REPORT S10/L5: GESTIONE UTENTI E GRUPPI

Studente: Vincenzo Zarola
Scenario: Cyber Warfare - "Zero Day Zone"

---

1. OBIETTIVO DELL'ESERCIZIO

In questo laboratorio ho simulato la gestione della sicurezza in un'azienda informatica divisa in due fazioni opposte. L'obiettivo era creare un ambiente sicuro dove ogni gruppo potesse accedere solo alle proprie risorse, applicando il principio del **Minimo Privilegio**.

Lo scenario si chiama **"Zero Day Zone"** e prevede due team:

- **White Hats (i buoni):** Esperti di sicurezza che difendono i sistemi.
- **Black Hats (i cattivi):** Hacker che cercano di attaccare i sistemi.

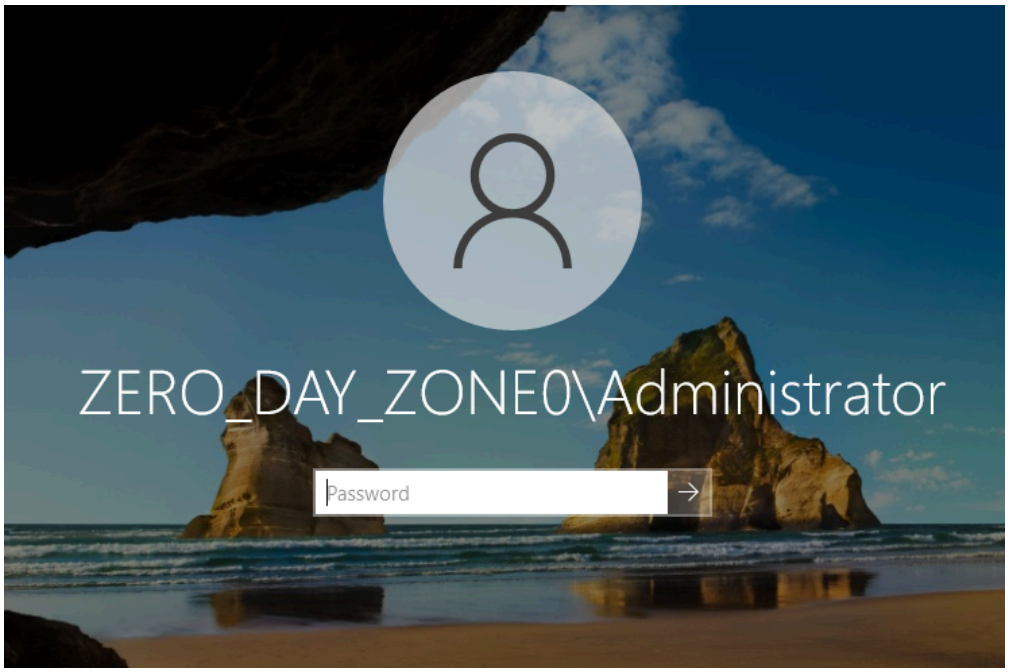
---

2. PREPARAZIONE DELL'AMBIENTE

Ho creato una rete virtuale composta da due macchine collegate tra loro:

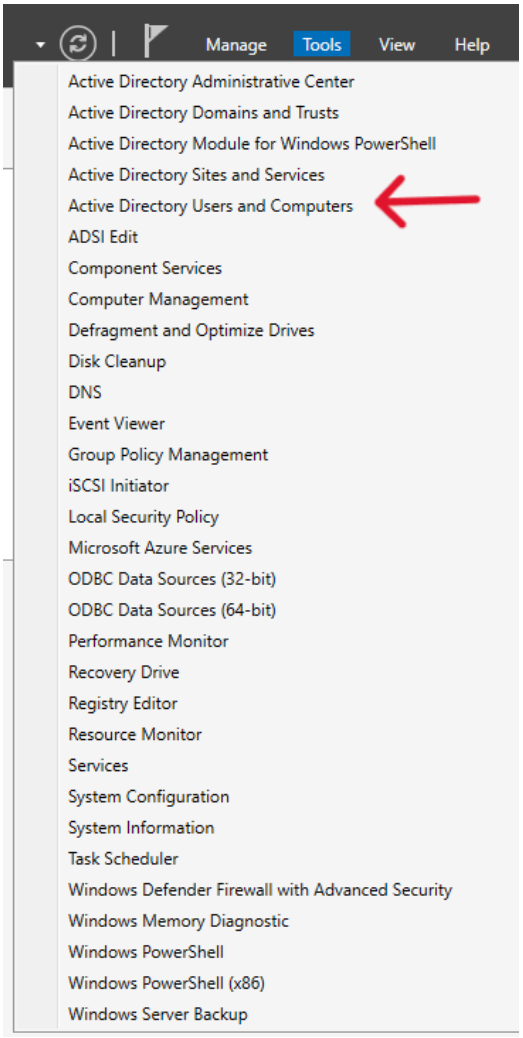
1. **Server:** Windows Server 2022 (il computer principale che gestisce tutto).
2. **Client:** Windows 10 Pro (il computer usato dagli utenti per lavorare).

