# U3W2L5 – Progetto Settimanale

Gestione Identity, Permessi NTFS e Accesso Remoto (Scenario YoRHa)

**Autore**: Elena Pagnacco **Ambiente**: Windows Server 2022 (VirtualBox)

## Sintesi

Il presente report documenta l'attività di laboratorio svolta per configurare una gerarchia di sicurezza basata sui ruoli (***RBAC - Role Based Access Control***) in ambiente Windows Server 2022. Lo scenario simula il mainframe del "Bunker" di YoRHa, dove è necessario segregare rigorosamente i dati classificati riguardanti il Consiglio dell'Umanità. L'esercizio pone enfasi sul principio del "***Least Privilege***", sulla gestione dei gruppi Active Directory, sui permessi NTFS/SMB e sull'amministrazione remota.

## Scopo del test e Scenario

L'obiettivo è proteggere il file system del server ("Bunker Mainframe"), garantendo che le unità di ricognizione (Scanner) possano operare sui dati di missione, ma siano bloccate dall'accedere ai segreti di livello "SS" riservati al Comando o alle unità di Esecuzione.

### I Ruoli Identificati:

- **Comando (YoRHa_Command):** *Commander White*. Controllo totale e amministrativo.
- **Type E - Executioner (YoRHa_Executioners):** *Unit 2B*. Unità d'élite con privilegi di sicurezza elevati per monitorare le attività e accedere ai dati classificati "Top Secret". Deve poter amministrare il server da remoto.
- **Type S - Scanner (YoRHa_Scanners):** *Unit 9S*. Unità specialista in raccolta dati. Tenta di accedere agli archivi, ma i suoi permessi devono essere limitati ai soli dati operativi. Non deve avere accesso remoto.
- **Disertori (Unit A2):** Unità radiata dai registri. Il suo account deve essere disabilitato per impedire qualsiasi accesso.

---

## Configurazioni primarie

### Networking e Indirizzamento IP

Per garantire la stabilità del collegamento col server lunare (Bunker), è stata impostata una configurazione statica.

### Dettagli Configurazione:

- **Interfaccia di Rete:** Internal Network (intnet).
- **Indirizzo IP Server:** 192.168.50.2
- **DNS Server Primario:** 127.0.0.1 (Localhost)

## Analisi della scelta DNS (Loopback vs IP Statico)

Per il server stesso, l'indirizzo di loopback 127.0.0.1 è stato configurato come DNS primario al posto dell'indirizzo IP della scheda di rete (192.168.50.2).

Questa configurazione segue le **Best Practices Microsoft** per mitigare il cosiddetto **"Island Problem"** (problema dell'isola). Durante la fase di avvio del sistema operativo (boot), può verificarsi una "race condition" in cui i servizi critici di Active Directory tentano di avviarsi prima che lo stack di rete fisico sia completamente inizializzato.

- Se il server puntasse a 192.168.50.2 e l'interfaccia non fosse ancora pronta, la risoluzione dei nomi fallirebbe, impedendo la corretta registrazione dei **record SRV** necessari al dominio.
- Puntando a 127.0.0.1, il traffico DNS rimane interno allo stack software (sempre disponibile), garantendo stabilità e resilienza indipendentemente dallo stato del cavo di rete virtuale.

*Nota:* I futuri client della rete (*Unità Androidi*) utilizzeranno invece l'IP 192.168.50.2 come loro server DNS per poter risolvere il dominio.

