Report Tecnico di Laboratorio: System Security & Access Control

Studente: Rocco Paolo Caccamo

Corso: Cybersecurity & Ethical Hacking

Oggetto: Configurazione Domain Controller, Gestione Identità (IAM) e Verifica ACL

Target: Windows Server 2022 (`EPICODE-SERVER`)

Data: 11 Febbraio 2026

---

1. Obiettivo dell'Esercitazione

Il presente documento illustra le procedure tecniche adottate per la messa in sicurezza di un'infrastruttura di dominio basata su Microsoft Active Directory. L'attività si focalizza sulla segregazione dei privilegi (Principle of Least Privilege), implementata attraverso una strutturazione gerarchica delle utenze e l'applicazione di Access Control Lists (ACL) sulle risorse di rete condivise.

---

2. Configurazione Infrastrutturale (Network & Domain)

La fase preliminare ha riguardato la configurazione dello stack TCP/IP del server per garantirne il funzionamento come Domain Controller. È stato assegnato l'indirizzo IP statico **192.168.50.2**. Il server DNS primario è stato impostato sull'indirizzo di loopback (**127.0.0.1**), configurazione mandataria per la corretta risoluzione dei servizi di directory locali.

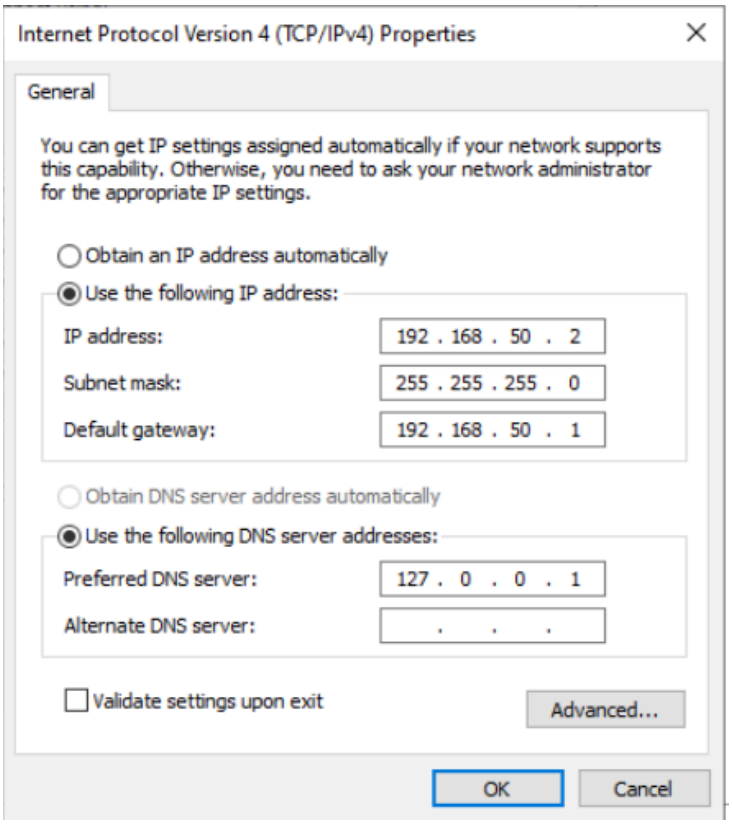

Fig. 1 - Configurazione interfaccia di rete: IP Statico e DNS locale.

A seguito della configurazione di rete, il server è stato promosso a Domain Controller per il nuovo dominio **Epicode.local**, con hostname definito come **EPICODE-SERVER**.

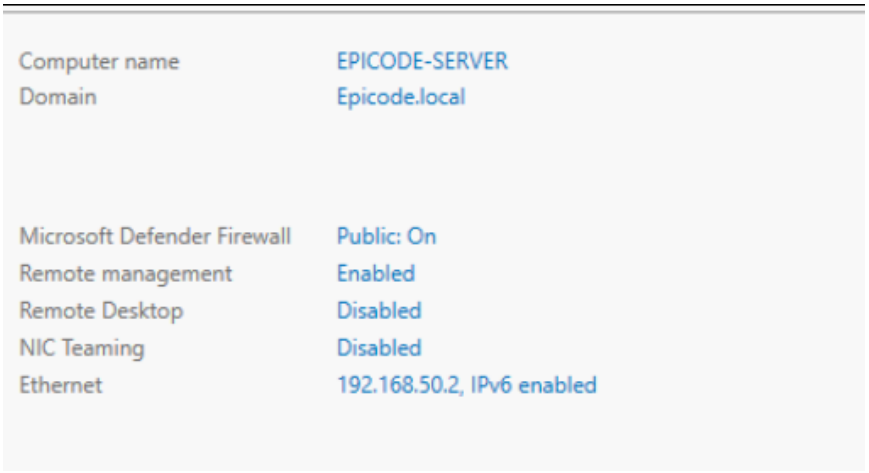

Fig. 2 - Proprietà di Sistema: verifica Hostname e Dominio.

