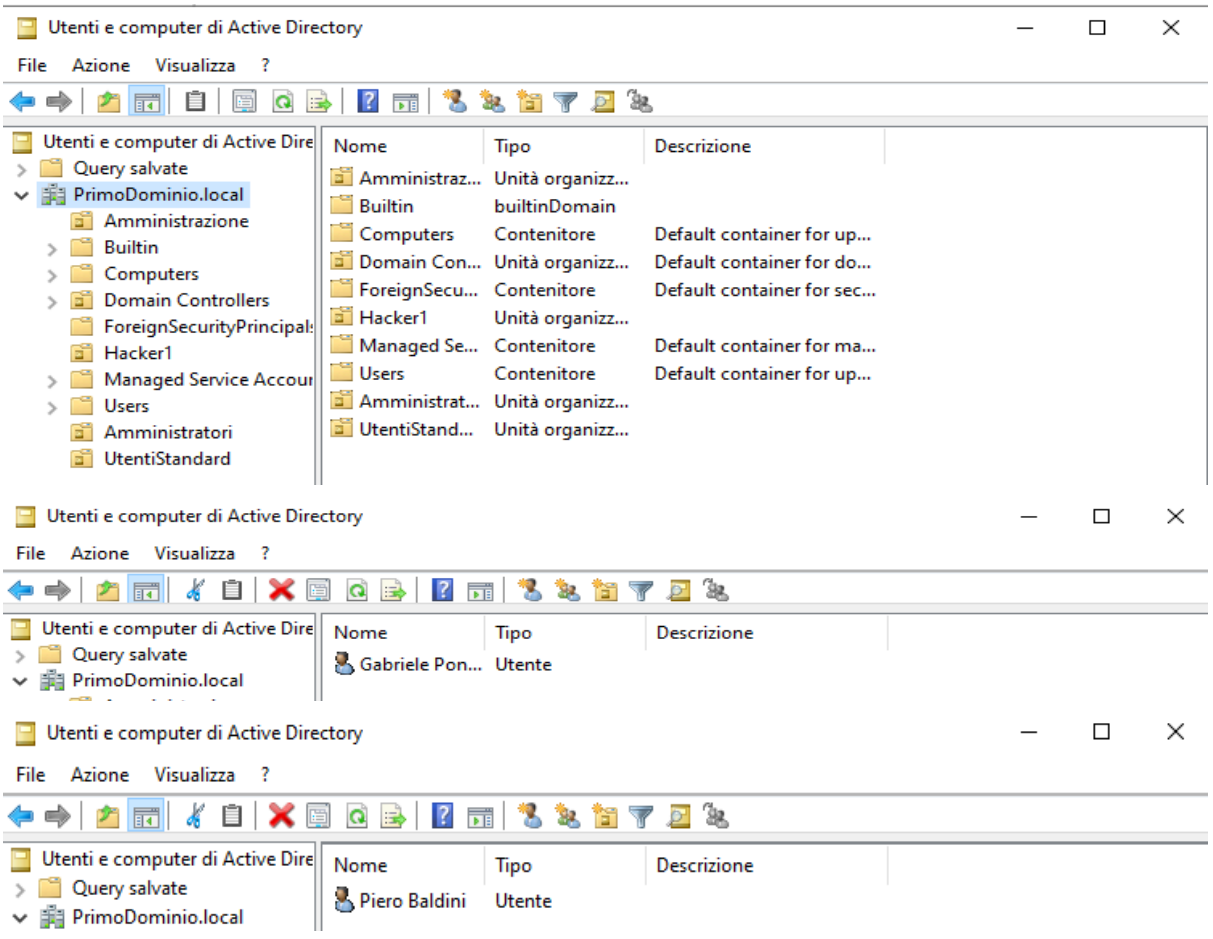
REPORT S10/L5

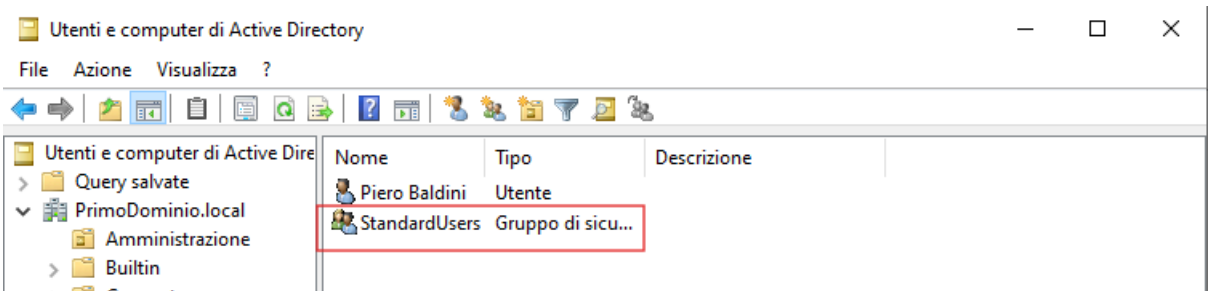
Obiettivo:Lo scopo di questo esercizio è di familiarizzare con la gestione dei gruppi di utenti in Windows Server 2022. Imparerai a creare gruppi, assegnare loro permessi specifici e comprendere l'importanza della gestione dei gruppi