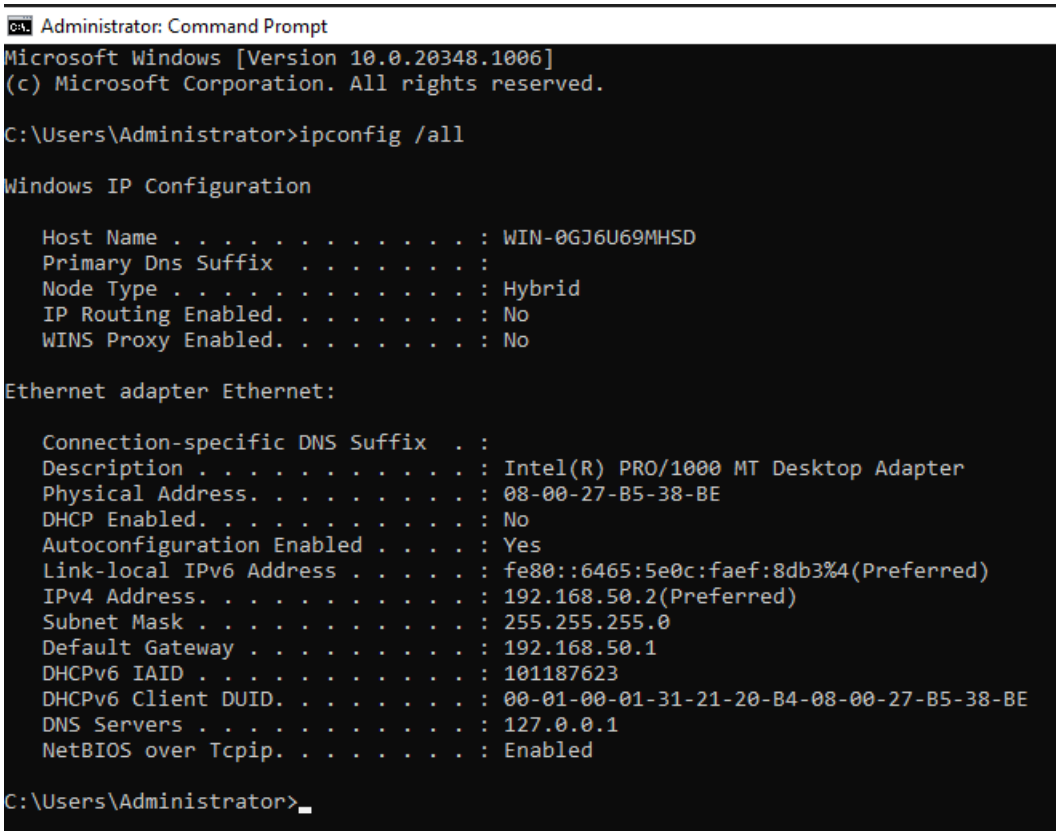


*Figura 1Verifica della configurazione di rete tramite riga di comando.*

# Configurazione Identificativo Sistema e Sincronizzazione Oraria

Prima di procedere con l'installazione dei ruoli server, sono state eseguite le configurazioni base per garantire la corretta identificazione e sincronizzazione del nodo nella rete.

## Dettagli Configurazione:

- **Hostname (Nome Computer):** Modificato da default a YoRHaBunkerServ.
    - *Motivazione:* Un naming convention coerente è essenziale per la gestione dei record DNS e per l'amministrazione remota.

- **Timezone e NTP:** Il fuso orario è stato allineato alla localizzazione corrente e l'orologio di sistema è stato sincronizzato.

### Analisi Critica (Il requisito Kerberos)

La sincronizzazione dell'orario è un prerequisito mandatorio per la promozione a Domain Controller. Il protocollo di autenticazione **Kerberos V5**, utilizzato da Active Directory, si basa su "timestamp" per prevenire attacchi di tipo *Replay Attack*. Se lo scostamento temporale (***Time Skew***) tra il Domain Controller e i futuri client superasse la soglia di tolleranza predefinita (solitamente **5 minuti**), i ticket di autenticazione verrebbero rifiutati, causando un disservizio totale (Denial of Service logico).


*Figura 2 Riepilogo delle impostazioni locali del server.*

---

# Configurazione dell'Infrastruttura (Identity & Access Management)

## Implementazione dell'Infrastruttura Identity (Active Directory)

In questa fase viene documentato il ***provisioning*** delle identità digitali e la strutturazione logica del dominio, necessarie per garantire l'autenticazione centralizzata e la gestione degli accessi basata sui ruoli (RBAC).

### Inizializzazione dei Servizi di Dominio (AD DS)

- **Procedura:** Server Manager > Manage > Add Roles and Features.
- **Configurazione:** Installazione del ruolo AD DS (**Active Directory Domain Services)** e promozione del server a **Domain Controller**.
- **Dominio:** Creazione della foresta **YoRHa.local**.

### Strutturazione Gerarchica (Organizational Units)

Per segregare le entità operative del Bunker e applicare future policy mirate, è stata creata una struttura logica dedicata.

- **Strumento:** Active Directory Users and Computers.
- **Oggetto creato:** Organizational Unit (OU) denominata **YoRHa_Forces**.

## Provisioning delle Identità e Ruoli (User Accounts & Groups)

All'interno della Organizational Unit (OU) dedicata YoRHa_Forces, sono stati creati i gruppi di sicurezza globale per mappare i ruoli operativi:

1. **Commander White** (Membro di YoRHa_Command): Privilegi amministrativi.
2. **Unit 2B** (Membro di YoRHa_Executioners): Unità operativa Type-E.
3. **Unit 9S** (Membro di YoRHa_Scanners): Unità di ricognizione.
4. **Unit A2** (Disertore): Account creato e impostato su **Disabled**, simulando la revoca dei certificati.

