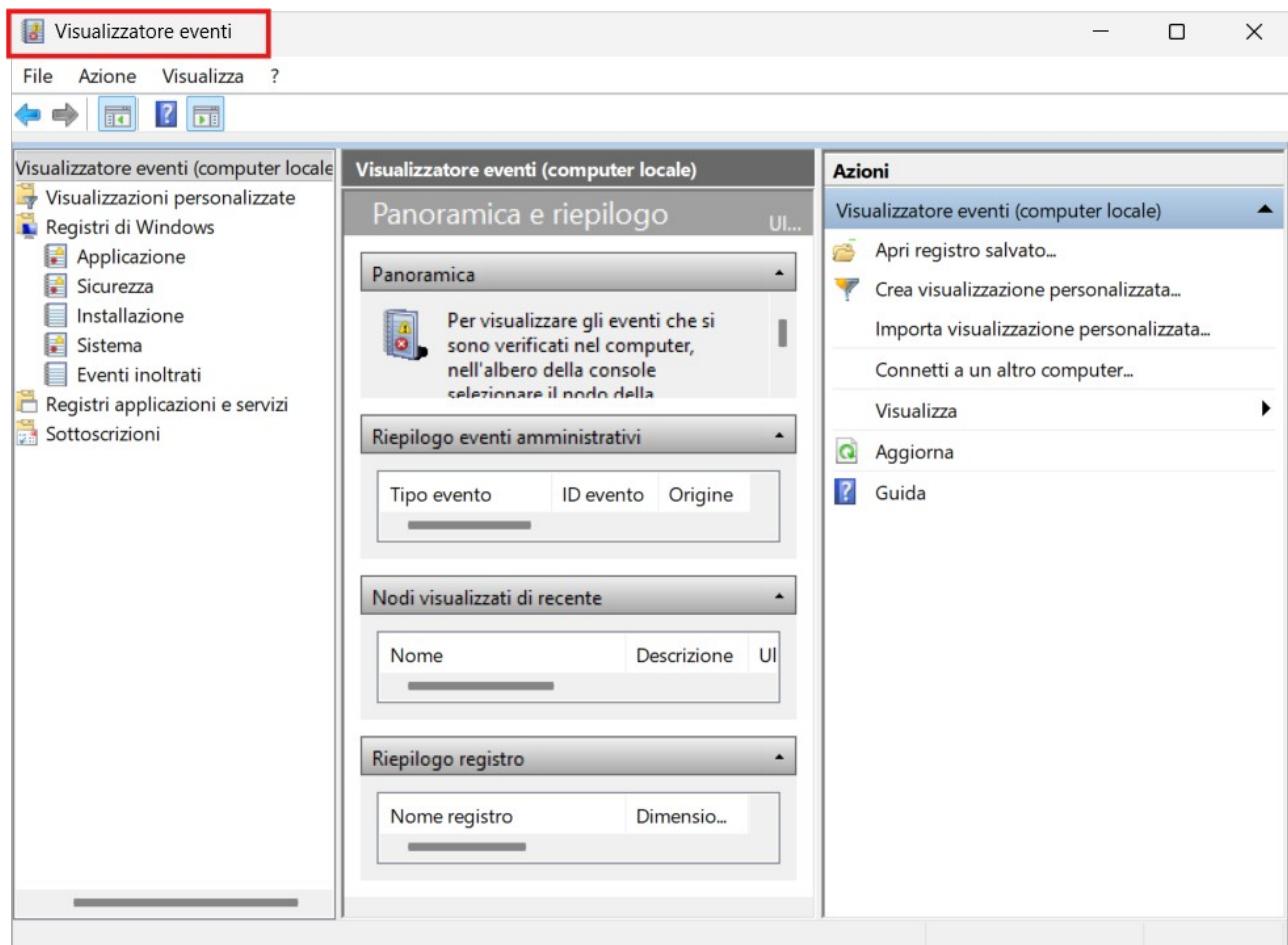
Introduzione:

Configuro e analizzo i **log di sicurezza di Windows** utilizzando il **Visualizzatore eventi**, con l'obiettivo di verificare la corretta registrazione degli eventi di **Login e Logoff**. L'attività riproduce una fase fondamentale del monitoraggio della sicurezza, **utile per il rilevamento di accessi legittimi e tentativi di autenticazione falliti**.