Ho configurato entrambe le macchine con indirizzi IP statici per farle comunicare correttamente. Successivamente ho impostato il server e ho effettuato l’accesso come amministratore.



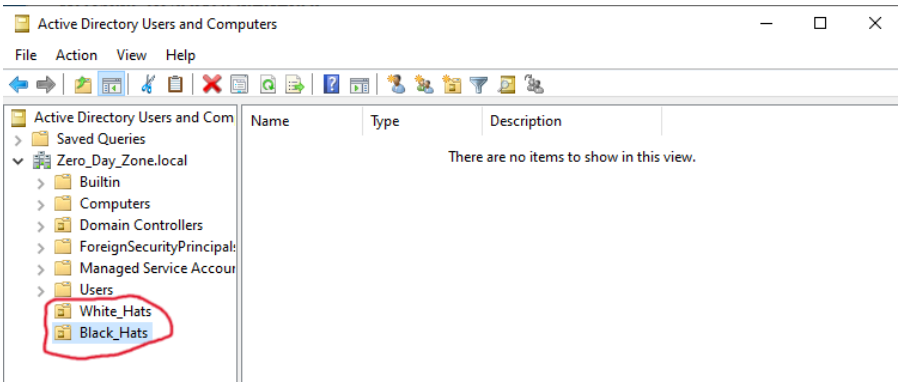
3. CREAZIONE DELLA STRUTTURA (Organizzazione)

Per prima cosa, ho aperto lo strumento di gestione degli utenti sul server (**Active Directory Users and Computers**).



Ho creato due "contenitori" (chiamati **Organizational Units**) per tenere separati i due team:

1. **White_Hats**
2. **Black_Hats**



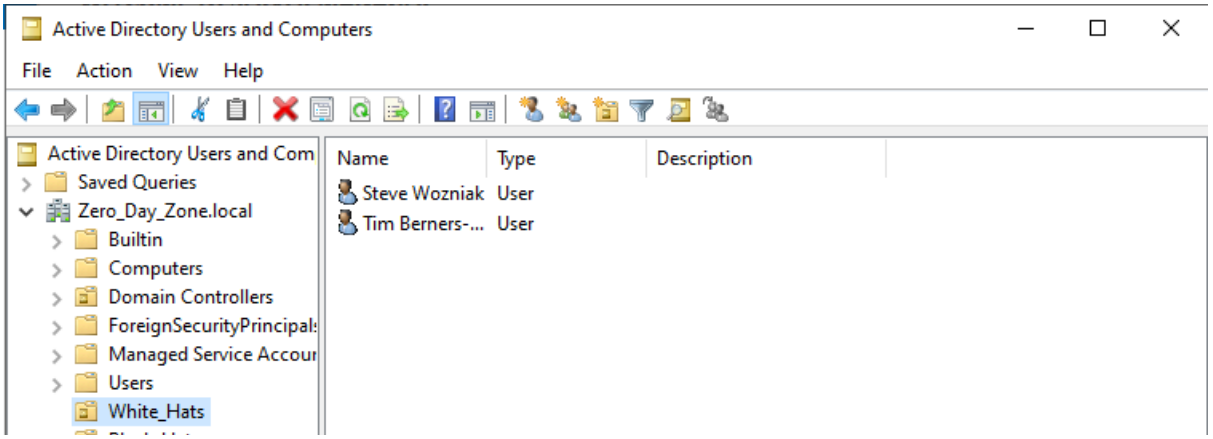
4. CREAZIONE DEGLI UTENTI E DEI GRUPPI

Successivamente, ho creato gli utenti reali e li ho assegnati ai rispettivi gruppi di lavoro.

