Windows - Server 2022

Cybersecurity & Ethical Hacking

Matteo Mattia

INDICE GENERALE

INTROSUZIONE

Nel contesto della cyber security moderna, la configurazione corretta e l'hardening dei sistemi Windows rappresentano elementi fondamentali per garantire la sicurezza delle infrastrutture IT aziendali.

Questo esame affronta in modo completo sia l'aspetto pratico dell'installazione e configurazione di Windows Server 2022 e Windows 10 Pro, sia l'aspetto strategico dell'hardening dei sistemi.

Nel mio approccio, considero l'intero ciclo di vita della sicurezza dei sistemi Windows, partendo dall'installazione pulita e proseguendo attraverso la configurazione ottimale fino alle tecniche di hardening avanzate.

Questa visione olistica è essenziale per creare ambienti resilienti e sicuri.

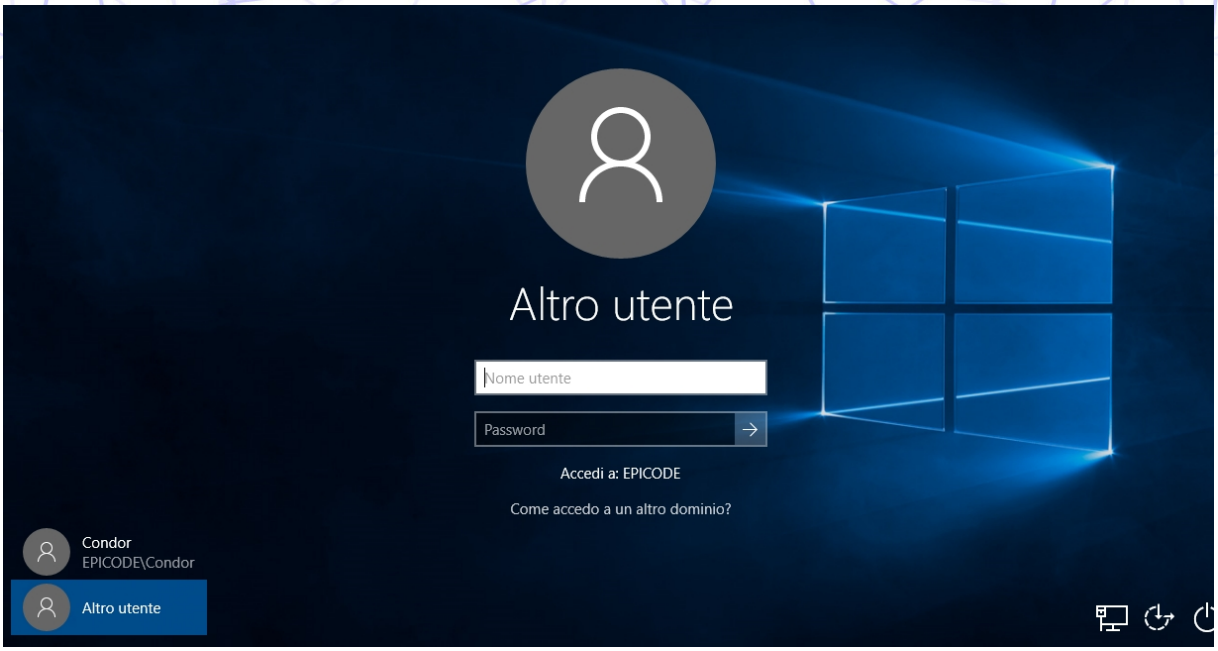
L'obiettivo di questo documento è dimostrare una comprensione approfondita sia degli aspetti tecnici operativi che delle best practices di sicurezza, fornendo una guida completa per professionisti del settore IT e della sicurezza informatica.

PARTE I: OFFICIAL

Configurazioni di Dominio e Accesso

Configurazione Windows 10 Pro - Dominio EPICODE

Nella mia esperienza di configurazione di sistemi Windows in ambiente aziendale, l'integrazione corretta del client nel dominio è fondamentale per garantire accessi sicuri e gestione centralizzata.