Svolgimento dell'esercizio:

1) Apertura del Visualizzatore eventi

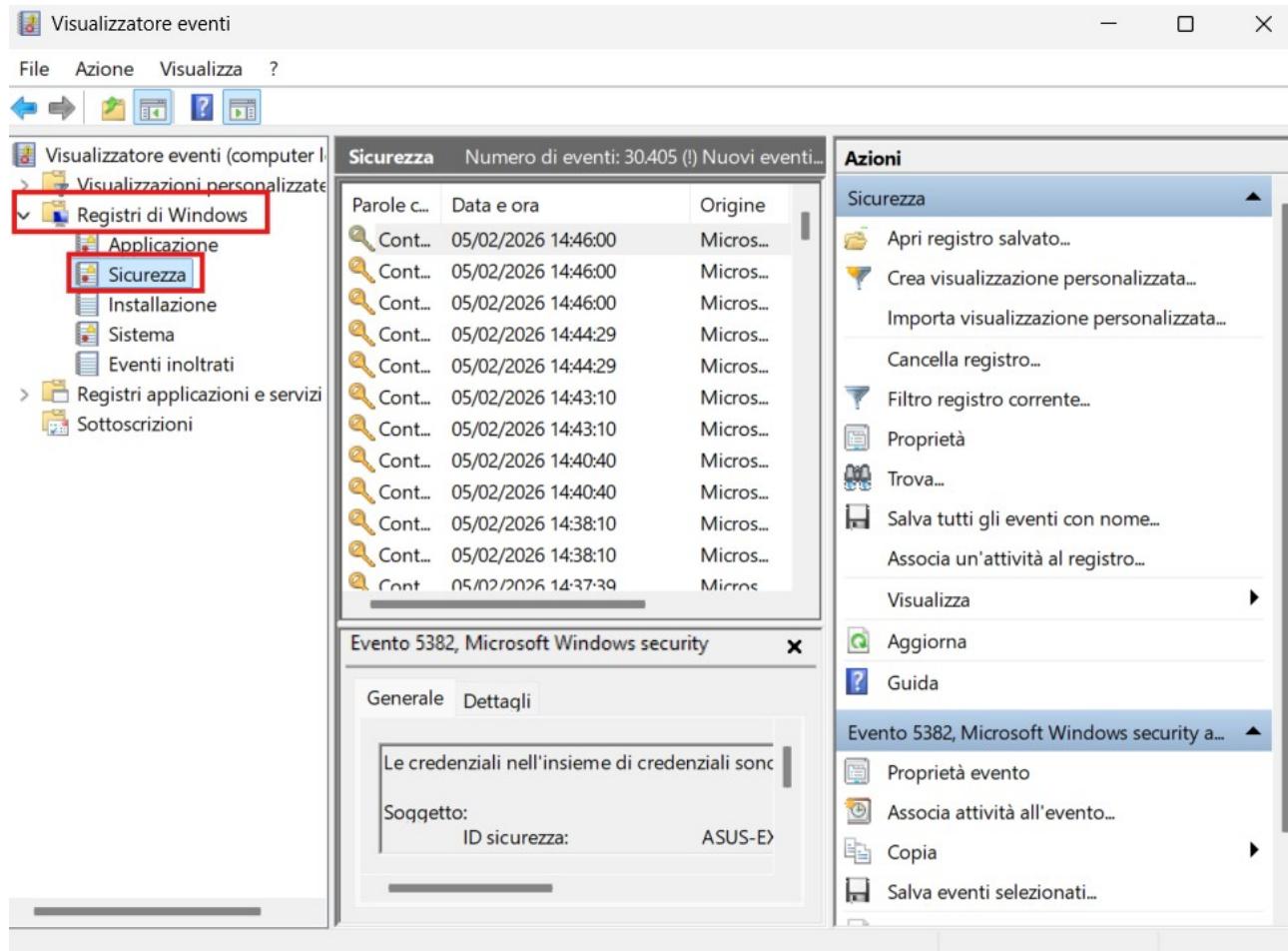
- Premo Win + R
- Digitò eventvwr
- Premo Invio