3. Gestione Identità e Accessi (IAM Structure)

Utilizzando la console *Active Directory Users and Computers*, è stata definita una struttura logica basata su Organizational Units (OU) per separare i ruoli aziendali dai ruoli tecnici/offensivi (simulazione).

È stata creata la **OU Amministrazione** contenente l'account utente standard **Chiara Bianchi**.

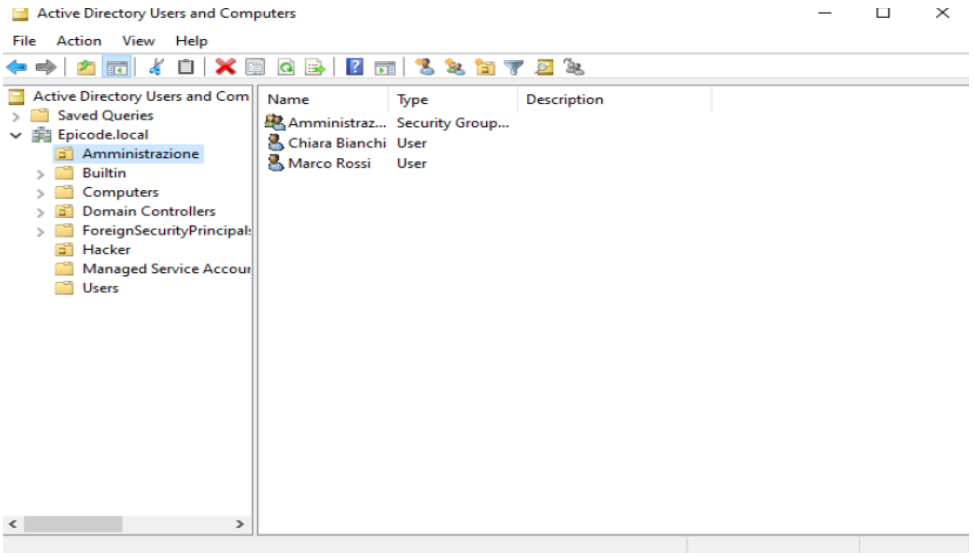

Fig. 3 - Struttura AD: OU Amministrazione.

Parallelamente, è stata creata la **OU Hacker** contenente il gruppo di sicurezza globale **Hacker 1** e gli utenti *Tyrell Wellick* e *Darlene Alderson*.

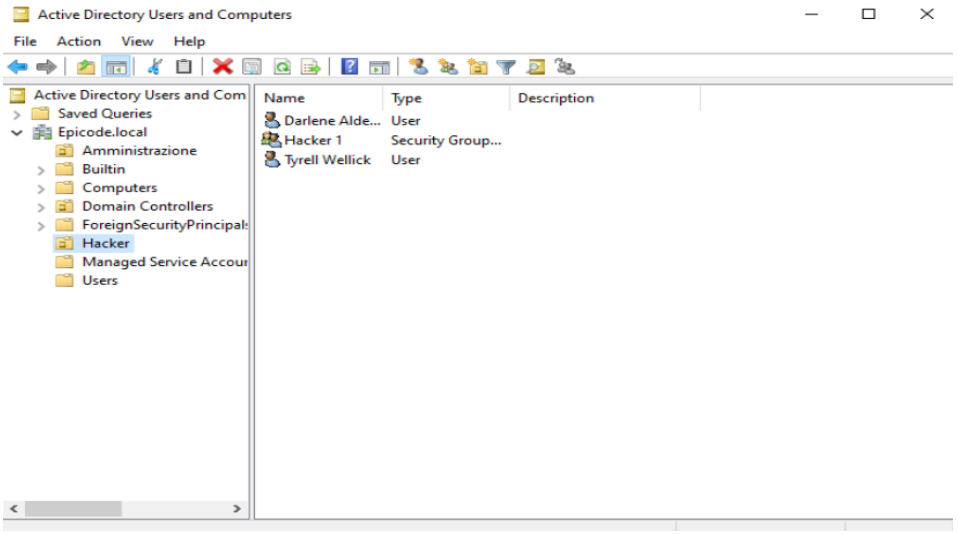

Fig. 4 - Struttura AD: OU Hacker e Gruppo di Sicurezza.

