

PROGETTO S10L5

Esercizio di oggi: Creazione di Gruppi in Windows Server 2022

Obiettivo

Lo scopo di questo esercizio è di familiarizzare con la gestione dei gruppi di utenti in Windows Server 2022. Imparerai a creare gruppi, assegnare loro permessi specifici e comprendere l'importanza della gestione dei gruppi per la sicurezza e l'amministrazione del sistema.

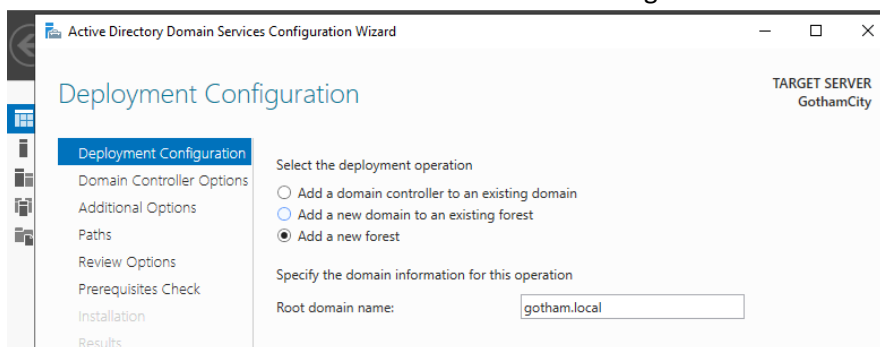
Istruzioni

- Preparazione:**
 - Accedi al tuo ambiente Windows Server 2022.
 - Assicurati di avere i permessi amministrativi necessari per creare e gestire gruppi.
- Creazione dei Gruppi:**
 - Crea due gruppi distinti. Puoi scegliere i nomi che preferisci per questi gruppi, ma assicurati che i nomi siano significativi per riflettere la loro funzione o ruolo all'interno dell'organizzazione (ad esempio, "Amministratori", "UtentiStandard", "MarketingTeam", "Sviluppatori", ecc.).
- Assegnazione dei Permessi:**
 - Per ogni gruppo, assegna permessi specifici. Puoi scegliere quali permessi concedere, ma assicurati di considerare i seguenti aspetti:
 - Accesso ai file e alle cartelle.
 - Esecuzione di programmi specifici.
 - Modifiche alle impostazioni di sistema.
 - Accesso remoto al server.
 - Documenta i permessi assegnati a ciascun gruppo, spiegando perché hai scelto tali permessi.
- Verifica:**
 - Una volta creati i gruppi e assegnati i permessi, verifica che le impostazioni siano corrette. Puoi farlo:
 - Creando utenti di prova e aggiungendoli ai gruppi.
 - Verificando che gli utenti abbiano i permessi assegnati in base al gruppo a cui appartengono.
- Documentazione:**
 - Scrivi un breve report che includa:
 - I nomi dei gruppi creati.
 - I permessi assegnati a ciascun gruppo.
 - I passaggi seguiti per creare e configurare i gruppi.
 - Eventuali problemi riscontrati e come li hai risolti.

L'obiettivo di questo progetto è familiarizzare con la gestione dei gruppi di utenti in un ambiente Windows Server 2022, creando gruppi, assegnando loro permessi specifici e verificando il corretto funzionamento delle impostazioni.