per la sicurezza e l'amministrazione del sistema.

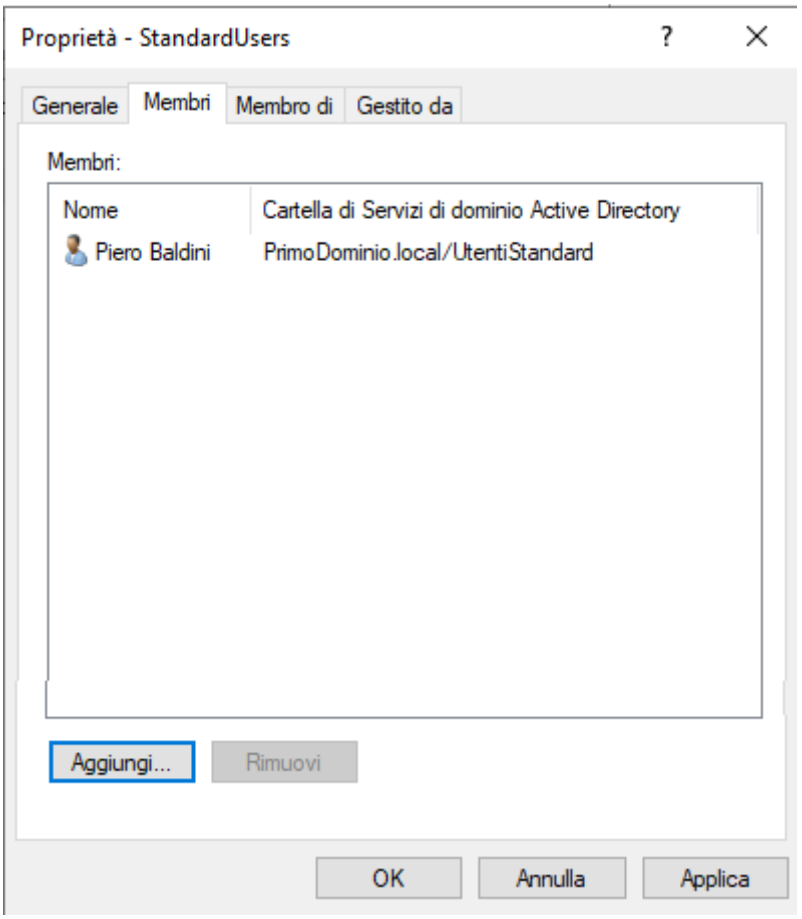
SVOLGIMENTO

Creazione dei gruppi

Ho creato due gruppi distinti: **Amministratori** e **UtentiStandard**. Successivamente, ho assegnato un utente a ciascun gruppo, Gabriele al gruppo Amministratori e Piero al gruppo UtentiStandard.