Il Visualizzatore eventi si apre correttamente.

2) Accesso al registro di Sicurezza

- Nel pannello sinistro **espando** **Registri di Windows**
- **Clicco su Sicurezza**



Visualizzo l'elenco degli eventi di sicurezza del sistema.

3) Configurazione delle proprietà del log Sicurezza

- **Clicco con il tasto destro** su Sicurezza
- **Seleziono Proprietà**
- **Imposto** una dimensione adeguata del log
- **Seleziono** l'opzione di gestione degli eventi (sovrascrittura/archiviazione)
- **Clicco su Applica** e poi su OK

Generale

Nome completo: Security
Percorso registro: %SystemRoot%\System32\Winevt\Logs\Security.evtx
Dimensione registro: 20,00 MB(20.975.616 byte)
Data creazione: mercoledì 19 febbraio 2025 00:17:10
Ultima modifica: giovedì 5 febbraio 2026 14:53:39
Ultimo accesso: giovedì 5 febbraio 2026 14:54:42

Abilita registrazione

Dimensione massima registro (KB):

Al raggiungimento della dimensione massima del registro eventi:

- Sovrascrivi eventi se necessario (dal più vecchio)
 Archivia il registro quando è pieno (non sovrascrivere gli eventi)
 Non sovrascrivere gli eventi (cancella i registri manualmente)

Cancella registro

OK

Annulla

Applica

Il log di sicurezza è ora correttamente configurato.

4) Abilitazione del logging di Login e Logoff

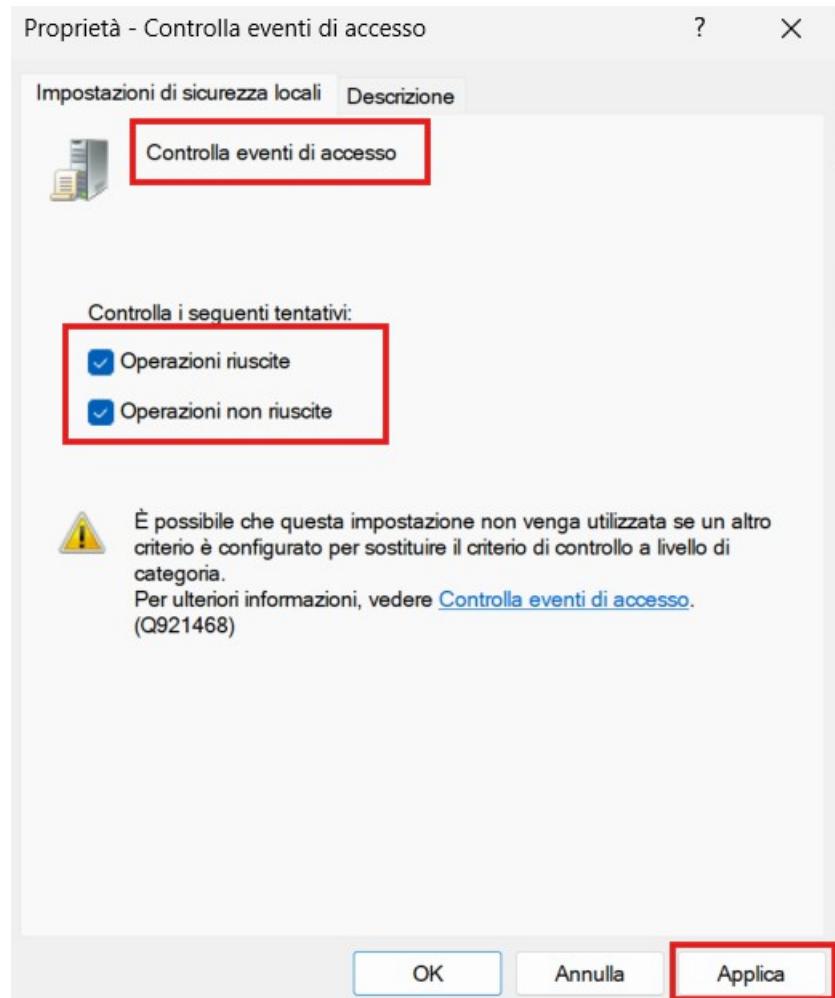
- Premo Win + R
- Digito secpol.msc
- Premo Invio