4. Configurazione Risorse e Permessi (ACL)

Sul File Server sono state predisposte due condivisioni di rete con permessi differenziati per testare la granularità degli accessi.

La risorsa **"Dati segreti"** è stata configurata concedendo permessi di lettura al gruppo *Amministrazione*.

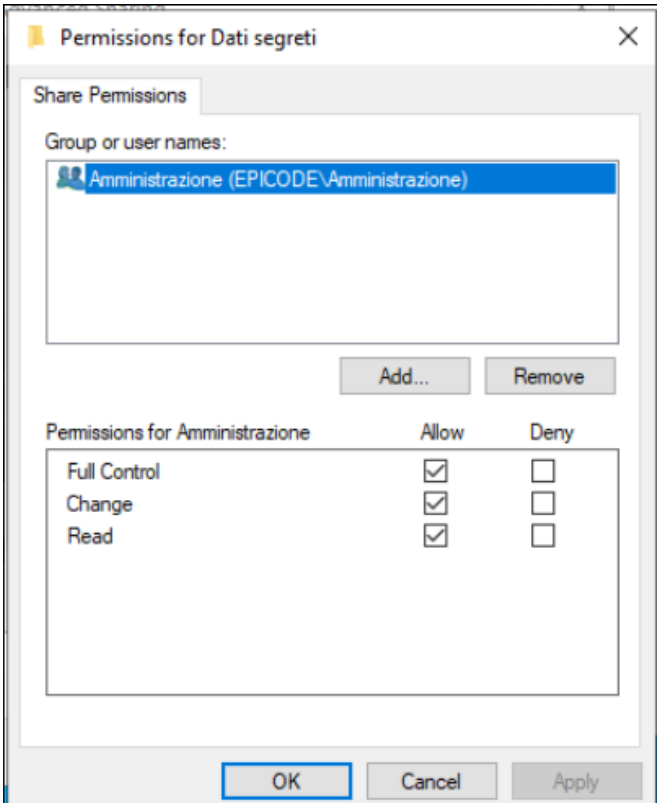

Fig. 5 - ACL: Permessi concessi al gruppo Amministrazione.

La risorsa **"Dati top"** è stata configurata restringendo l'accesso esclusivamente al gruppo di sicurezza *Hacker 1*.

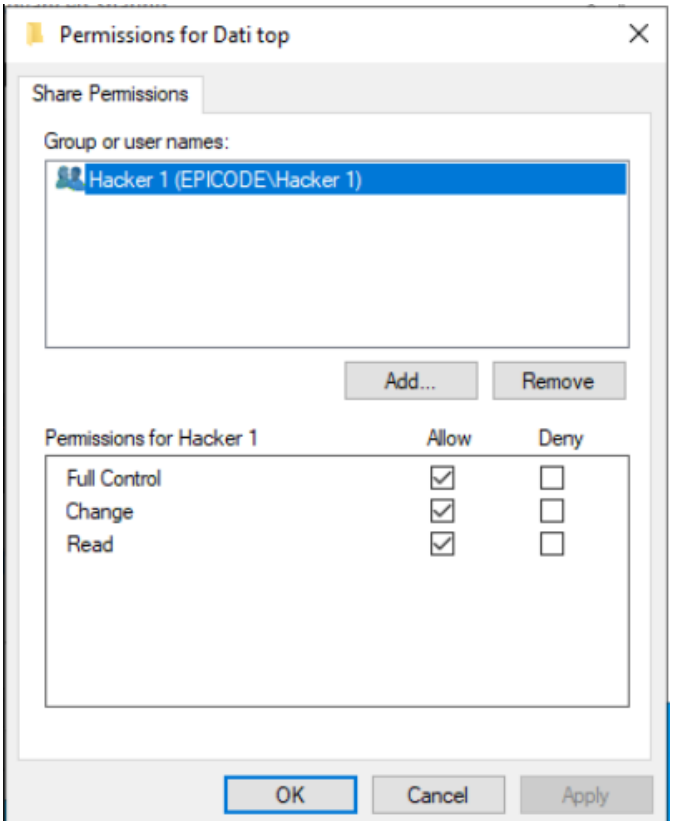

Fig. 6 - ACL: Restrizione permessi al solo gruppo Hacker 1.