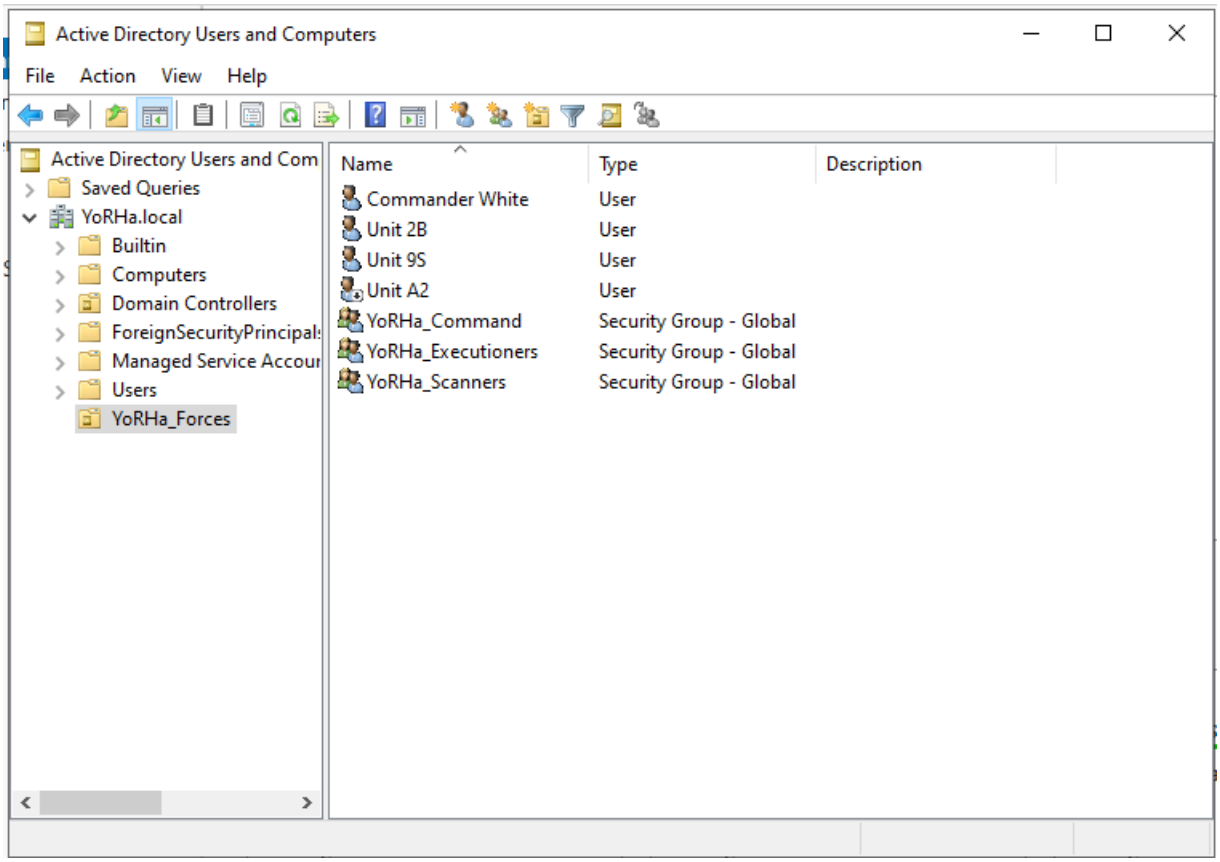


*Figura 3 Visualizzazione della OU YoRHa_Forces con i gruppi creati e l'utente A2 disabilitato (icona con freccia in basso).*

---

# Configurazione Risorse e Permessi (File System)

## Creazione Root Directory e Permessi NTFS (ACL)

In questa fase si definiscono le Access Control List (ACL) per le risorse condivise, applicando i permessi a livello di file system NTFS per garantire la sicurezza locale.

## Creazione Root Directory

- **Percorso:** C:\Bunker_Archives
- **Azione:** Creazione cartella e rimozione dei permessi ereditati di default (es. Users), mantenendo solo gli amministratori e i gruppi specifici.

## Assegnazione Permessi (DACL)

Tramite la scheda *Security* > *Edit*, sono stati assegnati i seguenti privilegi ai gruppi creati in Fase 1:

- **SYSTEM / Administrators: Full Control**.
- **YoRHa_Command: Full Control** (Gestione totale archivio).
- **YoRHa_Executioners (2B): Modify** (Lettura, Scrittura, Modifica).
- **YoRHa_Scanners (9S): Modify** (Lettura, Scrittura, Modifica).

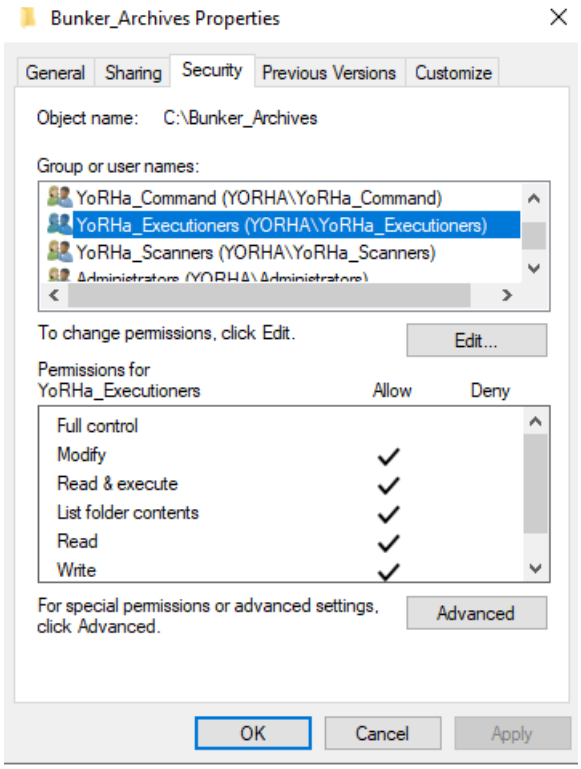


*Figura 4 Finestra delle proprietà di sicurezza che mostra i gruppi YoRHa aggiunti e i relativi permessi.*

## Pubblicazione della Risorsa in Rete (SMB Sharing)

La risorsa è stata condivisa in rete per permettere l'accesso dalle postazioni remote.

- **Nome Condivisione: Bunker_Archives**
- **Percorso di Rete:** \\YoRHaBunkerServ\Bunker_Archives
- **Permessi di Condivisione (Share Permissions):**
    - *Everyone:* Rimosso.
    - *YoRHa_Executioners / YoRHa_Scanners:* Change (Lettura/Scrittura).
    - *YoRHa_Command:* Full Control.