Nome	Descrizione
Criteri account	Criteri relativi alle password e al blocco degli acc...
Criteri locali	Criteri relativi alle opzioni di sicurezza, ai diritti u...
Windows Defender Firewall con sicurezza ...	Windows Defender Firewall con sicurezza avanz...
Criteri Gestione elenco reti	Criteri di gruppo per il nome, l'icona e il percors...
Criteri chiave pubblica	
Criteri restrizione software	
Criteri di controllo delle applicazioni	Criteri di controllo delle applicazioni
Criteri di sicurezza IP su Computer locale	Amministrazione sicurezza protocollo Internet (I...
Configurazione avanzata dei criteri di...	Configurazione avanzata dei criteri di controllo

Dal pannello:

- **Clicco su Criteri locali → Criteri di controllo**
- **Apro Controlla eventi di accesso (Audit logon events)**
- **Seleziono Successo e Errore**
- **Applico le modifiche**

Criterio	Impostazione di sicurezza
Controlla accesso agli oggetti	Nessun controllo
Controlla accesso al servizio directory	Nessun controllo
Controlla eventi accesso account	Nessun controllo
Controlla eventi di accesso	Nessun controllo
Controlla eventi di sistema	Nessun controllo
Controlla gestione degli account	Nessun controllo
Controlla modifica ai criteri	Nessun controllo
Controlla tracciato processo	Nessun controllo
Controlla uso dei privilegi	Nessun controllo



In questo modo abilito la registrazione degli eventi di accesso riusciti e falliti.