---

5. Verifica Operativa (Testing)

La validazione delle policy di sicurezza è stata effettuata simulando l'accesso di un utente standard. È stato eseguito il login alla workstation con le credenziali di **Chiara Bianchi** (`EPICODE\Chiara`).

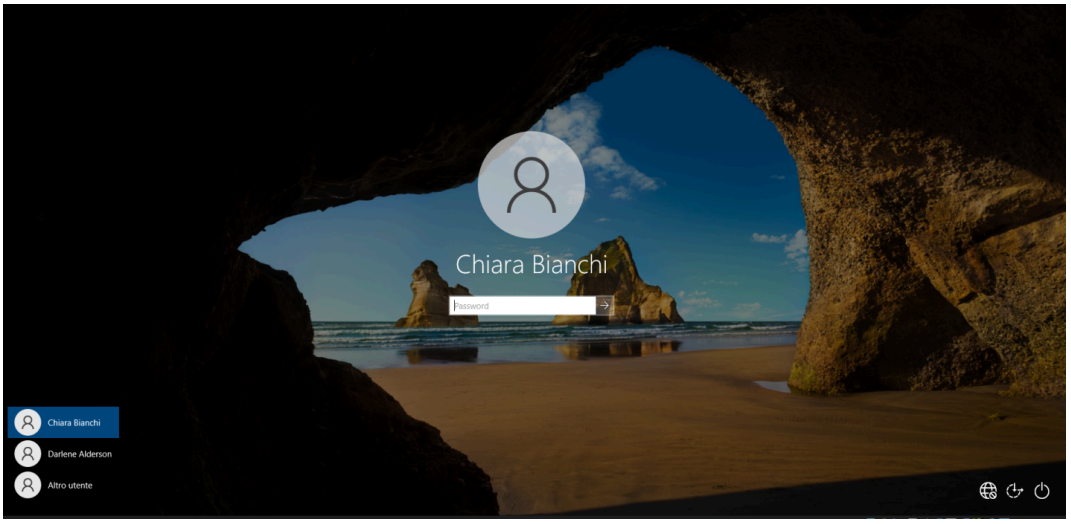

Fig. 7 - Fase di autenticazione utente.

Navigando verso la risorsa di rete `\\epicode-server`, sono state visualizzate le cartelle condivise.

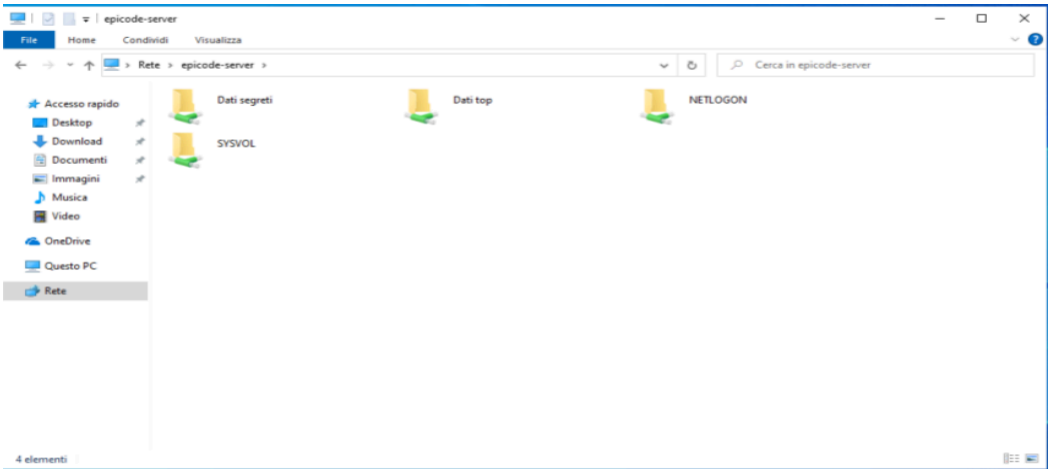

Fig. 8 - Enumerazione delle share di rete.

Risultato Test 1: Accesso Consentito L'accesso alla cartella **"Dati segreti"** è avvenuto correttamente, confermando l'associazione dell'utente al gruppo *Amministrazione*.