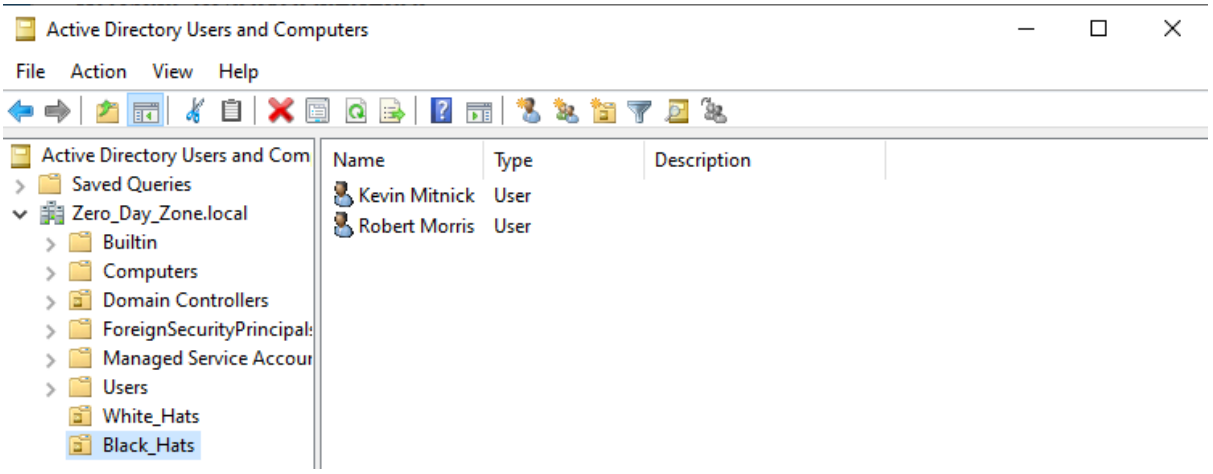
A. Utenti Creati

Ho scelto nomi di personaggi famosi nella storia dell'informatica per rendere lo scenario realistico:

- Nei **White Hats** ho creato: **Steve Wozniak** e **Tim Berners-Lee**.



- Nei **Black Hats** ho creato: **Kevin Mitnick** e **Robert Morris**.



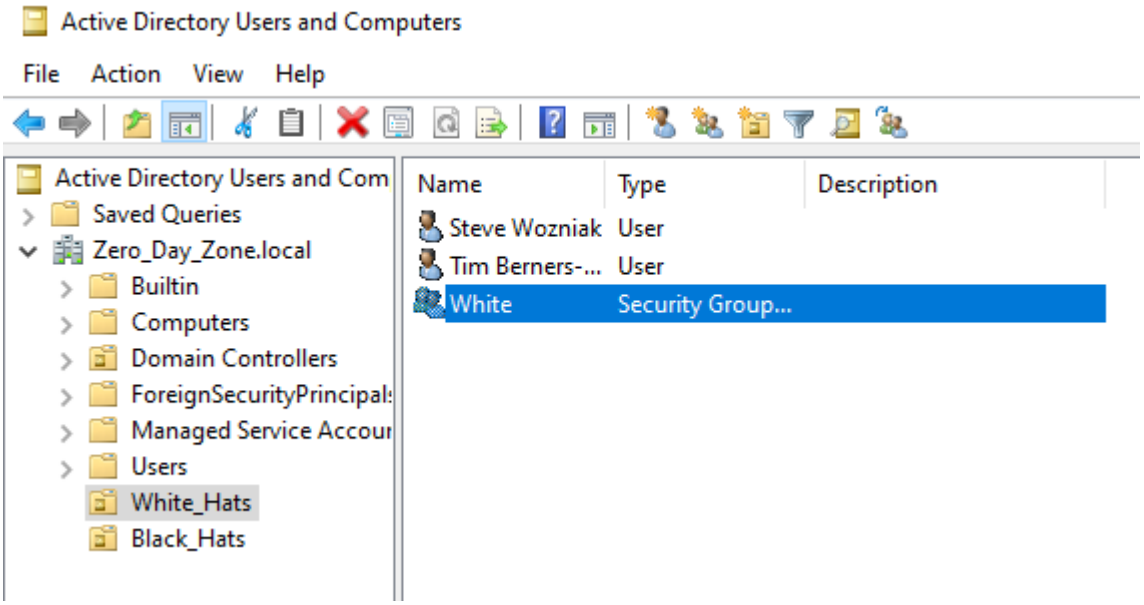
:

B. Gruppi di Sicurezza

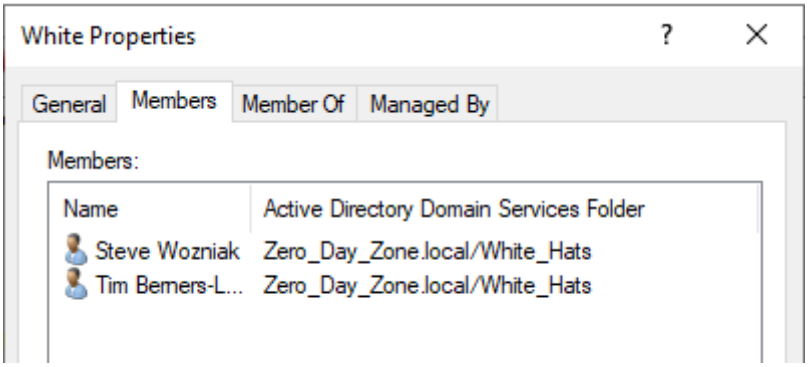
Per gestire i permessi in modo ordinato, ho creato due gruppi:

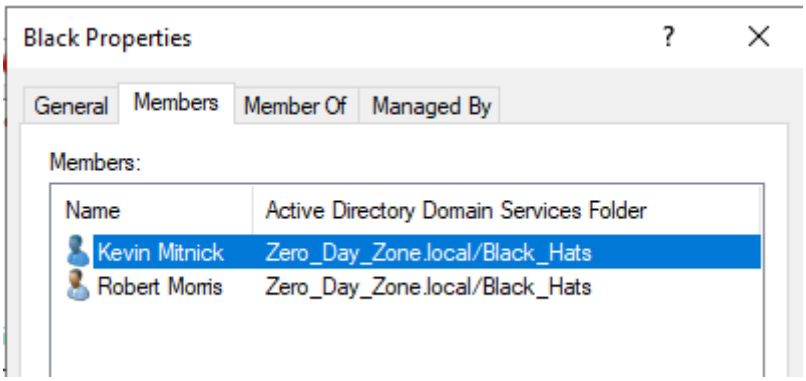
1. Gruppo **White** (per i White Hats).

2. Gruppo **Black** (per i Black Hats).



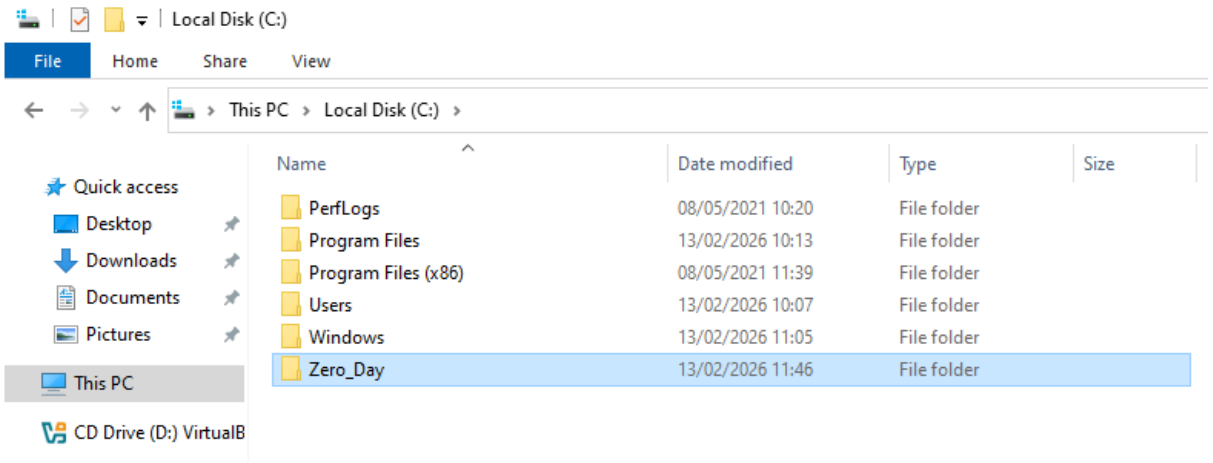
Ho poi inserito gli utenti nei rispettivi gruppi.