5) Generazione di eventi di test

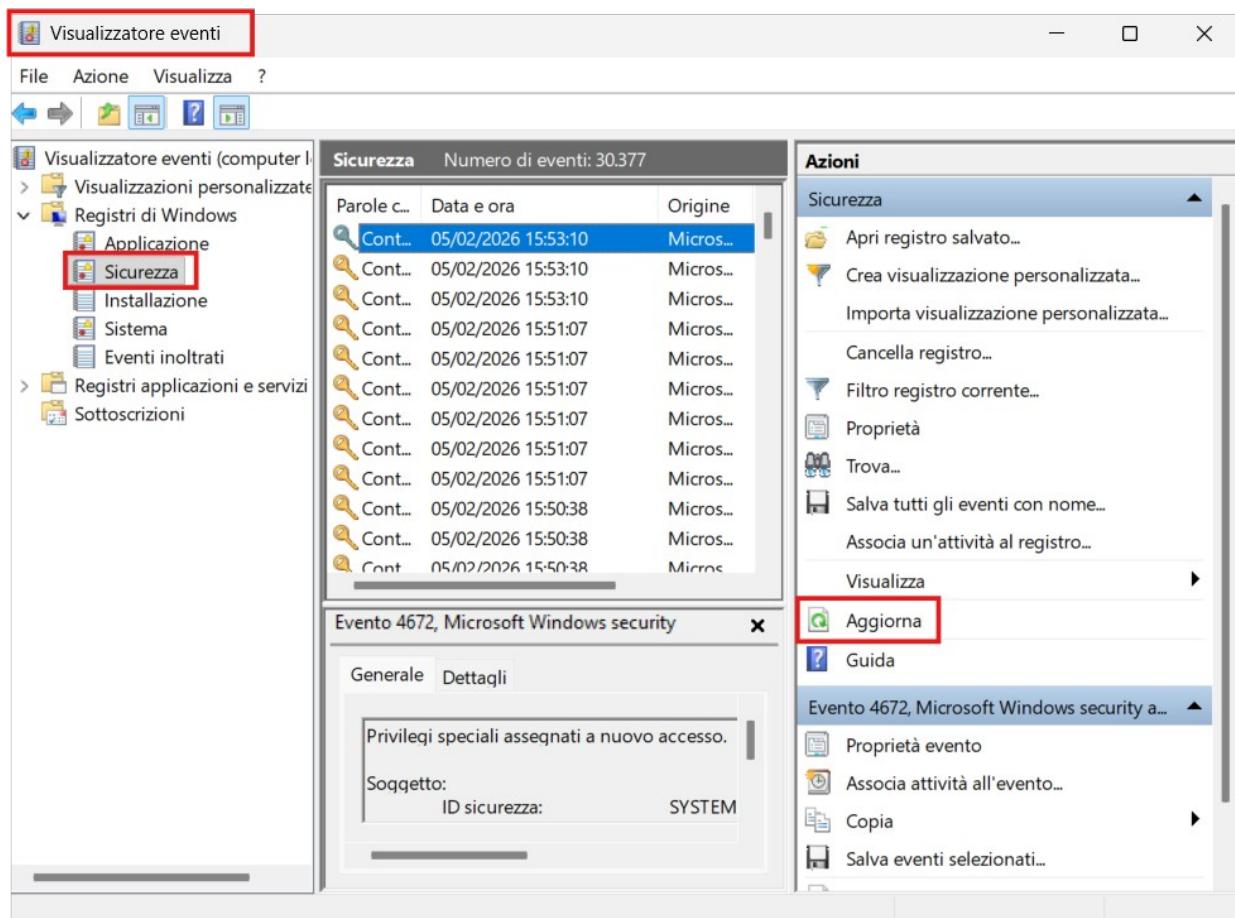
- **Blocco** il computer con Win + L
- **Eseguo** un login corretto
- **Eseguo** un tentativo di login errato
- (facoltativo) **Eseguo** il logoff dell'utente