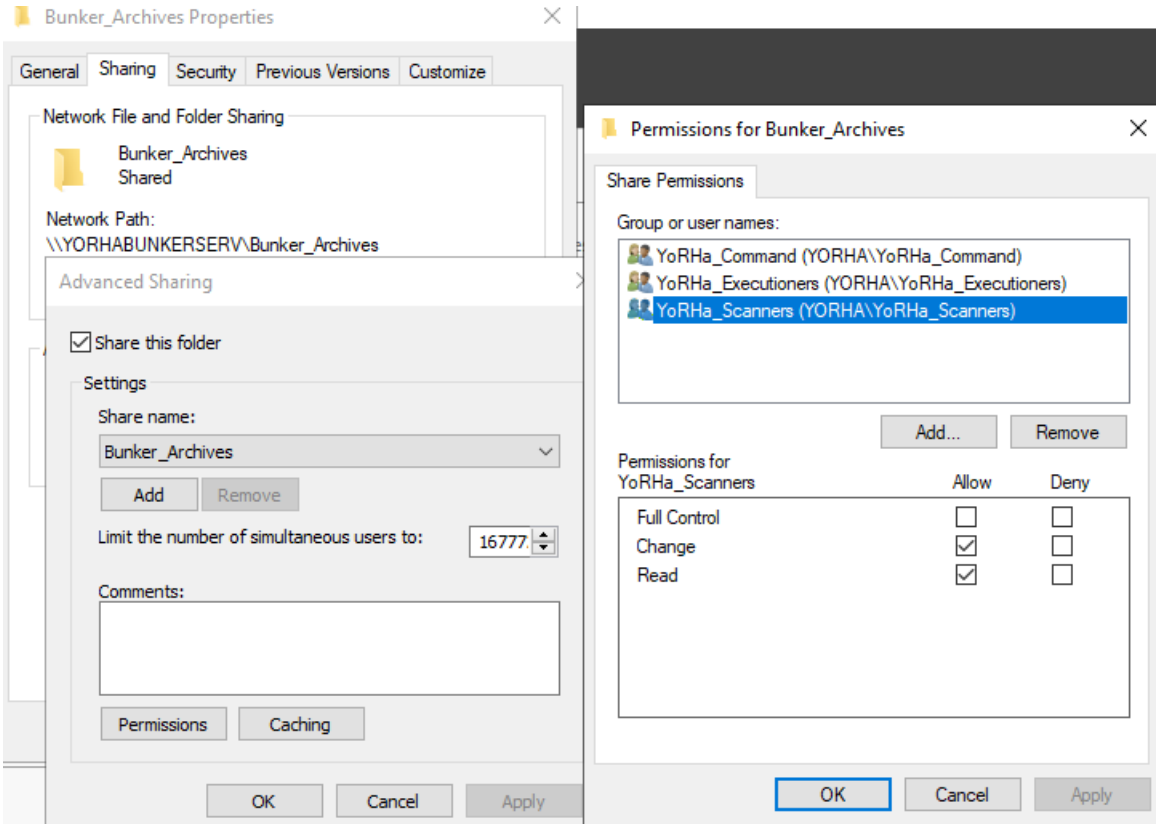


*Figura 5 Finestra delle proprietà di sharing che mostra i gruppi YoRHa aggiunti e i relativi permessi*

## Hardening e Segregazione Dati

All'interno dell'archivio è stata creata la sottocartella critica **Top_Secret_Truth**, contenente il file riservato ***[SS-Confidential]_YoRHa_Disposal_Plan.txt.***

Per proteggere questa risorsa, è stata implementata la **rottura dell'ereditarietà (Inheritance Blocking)** dei permessi NTFS:

1. **Azione:** Disabilitazione ereditarietà sulla cartella segreta.
2. **Modifica ACL:** Si è proceduto a revocare i permessi per il gruppo ***YoRHa_Scanners***.
3. **Risultato:** L'accesso per l'unità 9S risulta ora **negato**, mentre solo il gruppo ***YoRHa_Executioners*** mantiene il permesso *Modify* esplicito per la gestione dei file sensibili.

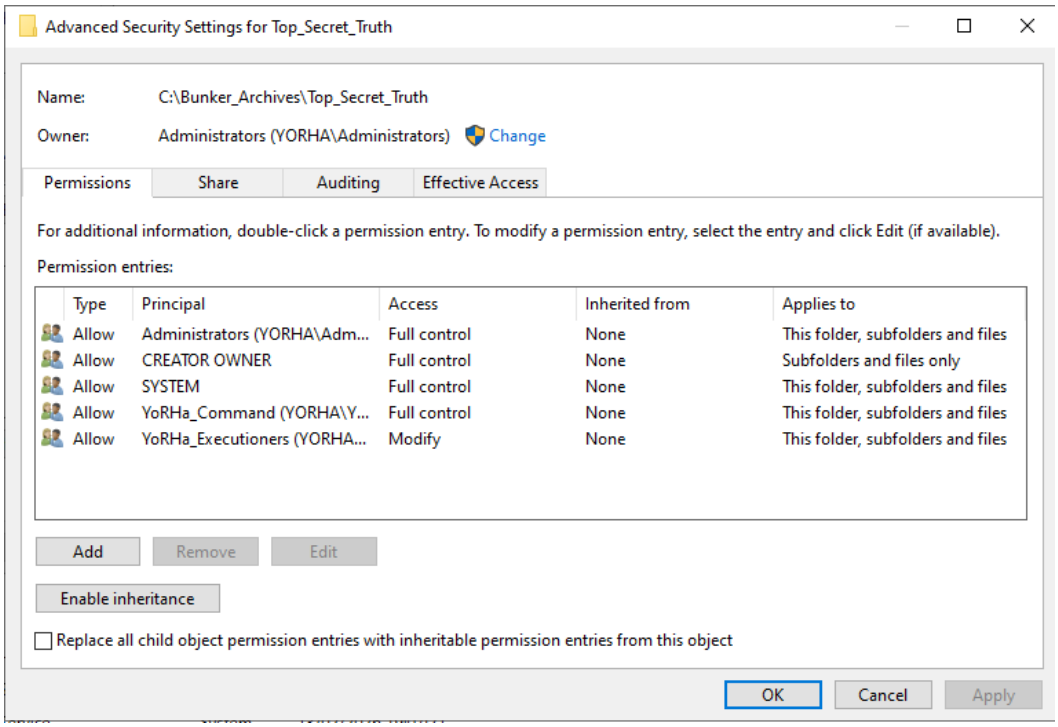


*Figura 6 Finestra "Advanced Security Settings" della cartella segreta. Evidenziata l'assenza del gruppo Scanners e la presenza del gruppo Executioners*