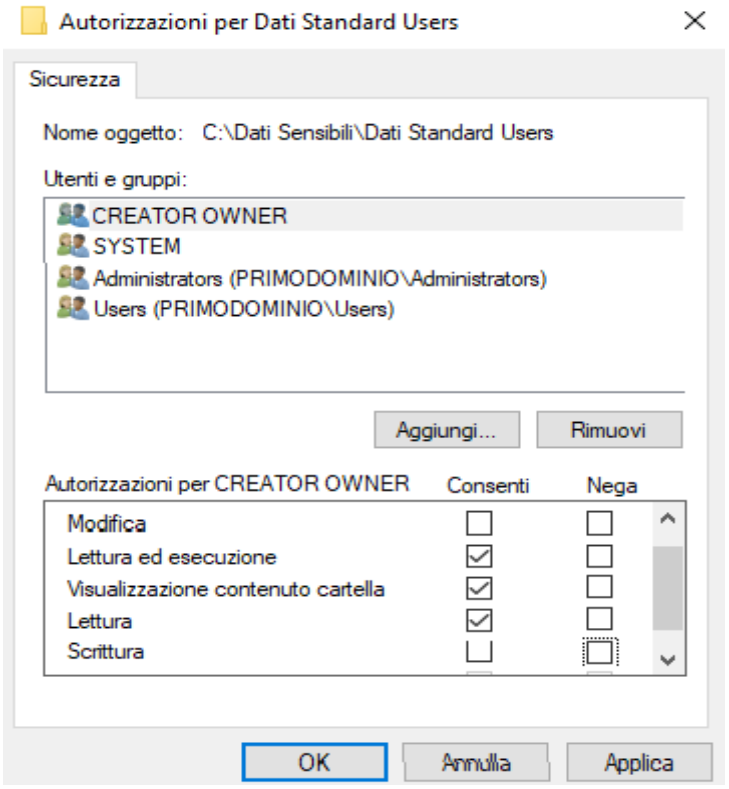


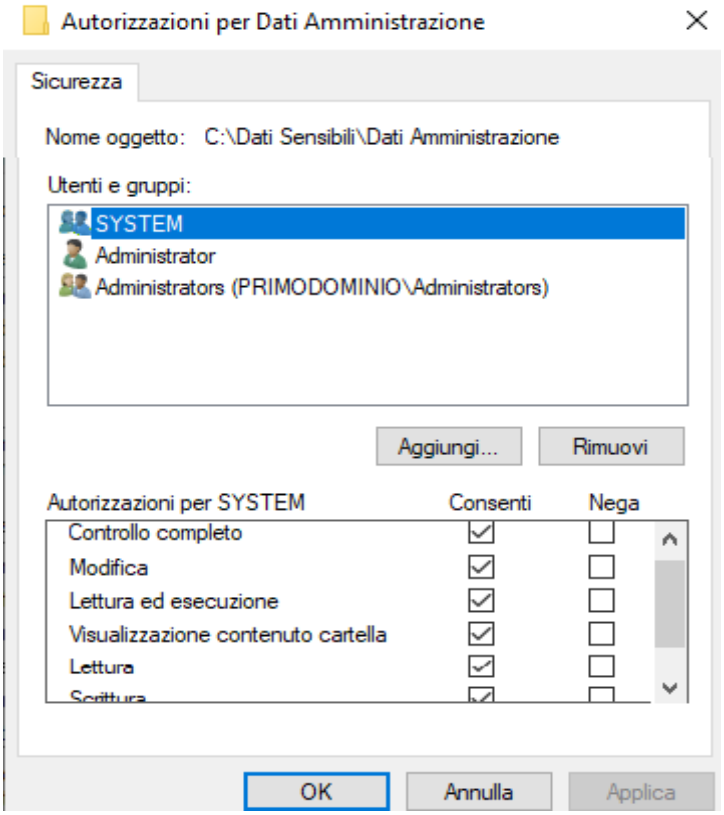

Utenti e computer di Active Directory
File
Azione
Visualizza
?
Utenti e computer di Active Dire
Query salvate
PrimoDominio.local
Amministrazione
Builtin
Nome
Tipo
Descrizione
Piero Baldini
Utente
StandardUsers
Gruppo di sicu...