Configurazione del Dominio

È stata creata una nuova foresta di dominio chiamata gotham.local

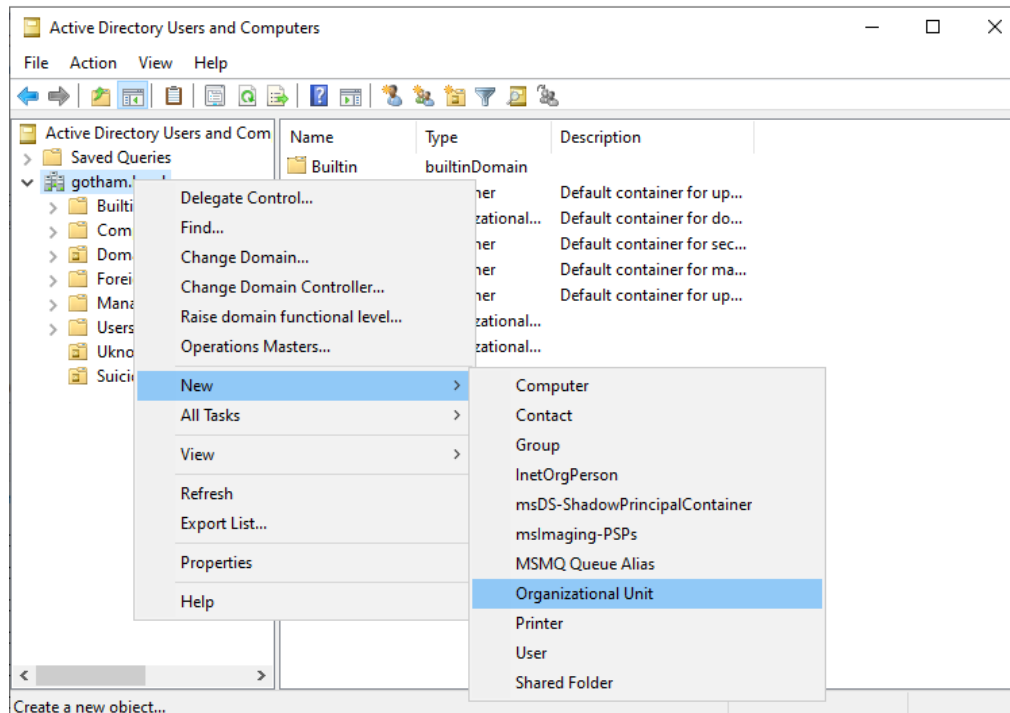


Computer name
Domain

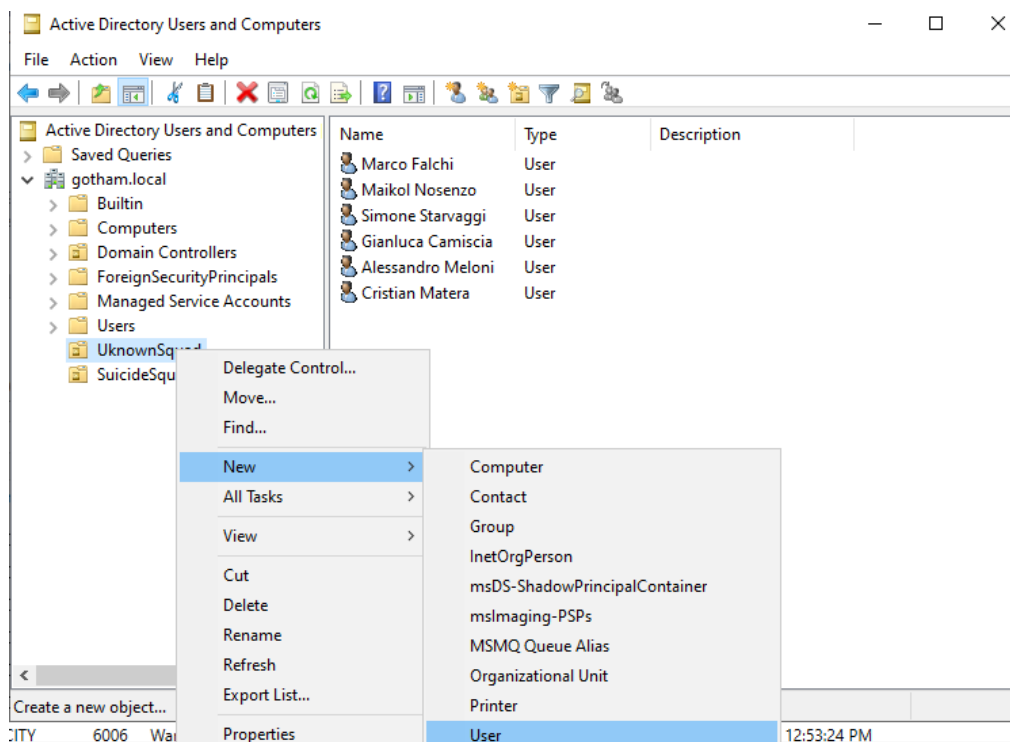
GothamCity
gotham.local

Creazione delle Unità Organizzative (OU)

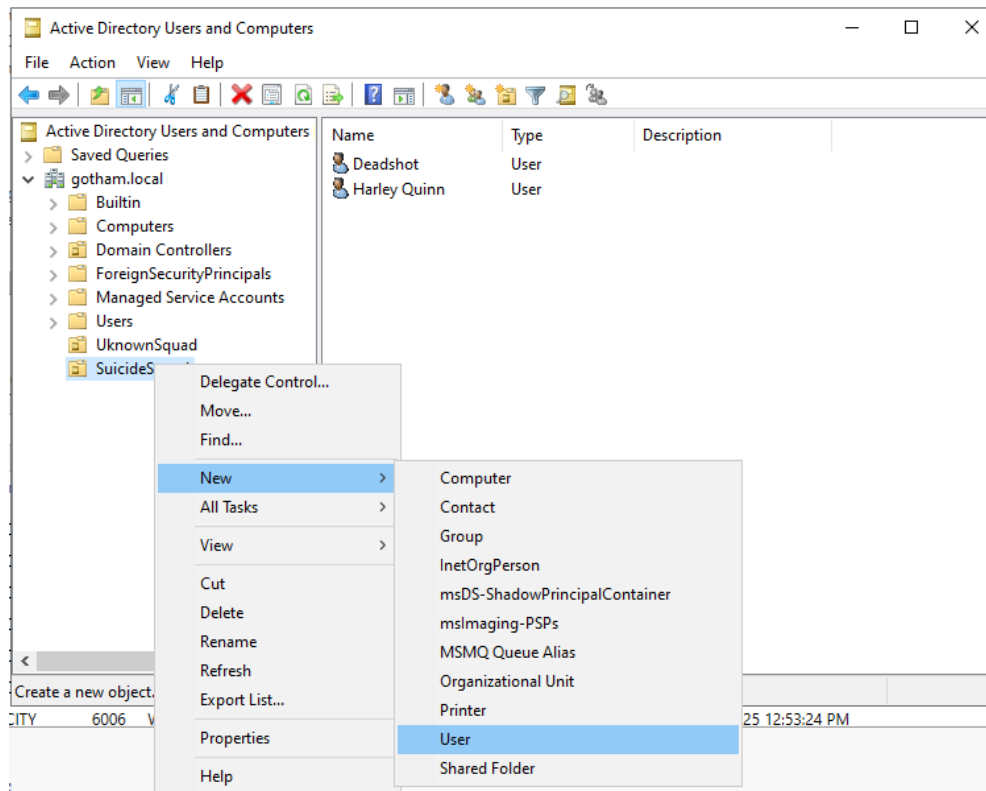
Utilizzando lo strumento **Active Directory Users and Computers**, sono state create due unità organizzative: UnknownSquad e SuicideSquad



Nell'OU UnknownSquad sono stati creati gli utenti Marco Falchi, Maikol Nosenzo, Simone Starvaggi, Gianluca Camiscia, Alessandro Meloni e Cristian Matera.