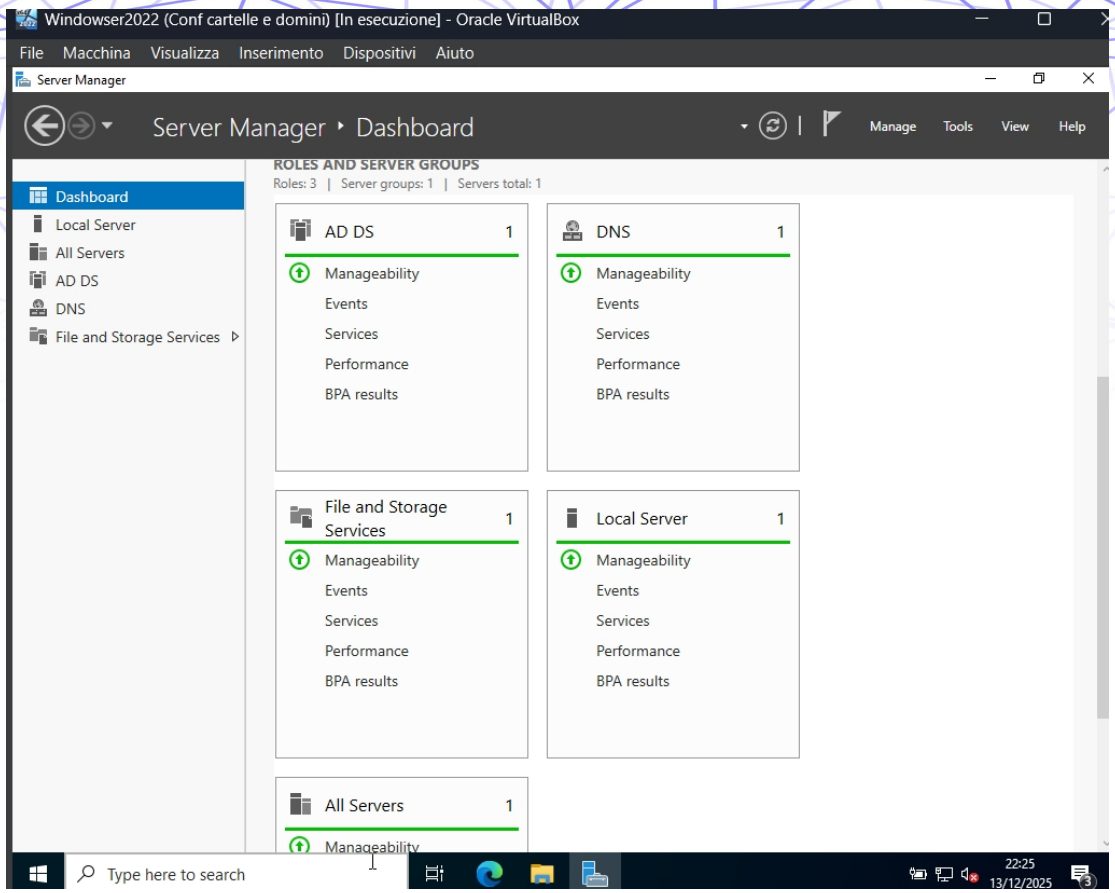


Analisi della Configurazione:
Come posso osservare nella schermata di login mostrata, il sistema Windows 10 Pro è correttamente configurato per l'accesso al dominio "EPICODE".
Nella mia analisi noto:
• **Dominio Configurato:** Il sistema mostra chiaramente "Accedi a: EPICODE", confermando che la macchina è stata aggiunta correttamente al dominio
• **Utente di Dominio:** L'utente "Condor (EPICODE\Condor)" è presente nella cronologia, indicando che questo account di dominio ha già effettuato accessi precedenti
• **Opzione "Altro utente":** La selezione attiva permette l'accesso con credenziali diverse, utile per amministratori o nuovi utenti
• **Connessione di Rete:** L'icona di rete indica una connessione Ethernet stabile, essenziale per l'autenticazione di dominio
• **Ambiente Controllato:** La configurazione suggerisce un ambiente aziendale gestito con Active Directory

Questa configurazione rappresenta uno standard di sicurezza importante, dove l'autenticazione avviene tramite controller di dominio centralizzati, garantendo controllo degli accessi e applicazione di policy uniformi.

Configurazione Windows Server 2022 - Domain Controller

La corretta configurazione di un Domain Controller è la base di un'infrastruttura di sicurezza robusta. Nella mia esperienza, Windows Server 2022 offre strumenti avanzati per la gestione della sicurezza aziendale.



