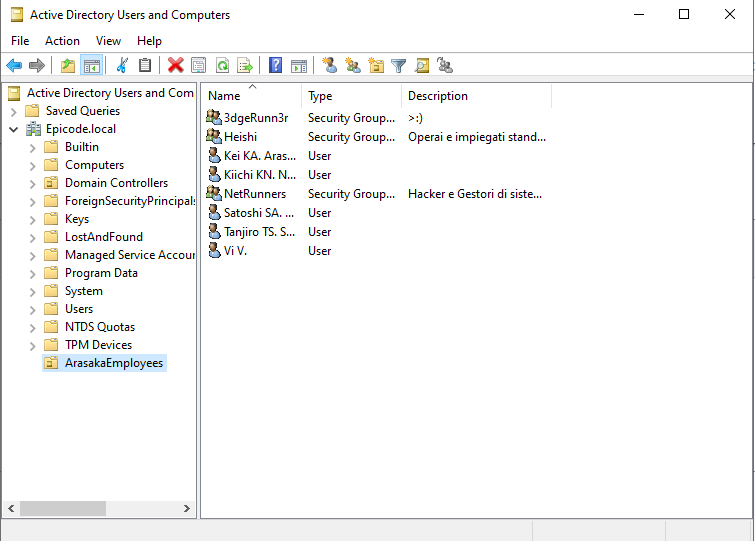
**Configurazione di Active Directory: Gestione Gruppi, Permessi e Policy**

**Introduzione**

In questa presentazione spiego i passi che ho seguito per configurare un ambiente Active Directory, includendo la creazione di gruppi, la gestione dei permessi e la definizione di policy per l'accesso.

**Passaggi Eseguiti**

**1. Creazione dei Gruppi e degli Utenti**

Ho creato i seguenti gruppi:

* **NetRunners (sistemisti)**
* **Heishi (dipendenti)**
* **3dg3runn3r (attaccante simulato)**

Per testare la configurazione, ho aggiunto alcuni utenti di prova:

* **Kei Arasaka** per i NetRunners.
* **Vi** per il gruppo 3dg3runn3r.

**2. Creazione delle Cartelle Condivise**

Successivamente, ho creato due cartelle condivise:

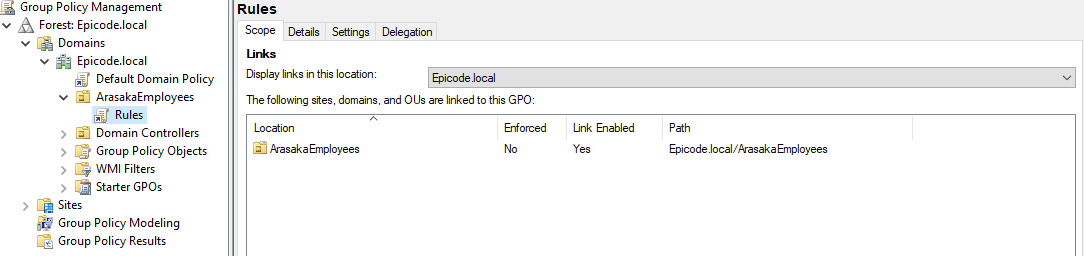
* Una per i **NetRunners**, assegnando loro i permessi di lettura, scrittura e modifica.
* Una per gli **Heishi**, a cui ho concesso i permessi di sola lettura e scrittura.

Inoltre, ho dato all'utente **Vi (3dg3runn3r)** il controllo totale su entrambe le cartelle, simulando il comportamento di un attaccante con privilegi elevati.

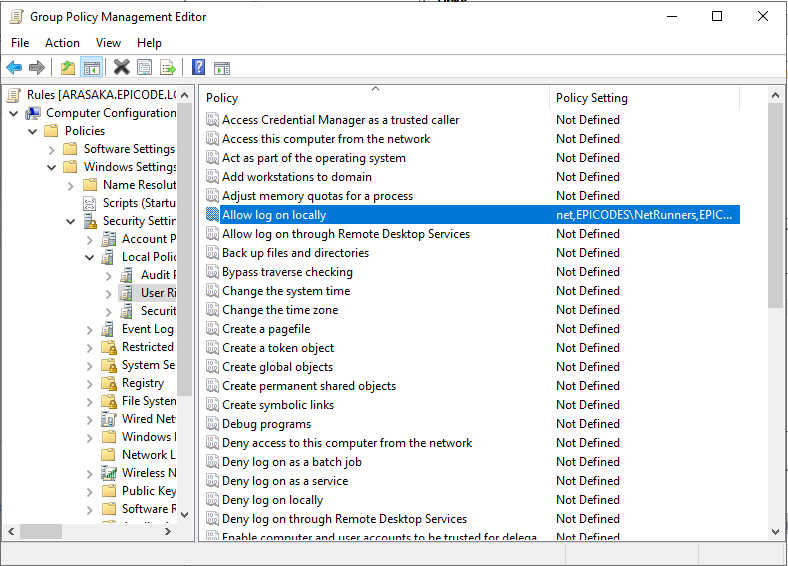
**3. Gestione dei Permessi**

Ho configurato i permessi in questo modo:

* **NetRunners:**
  + Permessi di lettura, scrittura e modifica su entrambe le cartelle.
* **Heishi:**
  + Permessi limitati a lettura e scrittura solo sulla propria cartella.
* **3dg3runn3r:**
  + Controllo totale su tutte le risorse condivise.

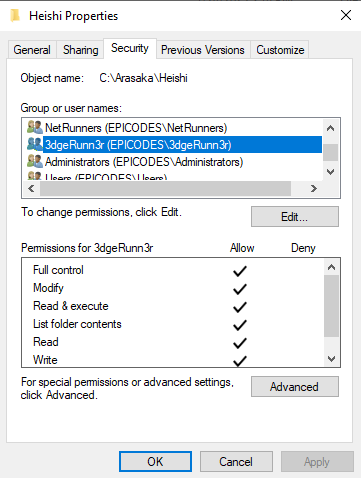
**4. Creazione e Configurazione delle Group Policy**

Ho creato una nuova GPO per gestire i permessi: (per brevità ho modificato solo il permesso di loggare localmente)

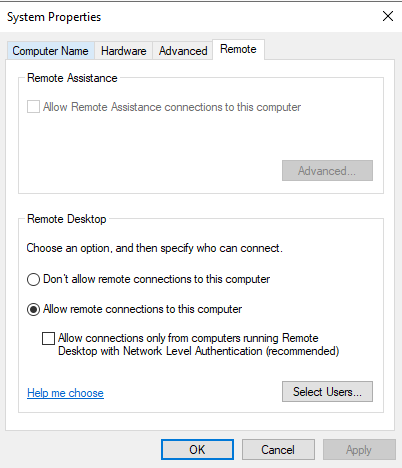
* Ho permesso a tutti i gruppi di effettuare il logon localmente.
* Ho specificato anche il permesso di accesso remoto per tutti i gruppi.

**5. Estensione dei Permessi (Concetto)**

Ho immaginato una configurazione più complessa per i gruppi:

* **NetRunners (sistemisti):**
  + Possibilità di modificare le impostazioni di sistema.
  + Diritto di loggare come servizio.
  + Permessi per gestire altre GPO.
* **Heishi (dipendenti):**
  + Limitati all'uso di applicazioni approvate tramite Software Restriction Policies.
  + Privilegi minimi per modificare le impostazioni.
* **3dg3runn3r (attaccante simulato):**
  + ****Simulato un attaccante con controllo totale su file, cartelle e configurazioni.

**6. Dati permessi di accesso remoto:**

****

**Difficoltà Riscontrate e Soluzione**

* **Problema:** Quando ho assegnato i permessi alle cartelle condivise, i NetRunners non riuscivano a modificare file nella cartella degli Heishi a causa di conflitti nei permessi NTFS.
* **Soluzione:**
  + Ho verificato le **permissions NTFS** e quelle di condivisione, scoprendo che le permissions NTFS erano impostate su "Sola Lettura" per i NetRunners.
  + Ho modificato le permissions NTFS, aggiungendo il gruppo NetRunners con privilegi di "Modifica".

**Test Eseguito**

Ho testato la configurazione sia localmente che da remoto:

* **Accesso Remoto:** Ho verificato che tutti i gruppi potevano accedere al sistema in remoto grazie ai permessi configurati nella GPO.
* **Risultati:**
  + **NetRunners:** Capacità di accedere e modificare i file come previsto.
  + **Heishi:** Accesso limitato alle risorse autorizzate.
  + **3dg3runn3r:** Controllo totale, simulando un attaccante che ha compromesso il sistema.

**Conclusioni**

Le impostazioni che ho configurato e testato hanno funzionato con successo. I gruppi rispondono correttamente ai permessi assegnati, garantendo una separazione chiara tra i livelli di accesso.

Questa configurazione evidenzia l'importanza di testare accuratamente le policy per identificare e risolvere eventuali conflitti nei permessi.