Nell'OU SuicideSquad sono stati creati gli utenti Deadshot e Harley Quinn

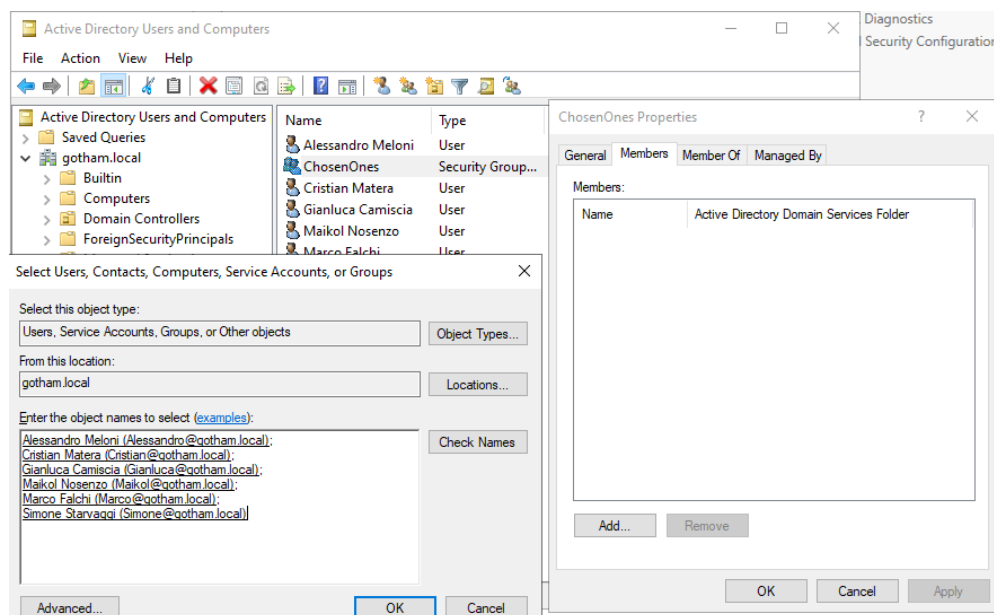


Creazione dei Gruppi

Sono stati creati due gruppi di sicurezza distinti:

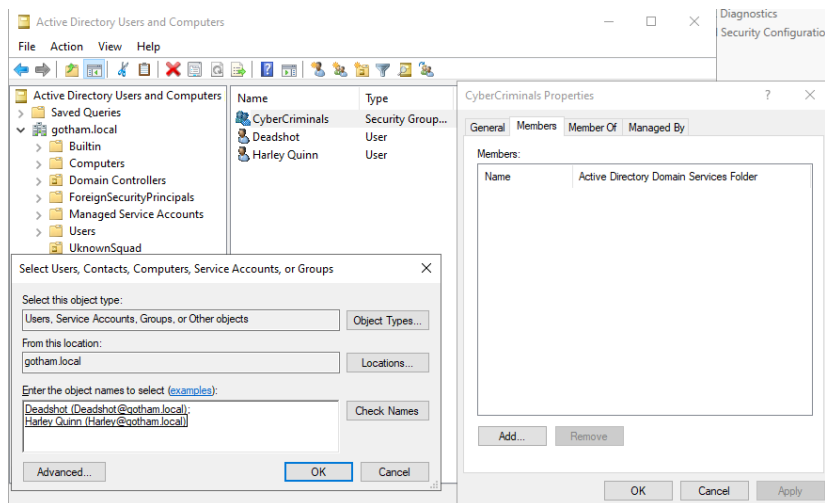
Gruppo ChosenOnes: Creato all'interno dell'OU UknownSquad.

A questo gruppo sono stati aggiunti tutti gli utenti dell'OU, ovvero: Alessandro Meloni, Cristian Matera, Gianluca Camiscia, Maikol Nosenzo, Marco Falchi e Simone Starvaggi.



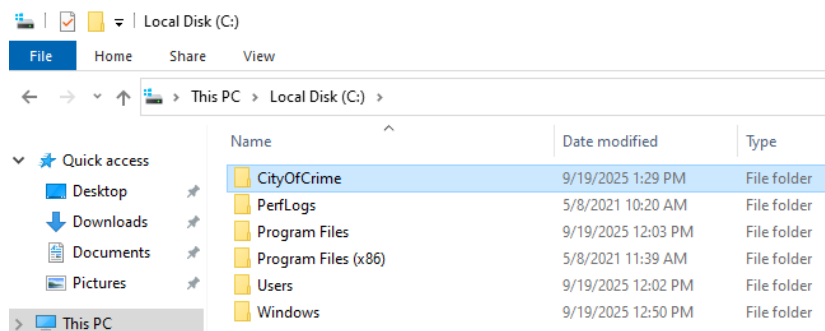
Gruppo CyberCriminals: Creato all'interno dell'OU SuicideSquad.

A questo gruppo sono stati aggiunti gli utenti Deadshot e Harley Quinn.