---

# Configurazione Accesso Remoto (RDP)

Per differenziare i privilegi di amministrazione, è stato configurato l'accesso tramite Desktop Remoto.

- **Gruppo YoRHa_Executioners:** Aggiunto manualmente al gruppo locale **"Remote Desktop Users"**.
- **Gruppo YoRHa_Scanners:** Escluso dal gruppo RDP.

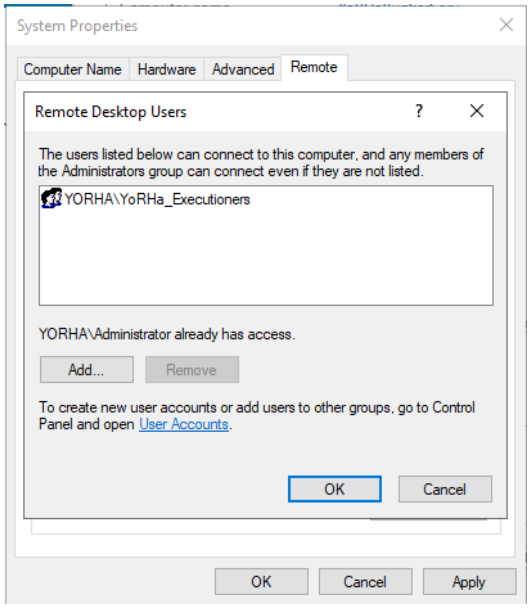


*Figura 7 Mapping del gruppo YoRHa_Executioners all'interno dei privilegi di accesso remoto del Bunker.*

---

# Configurazione Terminale Operativo (Windows 10 Pro N)

## Integrazione Client nell'Infrastruttura

È stata configurata una macchina virtuale client (Terminale di Campo) per simulare l'accesso degli androidi.

### Impostazioni di Rete e Risoluzione DNS

- **Interfaccia di Rete:** Internal Network (intnet).
- **Indirizzo IP Client:** 192.168.50.30 (Statico).
- **Server DNS Primario:** 192.168.50.2 (IP del "Bunker Mainframe").

## Analisi Critica (La Risoluzione DNS del Client)

Il client deve obbligatoriamente interrogare il server al 192.168.50.2. Se il DNS venisse lasciato in DHCP automatico o su un resolver pubblico (es. 8.8.8.8), il client non sarebbe in grado di risolvere il dominio privato YoRHa.local.

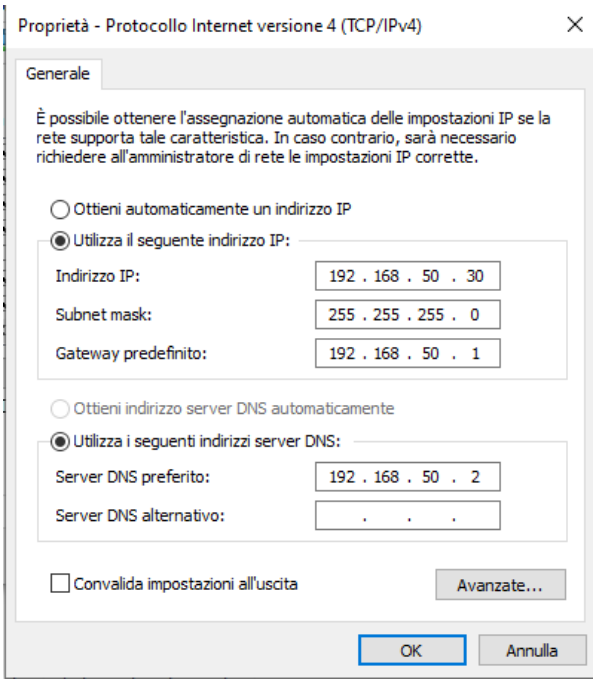


*Figura 8 Impostazioni scheda di rete IPv4 di Windows 10 Pro N con IP e DNS configurati*

## Join al Dominio (Integrazione in Active Directory)

- **Hostname:** YoRHa-T-01 (Terminal).
- **Dominio:** YoRHa.local.
- **Autorizzazione:** Credenziali di Commander White utilizzate per il join.

---

# Validazione e Testing (Proof of Concept)

La configurazione è stata verificata simulando le azioni degli utenti target.

## Test A: Efficacia della Segregazione (Unit 9S)

- **Scenario:** L'unità Scanner accede a \\YoRHaBunkerServ\Bunker_Archives e tenta di aprire la cartella Top_Secret_Truth.
- **Risultato:** Il sistema blocca l'accesso con errore: *"Network Access is denied" / "You do not have permission to access this folder"*.
- **Esito: SUCCESSO**.