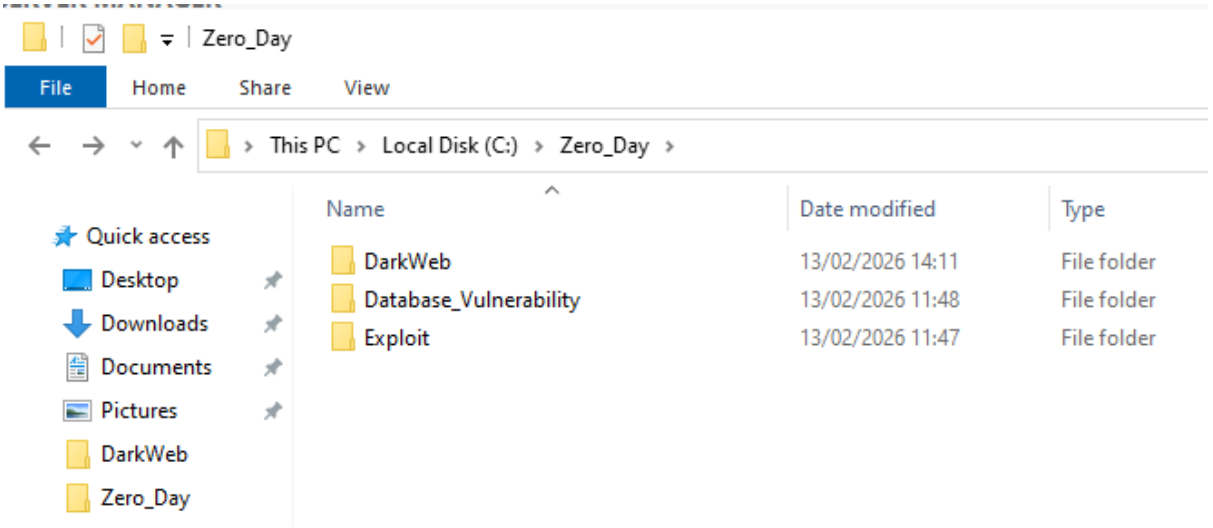




5. GESTIONE DELLE CARTELLE E DEI PERMESSI

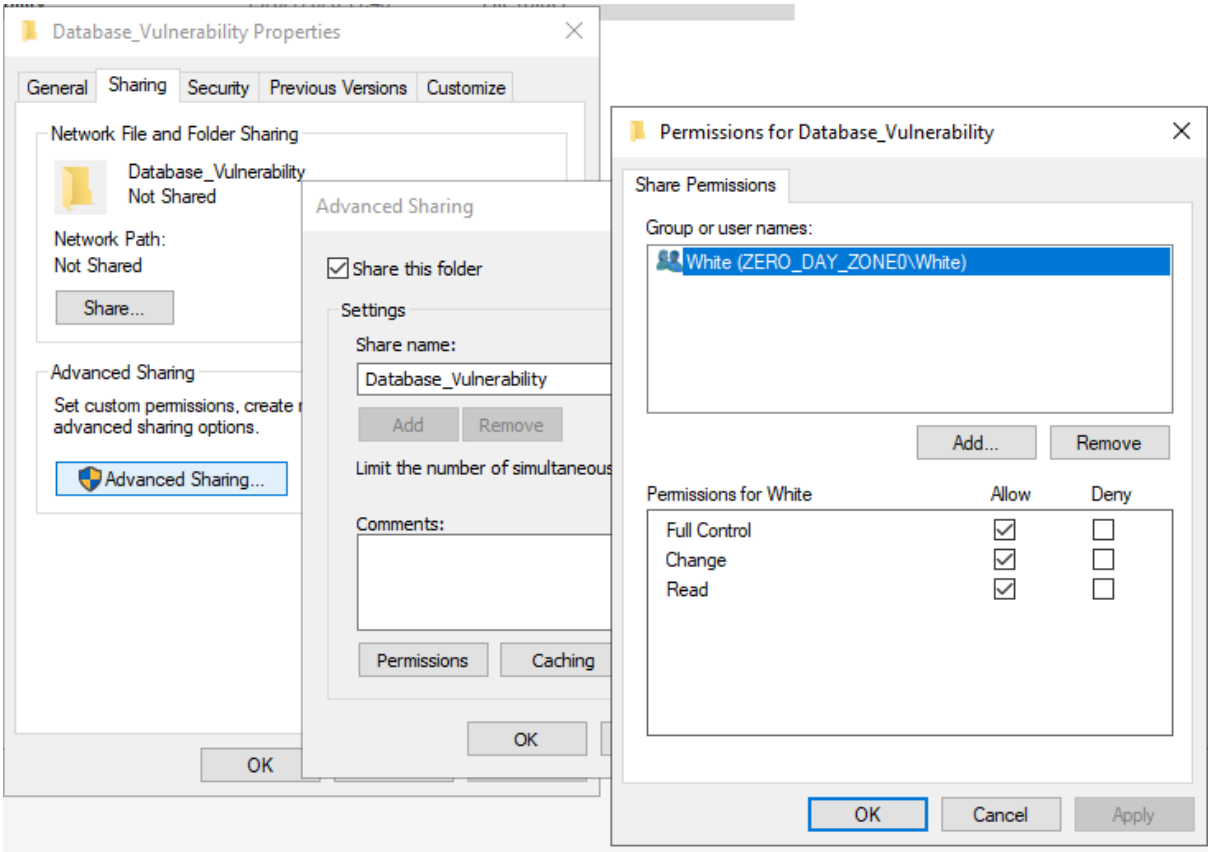
Ho creato sul server la cartella principale **C:\Zero_Day** e al suo interno ho creato tre sottocartelle specifiche, ognuna con regole di accesso diverse.