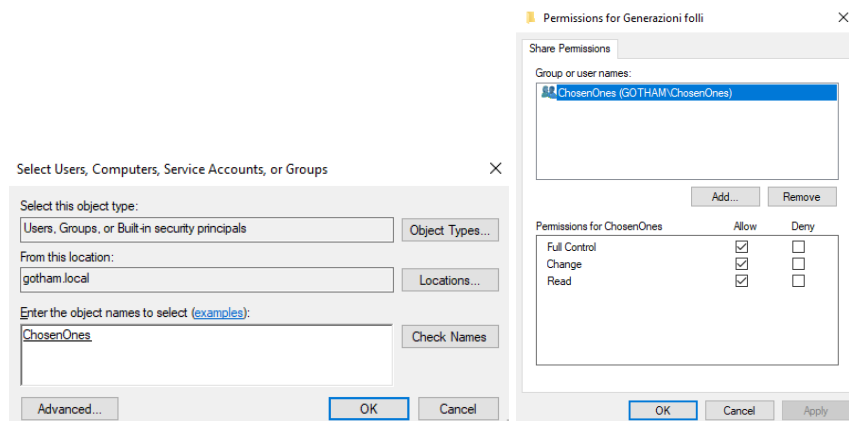


Creazione folders

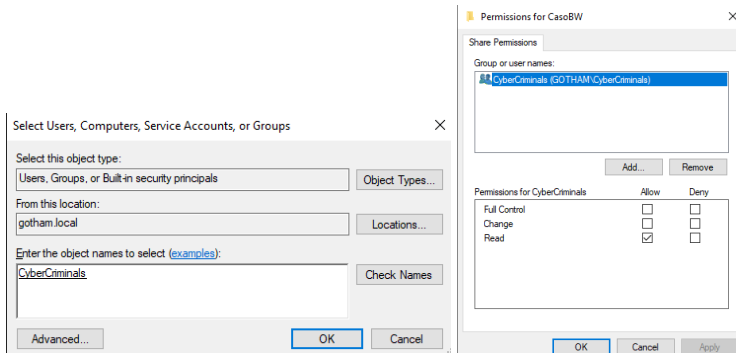
E' stato creato un folder chiamato CityOfCrime all'interno disco C:



All'interno creo cartella **Generazioni folli**, dopo di che proprietà della cartella/Sharing/Advanced Sharing/Permissions. Qui togliamo il gruppo "Everyone" e inseriamo il gruppo che avranno accesso alla cartella (ChosenOnes)

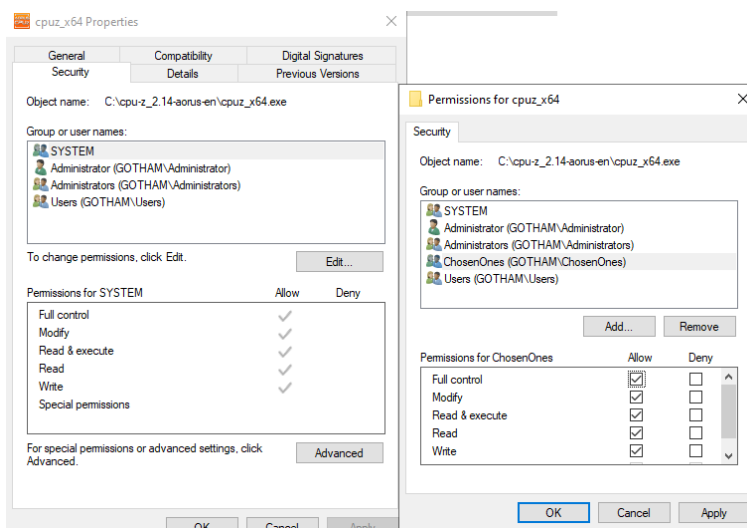


Creo cartella **CasoBW**, dopo di che proprietà della cartella/Sharing/Advanced Sharing/Permissions. Anche qui togliamo “Everyone” e inseriamo gli utenti che avranno accesso alla cartella, ma questa volta solo permessi di lettura

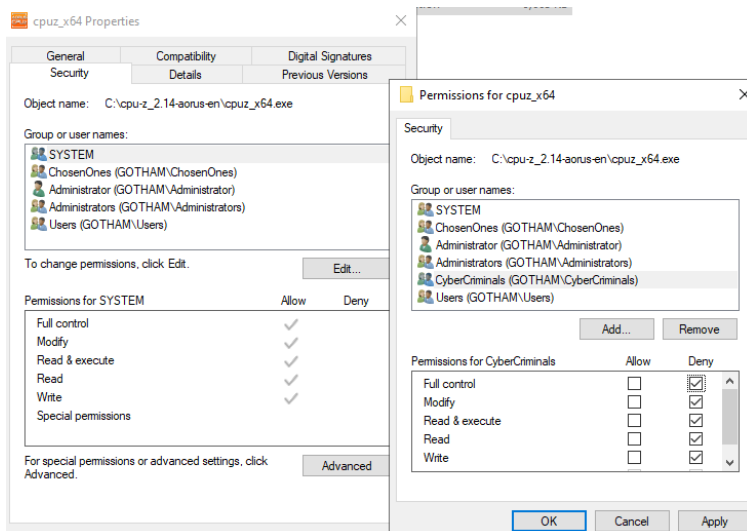


Permessi esecuzione

I permessi sono stati configurati per l'eseguibile di CPU-Z. Il gruppo **ChosenOnes** avrà il **full control** sull'eseguibile.