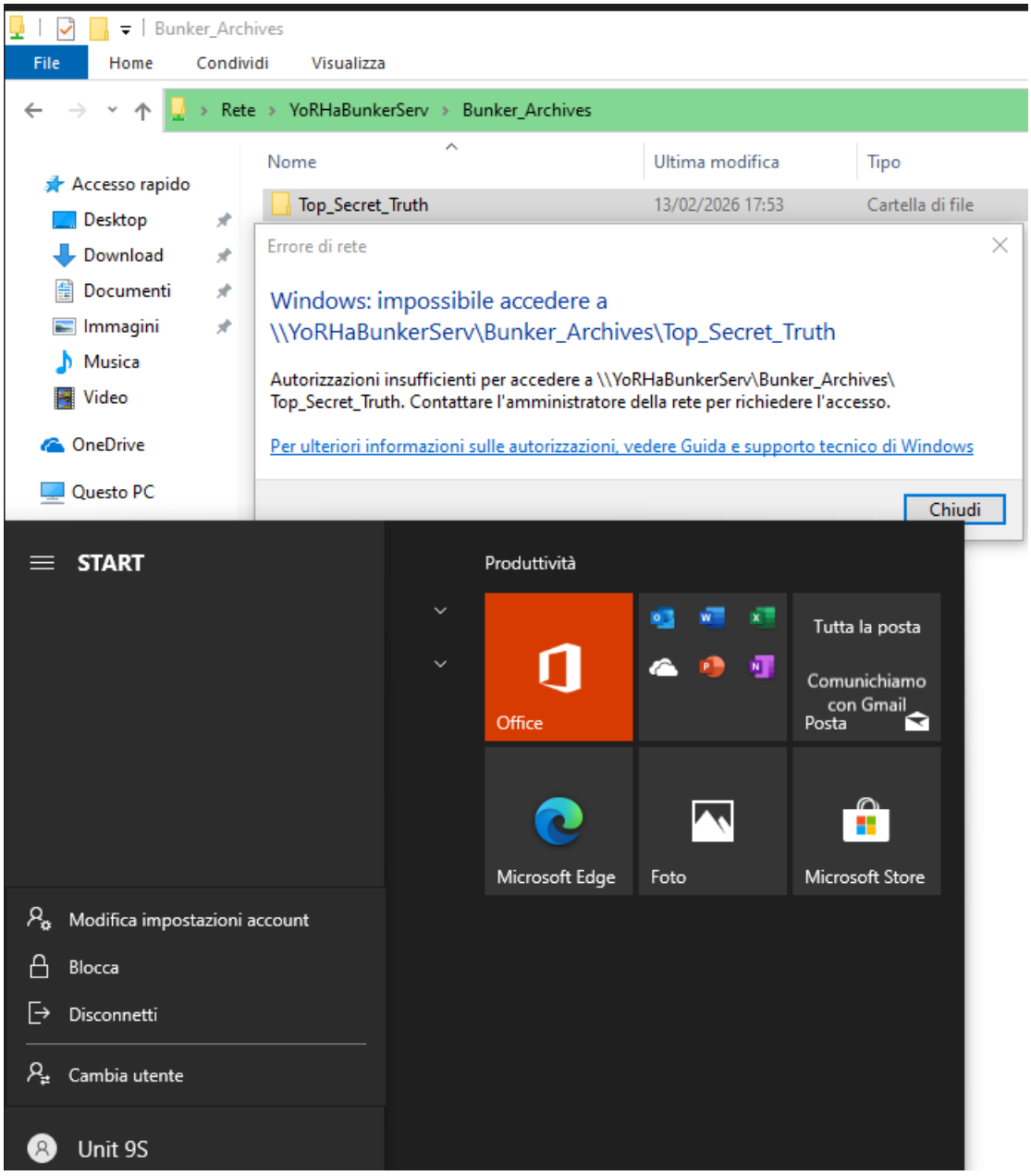


*Figura 9 Errore Access Denied per 9S*

## Test B: Verifica Privilegi Esecutivi (Unit 2B)

- **Scenario:** L'unità Executioner accede alla medesima cartella.
- **Risultato:** Accesso consentito. L'utente apre la cartella e visualizza la presenza del file [SS-Confidential]_YoRHa_Disposal_Plan.txt.

- **Esito: SUCCESSO**.