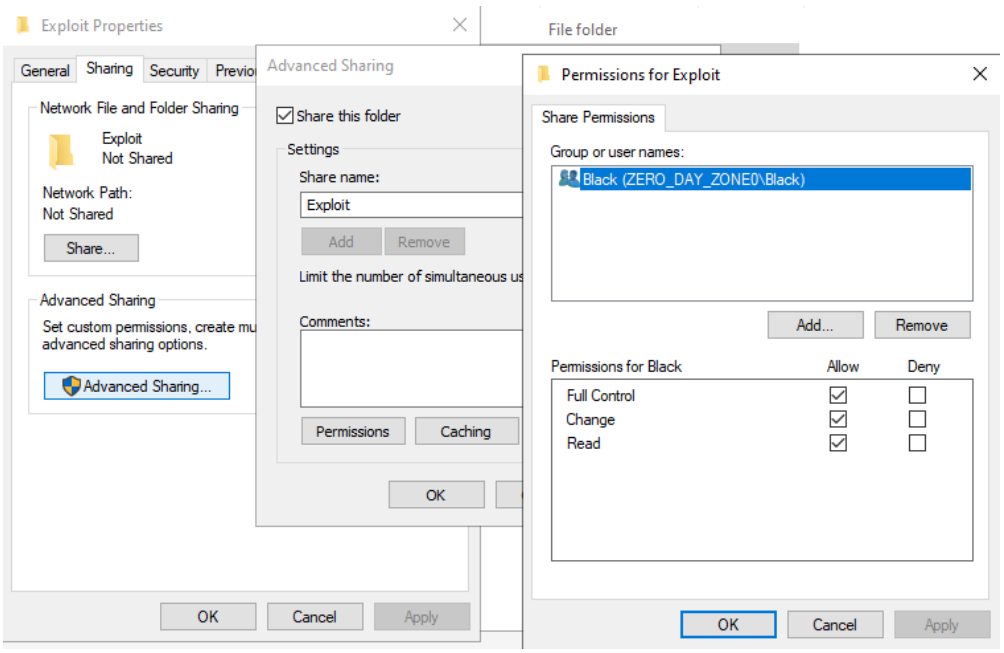


Configurazione dei Permessi (Chi può fare cosa?)