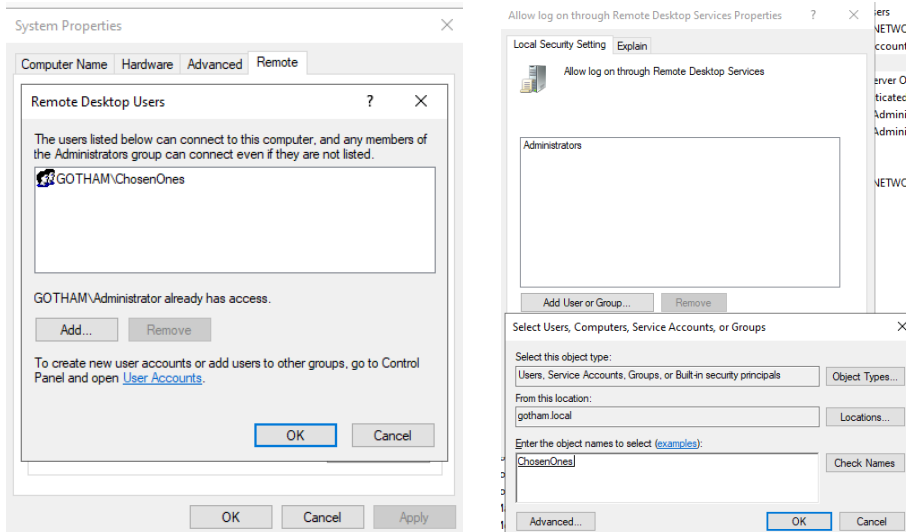


Permessi eseguibile CPU-Z per **CyberCriminals**, questo gruppo avrà **deny** su tutti i permessi



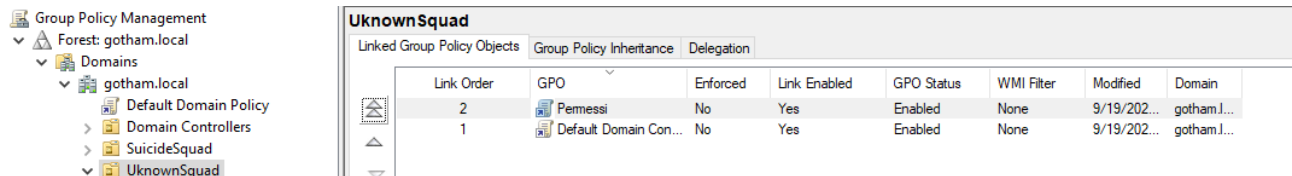
Accesso remoto al server

Tramite Win+R inseriamo sysdm.cpl, navighiamo su System Properties e al suo interno troveremo la tab Remote. Da qui aggiungiamo il gruppo che avrà accesso remoto al server. (**ChosenOnes**)

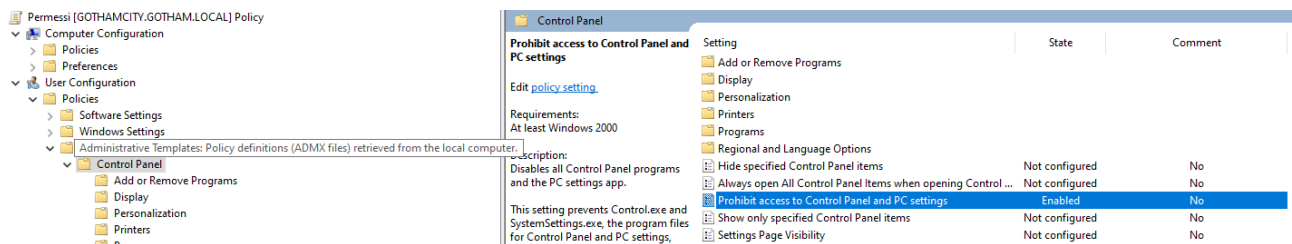


Modifiche alle impostazioni di sistema

Dopo aver creato una GPO personalizzata, tramite **Group Policy Management**, chiamata **Permessi**



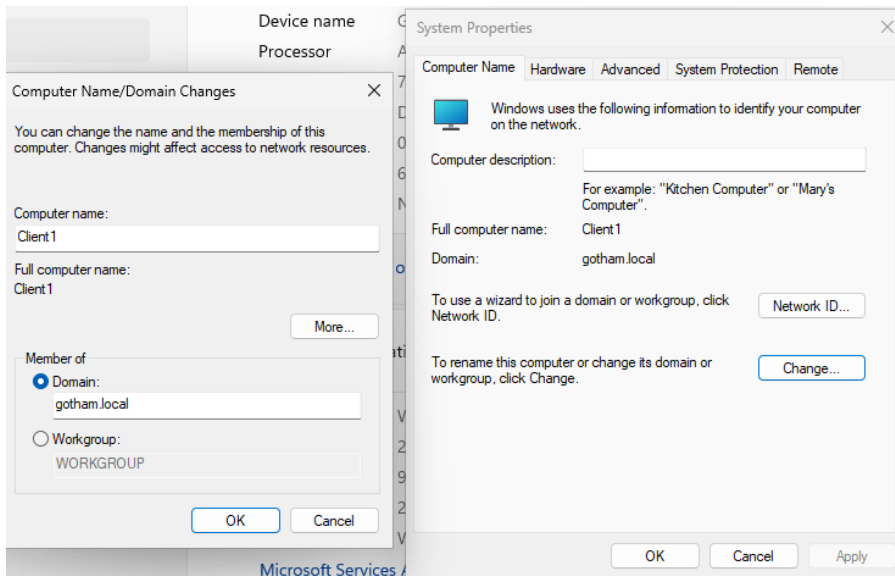
Nella sezione **User Configuration/Administrative Templates/Control Panel**, ho disabilitato l'accesso al pannello di controllo per tutti gli utenti del gruppo Unknown Squad, impostando Enable.



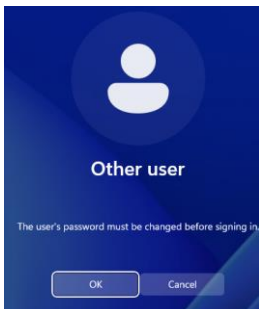
CONFIGURAZIONE CLIENT

È stato configurato un computer client per unirsi al dominio gotham.local e sono stati effettuati test per verificare il corretto funzionamento dei permessi assegnati.