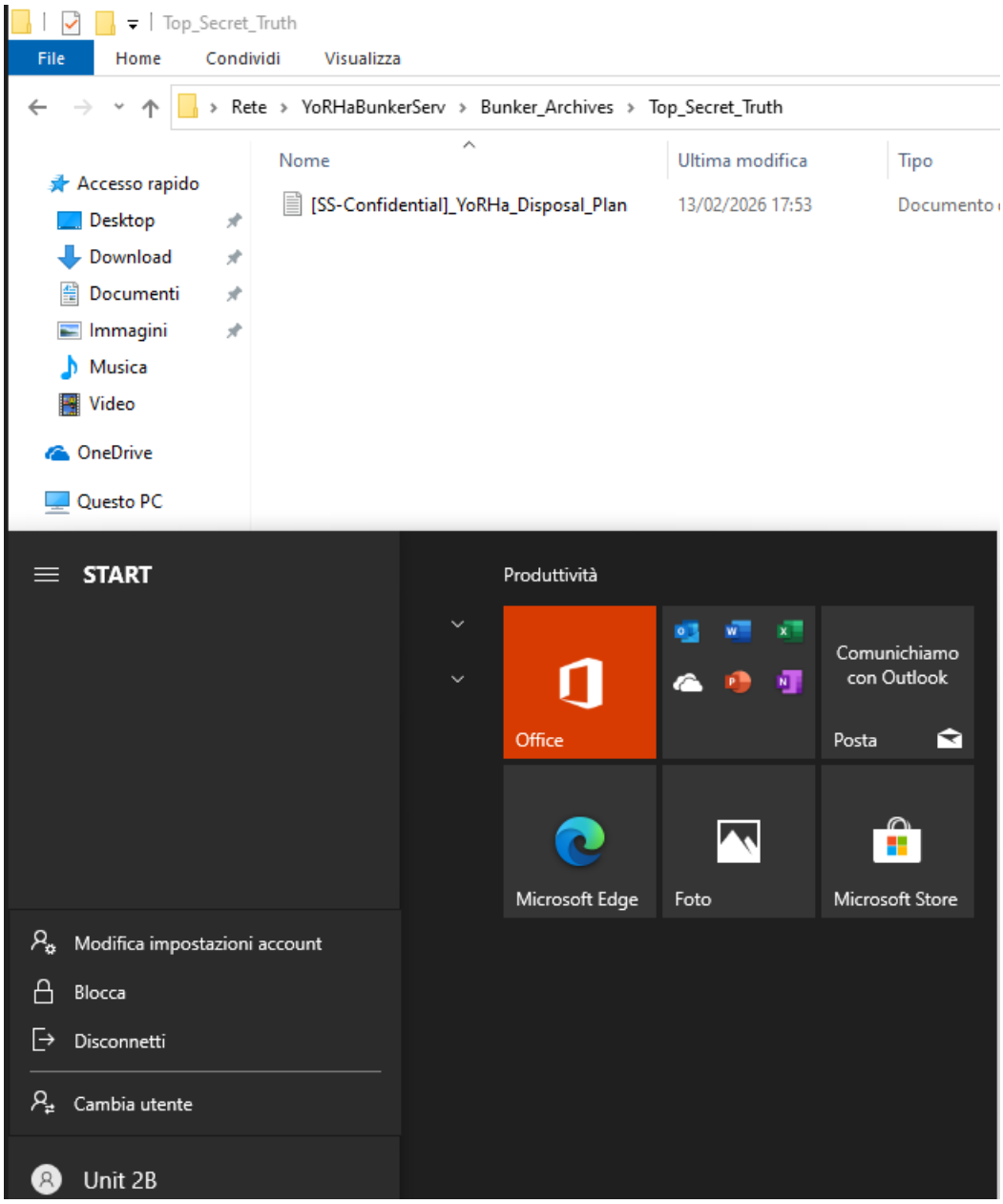


*Figura 10 Visualizzazione del file di testo contenente i dettagli sul protocollo di smaltimento YoRHa.*

## Test C: Verifica Blocco Account (Unit A2)

- **Scenario:** Tentativo di login al dominio da parte dell'unità disertrice.
- **Risultato:** Autenticazione fallita: *"Your account has been disabled. Please see your system administrator."*
- **Esito: SUCCESSO**.

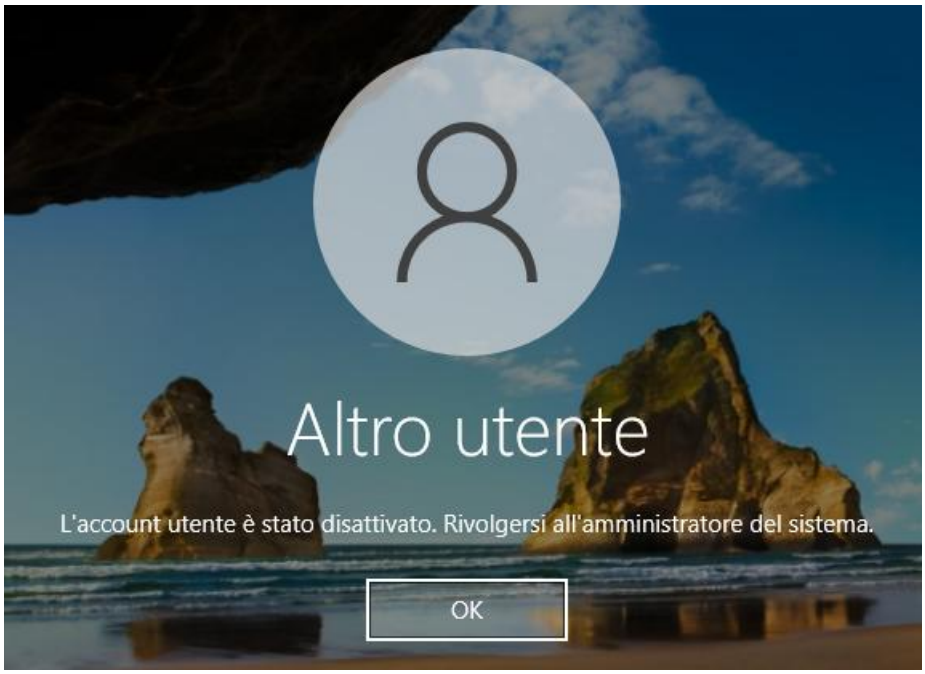


*Figura 11 Errore Login Account Disabilitato*

---

# Risoluzione Problemi (Troubleshooting)

Durante la fase di validazione finale (Proof of Concept), è emersa una criticità che ha richiesto interventi correttivi.