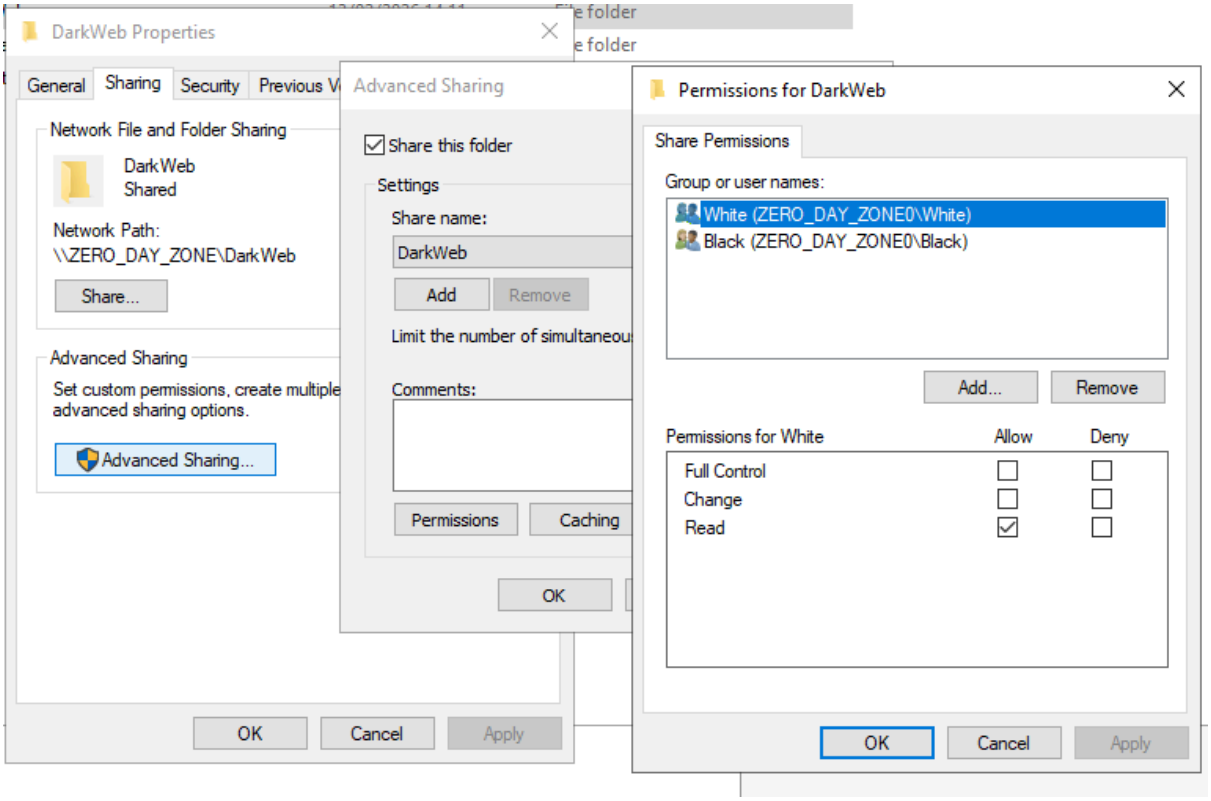
1. **Cartella "Database_Vulnerability"**
    - **A chi serve:** Ai White Hats per archiviare i dati sulle difese.
    - **Permesso:** Solo il gruppo **White** può leggere e modificare. I Black Hats sono esclusi.



2. **Cartella "Exploit"**
    - **A chi serve:** Ai Black Hats per sviluppare i loro codici di attacco.
    - **Permesso:** Solo il gruppo **Black** può leggere e modificare. I White Hats sono esclusi.



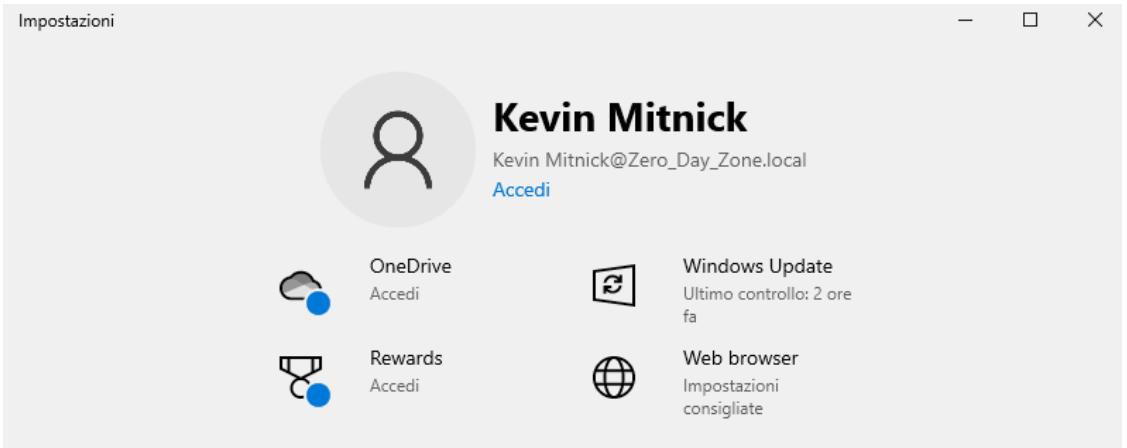
3. **Cartella "DarkWeb" (Nuova Aggiunta)**
    - **A chi serve:** È una zona "pubblica" di osservazione.
    - **Permesso: Entrambi i gruppi (White e Black)** possono **SOLO LEGGERE**. Nessuno può modificare o cancellare i file al suo interno.



---

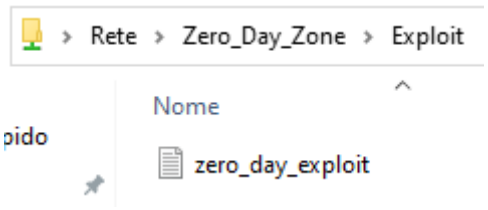
6. VERIFICA FINALE (Il Test)

Per dimostrare che tutto funzioni, mi sono spostato sul computer client (Windows 10) e ho fatto il login come **Kevin Mitnick** (un Black Hat).