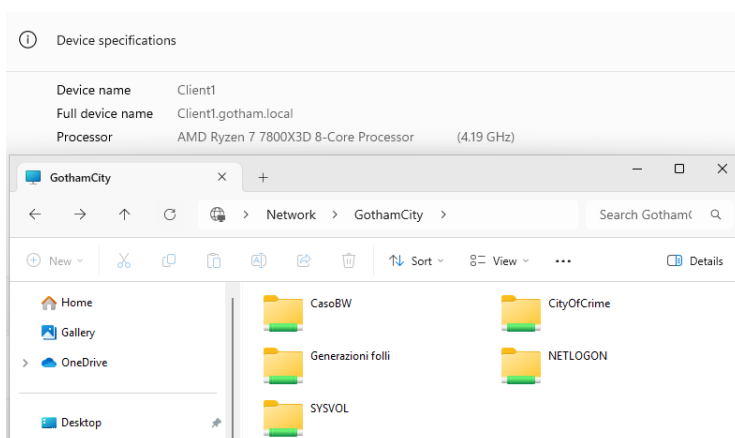
Accesso Utente e Dominio: L'utente Alessandro, membro del gruppo ChosenOnes, è stato in grado di accedere al dominio dopo aver cambiato la password. È stato possibile visualizzare le cartelle di dominio GothamCity.



Accesso Utente e Dominio: L'utente Alessandro, membro del gruppo **ChosenOnes**, è stato in grado di accedere al dominio dopo aver cambiato la password. È stato possibile visualizzare le cartelle di dominio GothamCity.

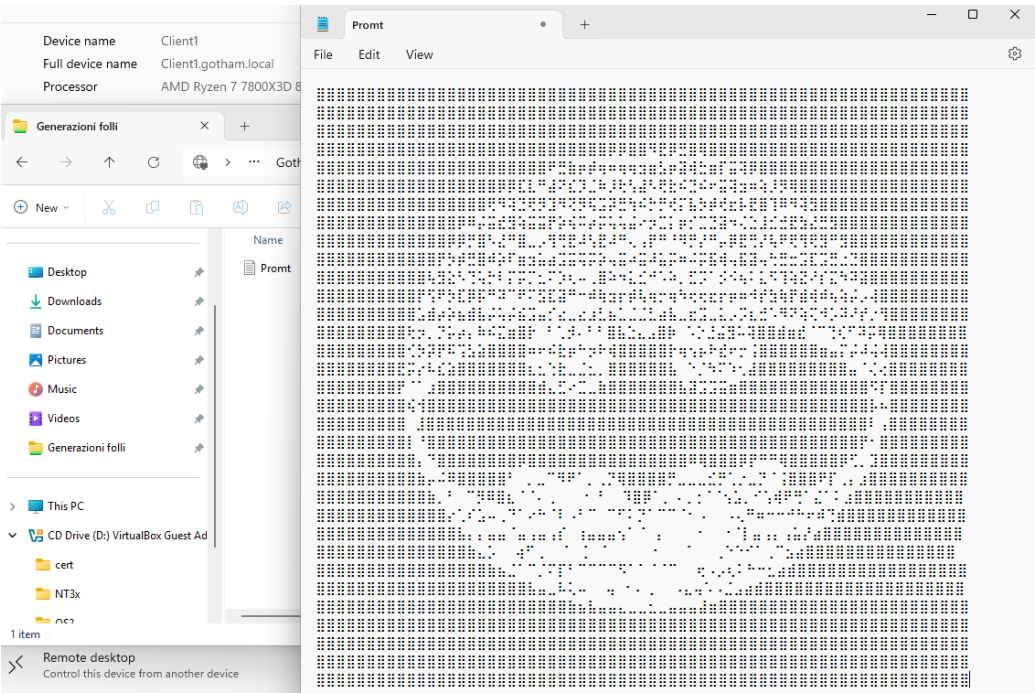


È stato possibile visualizzare le cartelle di dominio GothamCity.

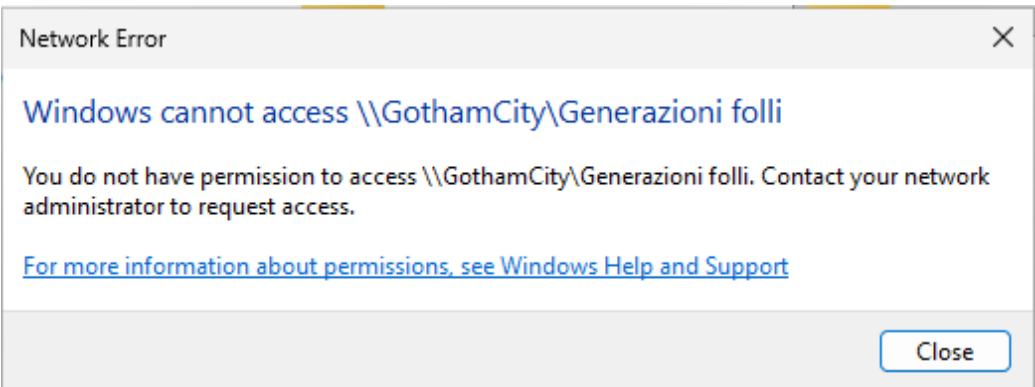
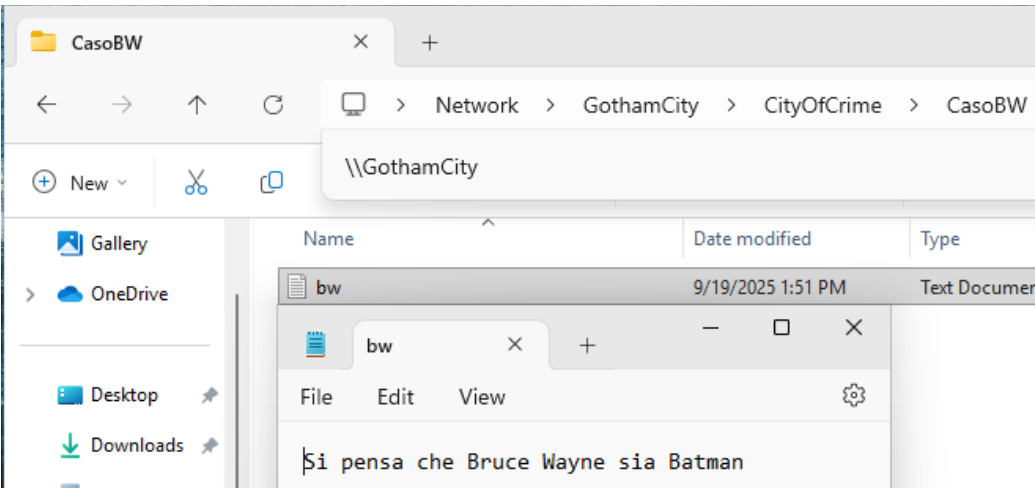