Genero così eventi reali da analizzare

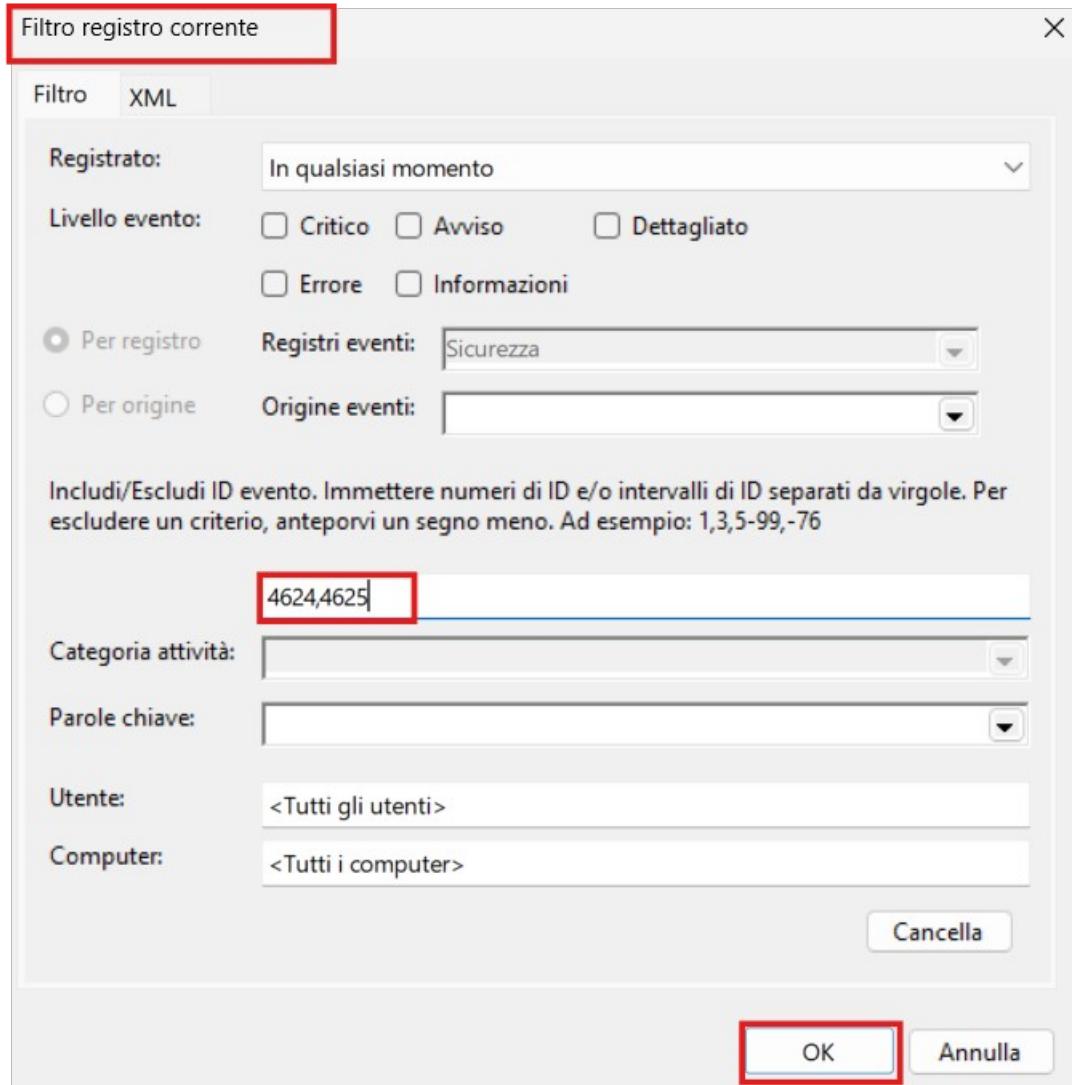
Screenshot non disponibile per combinazione di tasti non possibile in schermata di login

6) Verifica degli eventi nel registro Sicurezza

- **Torno** nel Visualizzatore eventi
- **Clicco** su **Sicurezza**
- **Aggiorno** il registro



- **Filtro** gli eventi per ID: **4624,4625** (uno alla volta)



NB: si raccomanda di inserire gli ID evento **uno alla volta**, applicando il filtro separatamente per ciascun ID, al fine di evitare che il sistema non visualizzi correttamente tutti gli eventi richiesti quando vengono inseriti contemporaneamente.

- 4624 → accesso riuscito

The screenshot shows the Windows Event Viewer interface. The left pane displays navigation categories like 'Visualizzazioni personalizzate', 'Registri di Windows' (with 'Sicurezza' selected), and 'Registri applicazioni e servizi'. The main pane is titled 'Sicurezza' and shows a list of 30,490 events. A specific event is highlighted: 'Cont... 05/02/2026 15:28:10'. Below it, a details window is open for 'Evento 4624, Microsoft Windows security'. The 'Generale' tab is selected, showing the message 'Accesso di un account riuscito.' (Successful account access). The 'Soggetto' section lists 'ID sicurezza: SYSTEM', 'Nome account: ASUS-EXPERTBOOK\$', 'Dominio account: WORKGROUP', and 'ID accesso: 0x3E7'. The right pane contains an 'Azioni' (Actions) menu with options like 'Cancella registro...', 'Filtro registro corrente...', and 'Salva file di registro filtrato con nome...'. A scroll bar on the right indicates more content.