Proprietà - StandardUsers
?
Generale
Membri
Membro di
Gestito da
Membri:
Nome
Cartella di Servizi di dominio Active Directory
Piero Baldini
PrimoDominio.local/UtentiStandard
Aggiungi...
Rimuovi
OK
Annulla
Applica

Assegnazione dei permessi

Ho assegnato permessi differenti ai due gruppi. Il gruppo Amministratori dispone di pieno controllo sul sistema, con la possibilità di gestire utenti, software e configurazioni, invece, il gruppo UtentiStandard ha accesso limitato per garantendo una maggiore sicurezza del sistema.





Problemi riscontrati

Ho avuto difficoltà nella verifica dei permessi degli utenti poiché non riuscivo a visualizzare la cartella condivisa dal PC dell'utente.
Purtroppo non sono riuscito a trovare una soluzione.

BONUS

Obiettivo:Lo scopo di questo esercizio è analizzare il seguente file di log con Splunk.

SVOLGIMENTO

Dall'analisi del file di log emergono diversi eventi sospetti, principalmente legati ad attività FTP potenzialmente malevole.

Accessi anonimi al server FTP

Sono stati rilevati numerosi tentativi di connessione anonima ai server FTP, utilizzando l'utente anonymous e l'indirizzo email IEUser@.
L'indirizzo IP di origine varia tra 192.168.203.45, 192.168.204.45 e altri appartenenti alla rete locale.
I messaggi di risposta del server confermano che l'accesso anonimo è consentito, ma con restrizioni minime.

Tentativi di cancellazione e upload di file

Sono stati rilevati numerosi tentativi di eliminazione (DELE) e archiviazione (STOR) di file in directory sospette, come `/.ftpduBnga4`, `/dept/env/` e `/dept/qdept/`. I tentativi sono stati negati (550 Operation not permitted) suggerendo che l'attaccante potrebbe non avere i permessi necessari, ma ha comunque cercato di alterare i file.

Uso dei comandi PORT e PASV

L'attaccante utilizza sia la modalità attiva (PORT) che passiva (PASV) per trasferire file, probabilmente nel tentativo di bypassare restrizioni firewall e controlli di sicurezza.

Remediations

Disabilitazione dell’Accesso Anonimo.
Modificare la configurazione del server FTP per impedire accessi anonimi e riavviare il servizio per applicare le modifiche.

Monitoraggio e Blocco dei Trasferimenti di File Sospetti
Utilizzare strumenti di monitoraggio per rilevare accessi FTP sospetti e configurare regole firewall per bloccare trasferimenti non autorizzati.

Regole di Accesso Restrittive per Cartelle Critiche
Limitare l’accesso alle cartelle sensibili con policy di gestione degli accessi.

Rafforzamento del Firewall e delle Restrizioni di Rete
Bloccare accessi FTP non autorizzati tramite firewall e consentire l’uso del protocollo FTP solo a utenti specifici e IP approvati.

Conclusione per i manager

Dall'analisi del log emergono diversi segnali di attività sospette tra cui accessi anonimi ai server FTP che rappresentano un rischio elevato di compromissione, tentativi di upload e cancellazione di file critici che indicano possibili attività malevole che potrebbero suggerire la distribuzione di malware.
Per prevenire questi rischi è fondamentale disabilitare gli accessi anonimi e rafforzare le policy di autenticazione, oltre a monitorare e bloccare i trasferimenti di file sospetti attraverso strumenti di analisi dei log. È inoltre necessario applicare restrizioni sui permessi delle directory FTP per impedire alterazioni non autorizzate.