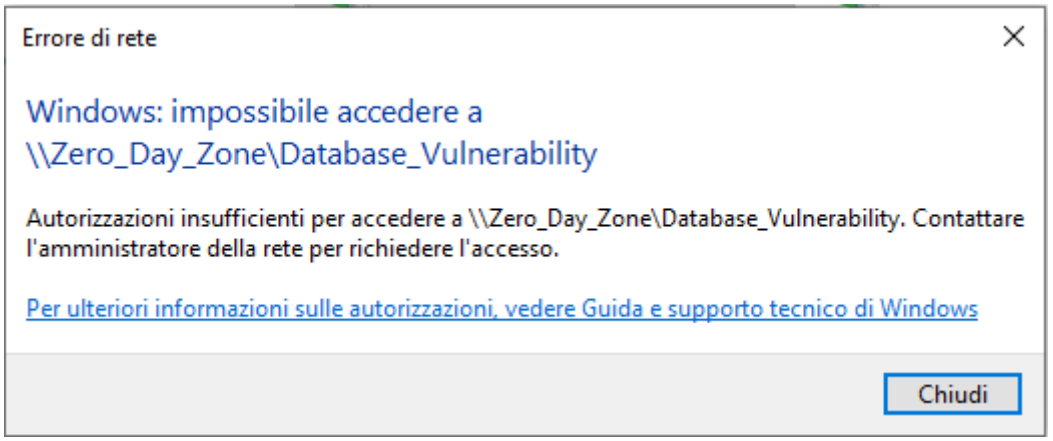


Risultati dei Test:

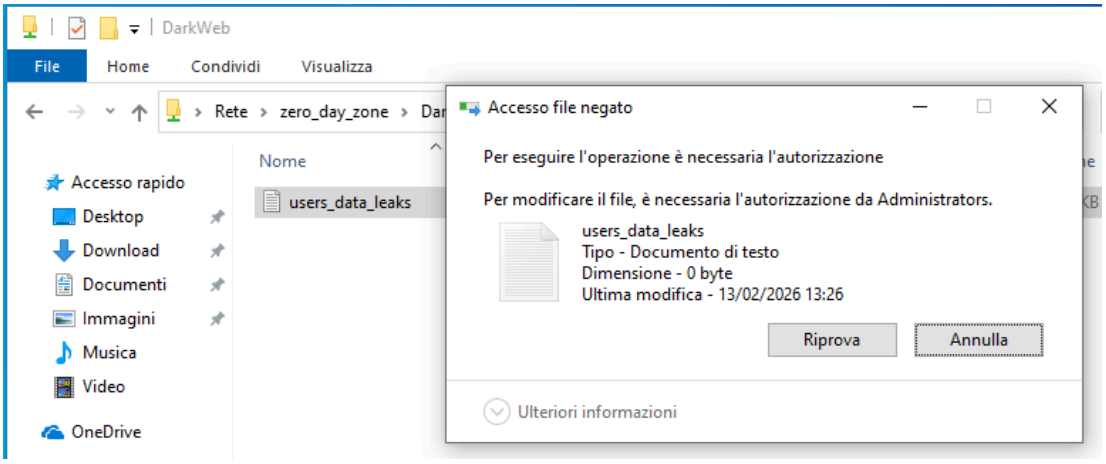
1. **Accesso Riuscito:** Ho provato ad aprire la cartella **Exploit** (la sua cartella di lavoro). Il sistema mi ha fatto entrare e vedere i file. Tutto corretto.



2. **Accesso Negato:** Ho provato ad aprire la cartella **Database_Vulnerability** (riservata ai nemici White Hats). Il sistema mi ha bloccato con un messaggio di errore. Sicurezza confermata.



3. **Accesso Sola Lettura:** Ho aperto la cartella **DarkWeb**. Sono riuscito a entrare, ma quando ho provato a modificare un file, il sistema mi ha impedito di salvarlo, confermando che ho solo i permessi di lettura.



7. CONCLUSIONE

L'esercizio è riuscito perfettamente. Ho dimostrato come dividere gli utenti in gruppi e assegnare permessi specifici permetta di controllare l'accesso ai dati sensibili, garantendo sicurezza e ordine anche in uno scenario "conflittuale" come questo.