## Problema: Visibilità della risorsa negata (Information Disclosure)

- **Sintomo:** Durante il Test A, l'unità 9S riceveva correttamente l'errore "Accesso Negato" tentando di entrare nella cartella, ma poteva ancora **visualizzare l'icona e il nome** della cartella Top_Secret_Truth all'interno della condivisione di rete.
- **Diagnosi:** Questo comportamento costituisce un rischio di sicurezza: la semplice esistenza della cartella rivela che ci sono dati nascosti. La causa è che la funzionalità **ABE (Access-Based Enumeration)** è disabilitata di default in Windows Server. Senza ABE, il sistema mostra l'elenco completo delle cartelle anche agli utenti che non hanno i permessi per aprirle.
- **Soluzione:** È stata attivata l'enumerazione basata sull'accesso (ABE) per filtrare la visibilità delle risorse in base ai permessi dell'utente.
    - *Procedura:*
        1. In **Server Manager**, navigare su *File and Storage Services -> Shares*.
        2. Selezionare la condivisione **Archives**, cliccare col tasto destro e scegliere *Properties*.
        3. Nella sezione *Settings*, attivare la spunta su **Enable access-based enumeration**.
- **Verifica:** La cartella Top_Secret_Truth è risultata completamente invisibile al gruppo Scanners, apparendo a Executioners e Command.

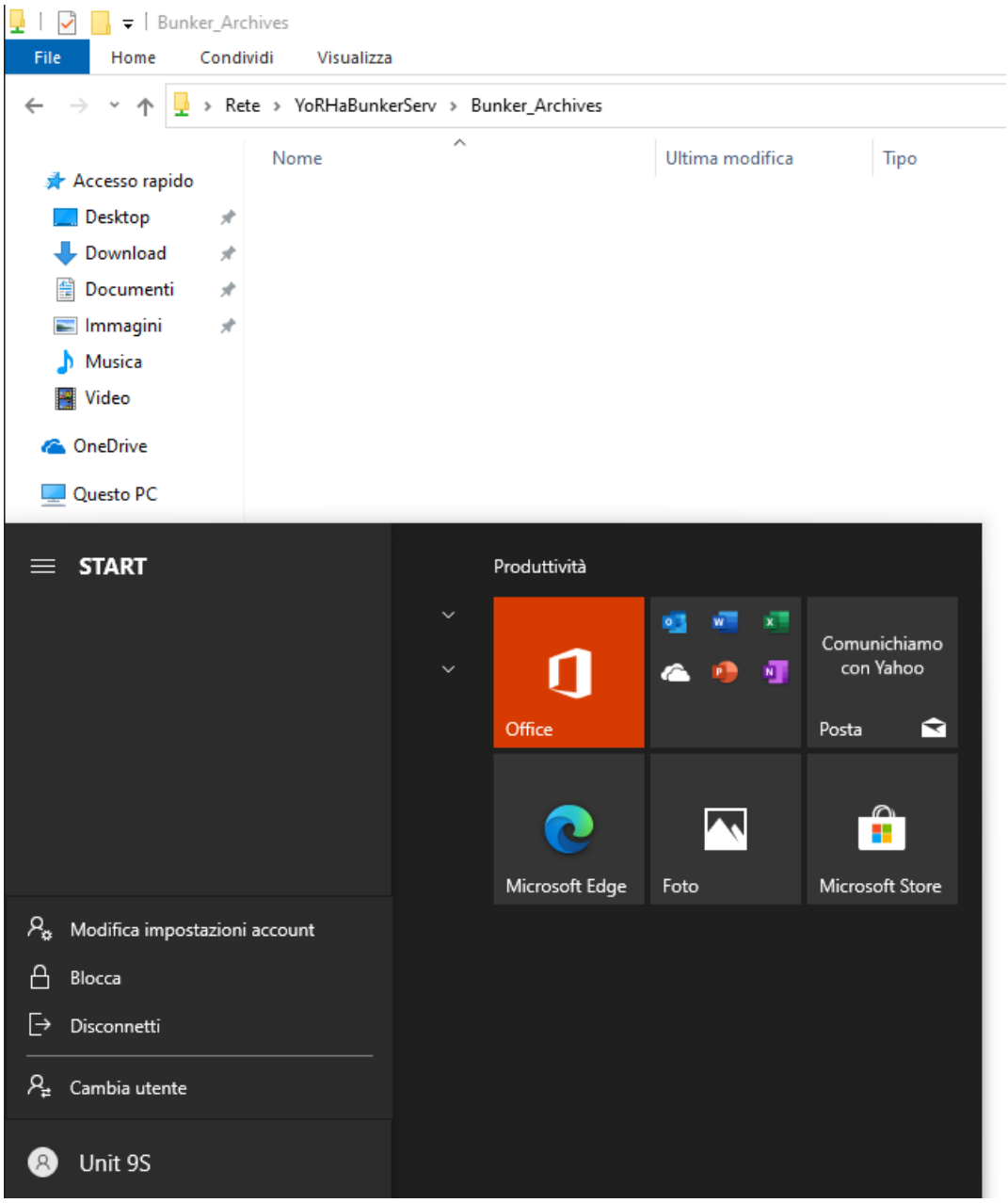


*Figura 12 Cartella Top_Secret_Truth completamente invisibile per il gruppo YoRHa_Scanners*

# Conclusioni

L'infrastruttura di sicurezza implementata rispecchia i requisiti operativi del Bunker. L'uso combinato di permessi di condivisione (SMB) aperti e permessi NTFS restrittivi, unito all'attivazione dell'ABE, garantisce la massima sicurezza e la corretta segregazione dei ruoli (SoD).