TEST PERMESSI CARTELLE

L'utente Alessandro, appartenente al gruppo ChosenOnes, ha avuto accesso completo alla cartella Generazioni folli, confermando che i permessi sono stati applicati correttamente.

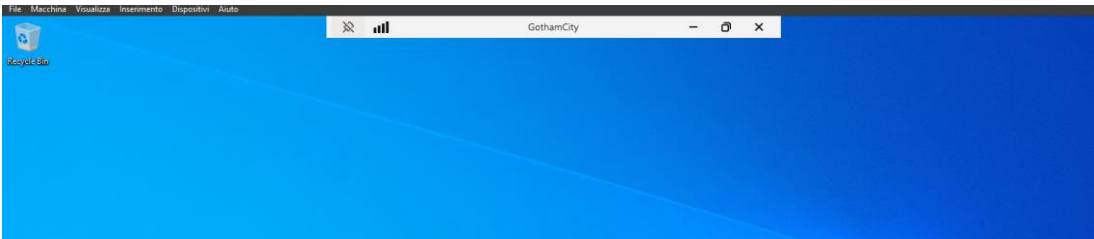
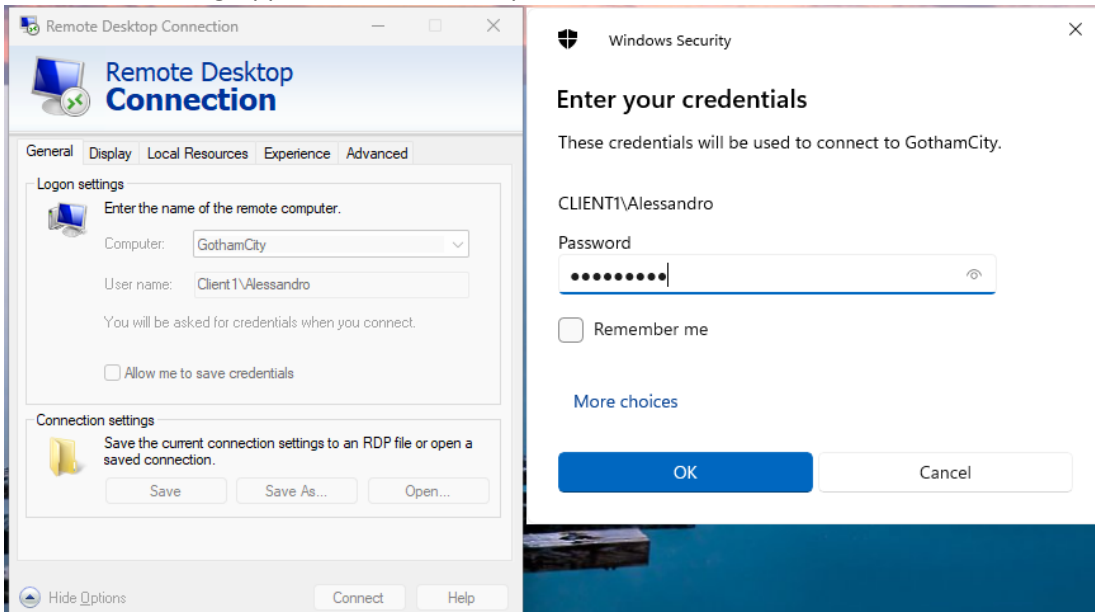


Il gruppo **CyberCriminals** può accedere al file **BW (BruceWayne)**, ma non può accedere a Generazioni folli

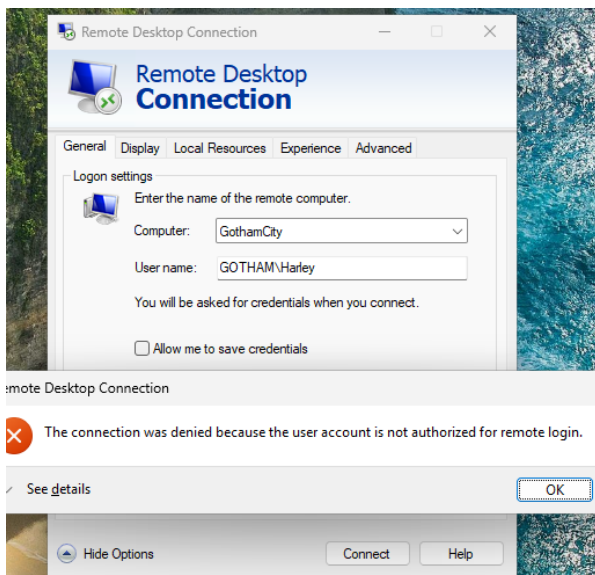


TEST ACCESSO REMOTO

L'utente Alessandro è riuscito a stabilire una connessione di desktop remoto al server GothamCity, verificando che il gruppo ChosenOnes ha i permessi necessari.