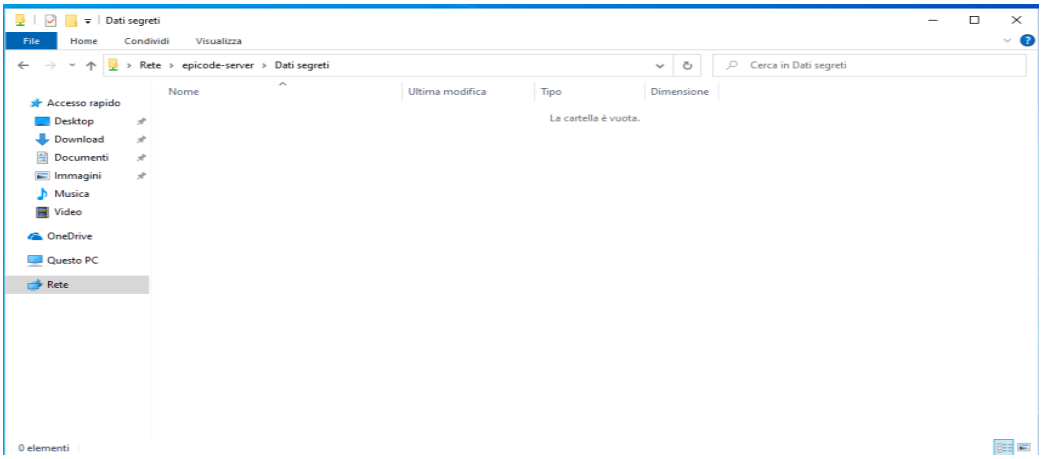

Fig. 9 - Verifica accesso positivo.

Risultato Test 2: Accesso Negato Il tentativo di accesso alla cartella **"Dati top"** è stato bloccato dal sistema operativo, che ha restituito un errore di autorizzazione. Ciò conferma che l'utente Chiara Bianchi, non appartenendo al gruppo *Hacker 1*, non possiede token di sicurezza validi per tale risorsa.

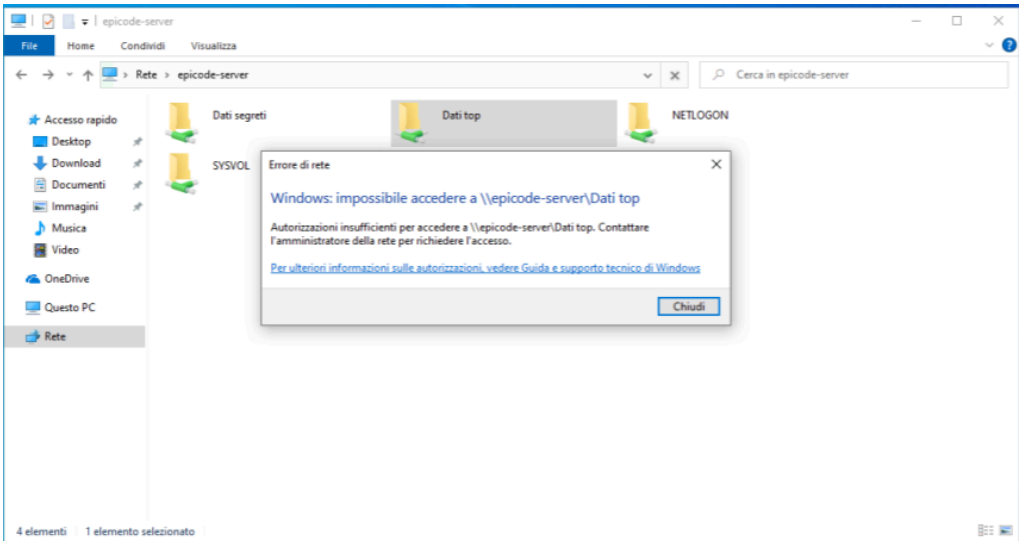

Fig. 10 - Verifica blocco accesso (Access Denied).

---

6. Conclusioni

L'esercitazione ha dimostrato la corretta applicazione del modello RBAC (Role-Based Access Control) in ambiente Windows Server 2022. La configurazione dei permessi ha impedito con successo l'accesso orizzontale non autorizzato, garantendo la riservatezza dei dati in base all'appartenenza ai gruppi di sicurezza definiti in Active Directory.