This screenshot shows the 'Proprietà evento - Evento 4624, Microsoft Windows security auditing' dialog box. The 'Generale' tab is active. The message 'Accesso di un account riuscito.' is displayed. The 'Soggetto' section shows the same information as the Event Viewer: 'ID sicurezza: SYSTEM', 'Nome account: ASUS-EXPERTBOOK\$', 'Dominio account: WORKGROUP', and 'ID accesso: 0x3E7'. Below this, the 'Informazioni di accesso' section is partially visible. At the bottom, event details are listed: 'Nome registro: Sicurezza', 'Origine: Microsoft Windows security', 'Registrato: 05/02/2026 15:33:10', 'ID evento: 4624', 'Categoria attività: Logon', 'Livello: Informazioni', 'Parole chiave: Controllo riuscito', 'Utente: N/D', 'Computer: Asus-ExpertBook', and 'Opcode: Informazioni'. The 'Registrato:' field is highlighted with a red box.

- 4625 → accesso fallito

Visualizzatore eventi

File Azione Visualizza ?

Visualizzatore eventi (computer locale)

- Visualizzazioni personalizzate
- Registri di Windows
 - Applicazione
 - Sicurezza**
 - Installazione
 - Sistema
 - Eventi inoltrati
- Registri applicazioni e servizi
- Sottoscrizioni

Sicurezza Numero di eventi: 30.407

Filtrati: Registro: Security; Origine: ; ID evento: 4625

Parole c...	Data e ora	Origine
Cont...	05/02/2026 15:27:19	Micros...
Cont...	05/02/2026 15:27:15	Micros...
Cont...	05/02/2026 15:07:24	Micros...
Cont...	05/02/2026 14:22:33	Micros...
Cont...	05/02/2026 08:51:13	Micros...
Cont...	04/02/2026 23:00:34	Micros...
Cont...	04/02/2026 09:02:16	Micros...
Cont...	03/02/2026 21:48:12	Micros...
Cont...	03/02/2026 16:26:41	Micros...
Cont...	03/02/2026 12:00:26	Micros...

Evento 4625, Microsoft Windows security

Generale Dettagli

Accesso di un account non riuscito.

Soggetto: ID sicurezza: SYSTEM Nome account: ASUS-EXPERTBOOK\$ Dominio account: WORKGROUP ID accesso: 0x3E7

Azioni

- Cancella registro...
- Filtro registro corrente...
- Cancella filtro
- Proprietà
- Trova...
- Salva file di registro filtrato con nome...
- Associa un'attività al registro...
- Salva filtro in una visualizzazione pers...
- Visualizza
- Aggiorna
- Guida

Proprietà evento - Evento 4625, Microsoft Windows security auditing.

Generale Dettagli

Accesso di un account non riuscito.

Soggetto:

ID sicurezza:	SYSTEM
Nome account:	ASUS-EXPERTBOOK\$
Dominio account:	WORKGROUP
ID accesso:	0x3E7

Tipo di accesso: ?

Nome registro: Sicurezza

Origine: Microsoft Windows security i Registrato: **05/02/2026 15:27:19**

ID evento: 4625 Categoria attività: Logon

Livello: Informazioni Parole chiave: Controllo non riuscito

Utente: N/D Computer: Asus-ExpertBook

Opcode: Informazioni

Ho verificato correttamente la presenza degli eventi generati.

Conclusioni ultime:

L'esercizio ha consentito di **configurare e verificare correttamente il registro di sicurezza di Windows**, assicurando la registrazione degli eventi di Login e Logoff.

Attraverso l'**analisi degli ID evento 4624 e 4625** è stato possibile confermare il corretto funzionamento del sistema di auditing locale, dimostrando come i log rappresentino uno strumento fondamentale per il monitoraggio degli accessi e per le attività di sicurezza e analisi degli incidenti.