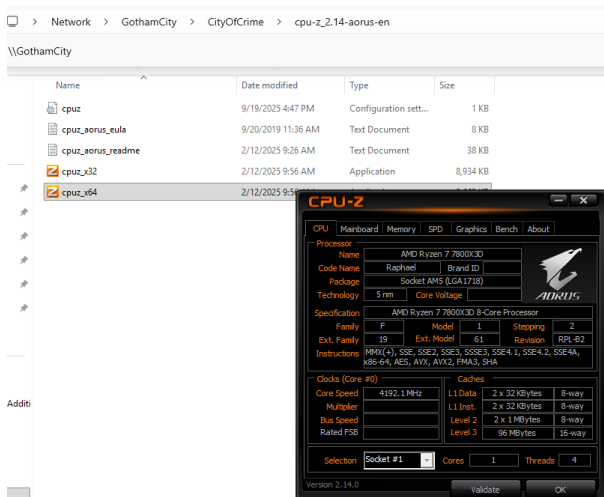


Il gruppo **CyberCriminals** non può accedere perché non autorizzato

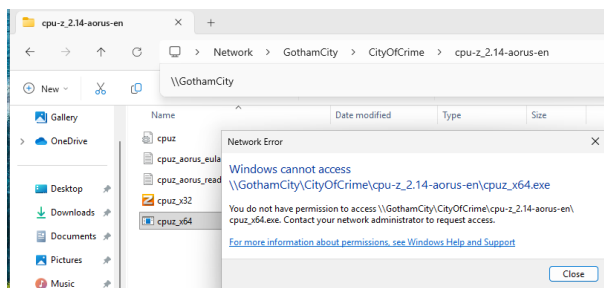


TEST PERMESSI ESECUZIONE

L'utente Alessandro ha eseguito con successo CPU-Z, dimostrando che il gruppo ChosenOnes ha i permessi di esecuzione necessari.

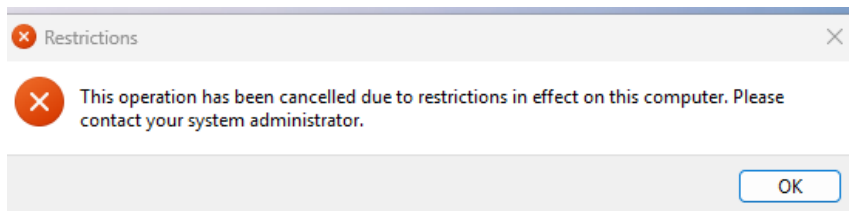


Il gruppo **CyberCriminals** non può eseguire CPU-Z, dimostrando che il suo gruppo non ha i permessi di esecuzione necessari.

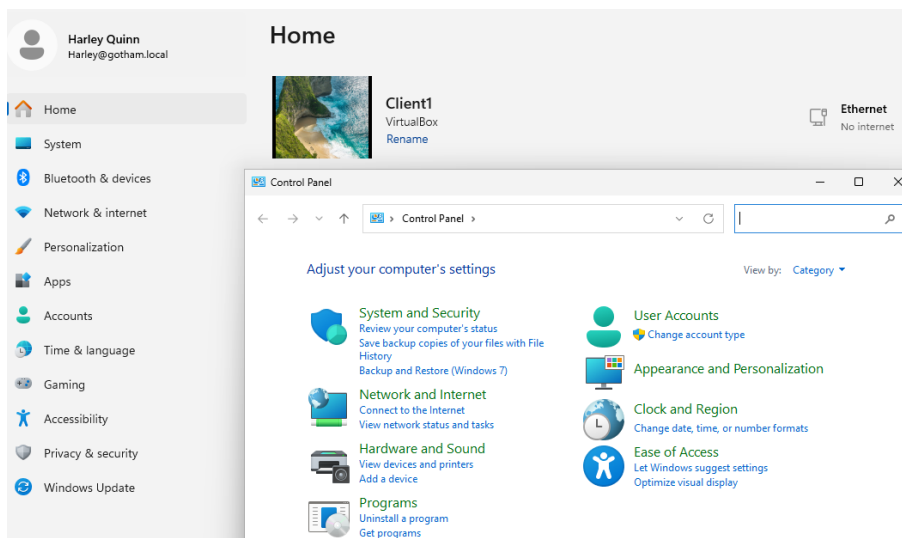


TEST IMPOSTAZIONI DI SISTEMA

Nessun membro del gruppo **UknownSquad** può accedere al Pannello di Controllo



Mentre i membri del gruppo **CyberCriminals** può



Il progetto ha documentato i passaggi per la creazione e la gestione di gruppi di utenti in un ambiente di dominio, dimostrando la corretta implementazione e verifica dei permessi.

Gruppi creati:

- **ChosenOnes**
- **CyberCriminals**

Permessi assegnati:

- **ChosenOnes:**
 - Full Control su file
 - Full Control sull'eseguibile di CPU-Z
 - Accesso remoto al server
- **CyberCriminals:**
 - Sola lettura su file
 - Permessi accesso al Pannello di Controllo