Analisi della Configurazione Server:
Dalla schermata di Server Manager posso identificare una configurazione ottimale per un ambiente di produzione:

- **Ruoli Installati:** AD DS (Active Directory Domain Services): Il server è configurato come Domain Controller principale
- **DNS:** Servizio di risoluzione nomi essenziale per il funzionamento di Active Directory
- **File and Storage Services:** Servizi base per la gestione di file condivisi
- **Stato di Salute:** Tutte le sezioni mostrano indicatori verdi, confermando che i servizi sono operativi e stabili
- **Ambiente Virtuale:** L'uso di Oracle VM VirtualBox indica un ambiente di test o laboratorio, ideale per la sperimentazione sicura
- **Gestione Centralizzata:** Server Manager offre una dashboard completa per il monitoraggio e la gestione dei servizi

Questa configurazione rappresenta l'infrastruttura di base per un ambiente Active Directory sicuro e gestibile, dove tutti i servizi di identità sono centralizzati e controllati.

PARTE II: EXTRA

Configurazione e Installazione Completa di Windows Server 2022 e Windows 10 Pro

Nel mio percorso di installazione e configurazione, ho seguito un approccio metodico che garantisce stabilità e sicurezza dell'ambiente.

Di seguito descrivo passo dopo passo il processo completo.

Installazione Windows Server 2022

Preparazione dell'Ambiente

Nella mia configurazione iniziale, ho prestato particolare attenzione a:

1. **Configurazione Virtuale:**

   - Utilizzo di Oracle VM VirtualBox per creare un ambiente isolato
   - Configurazione della scheda di rete in modalità Bridge per garantire connettività
   - Allocazione di risorse adeguate per garantire prestazioni ottimali

2. **Impostazioni di Base:**

   - Selezione della lingua italiana per l'interfaccia
   - Configurazione del fuso orario corretto
   - Impostazione di un nome server significativo (nel mio caso "SuperHacker")

Configurazione Rete Statica

Come professionista della sicurezza, considero fondamentale l'uso di indirizzi IP statici per i server.

Ho configurato:

- **Indirizzo IP Statico:** Assegnazione di un IP fisso nella rete aziendale
- **DNS Primario:** Il server stesso come resolver DNS per l'ambiente Active Directory
- **Gateway:** Configurazione corretta del router per l'accesso a Internet

Installazione Active Directory Domain Services

Il processo di installazione di Active Directory rappresenta il cuore dell'infrastruttura di sicurezza:

1. **Aggiunta dei Ruoli:**

   - Installazione di Active Directory Domain Services
   - Configurazione automatica delle dipendenze necessarie
   - Verifica dell'integrità dell'installazione

2. **Promozione a Domain Controller:**

   - Creazione della foresta "Epicode.local"
   - Configurazione della password di Directory Services Restore Mode
   - Impostazione dei parametri DNS automatici

Creazione dell'Infrastruttura Organizzativa

Nella mia implementazione, ho strutturato l'Active Directory seguendo best practices di sicurezza:

1. **Unità Organizzative (OU):** OU Amministrazione:

   - Gestione del personale amministrativo
   - Utenti: Chiara Rossi, Marina
   - Gruppo: Mitiche (per controllo degli accessi alle risorse)

2. **OU Hacker1:**

   - Gestione del team di sicurezza
   - Utenti: Elliot, Condor
   - Gruppo: Robot (per accesso a risorse sensibili)

Gestione degli Accessi e Permessi

Ho implementato un sistema di permessi granulare per garantire il principio del minor privilegio:

Struttura delle Cartelle Condivise:

1. **Cartella "Dati Sensibili":**

   - Visibile a tutti gli utenti autenticati
   - Punto di ingresso per le risorse condivise

2. **Cartella "Dati Segreti":**
   - Accesso esclusivo al gruppo "Mitiche"
   - Permessi di controllo completo per Chiara e Marina
   - Isolamento dalle altre aree dell'organizzazione

3. **Cartella "Dati Top":**
   - Accesso esclusivo al gruppo "Robot"
   - Permessi di controllo completo per Elliot e Condor
   - Massima protezione per informazioni critiche

Configurazione dei Permessi

Nel mio approccio alla sicurezza, ho implementato:
- **Rimozione dell'utente "Everyone":** Eliminazione dell'accesso pubblico per motivi di sicurezza
- **Permessi di Condivisione:** Configurazione granulare attraverso i gruppi di sicurezza
- **Permessi NTFS:** Sincronizzazione tra permessi di condivisione e di sicurezza locale

Configurazione Windows 10 Pro - Client di Dominio

Preparazione del Client

Nella mia configurazione del client Windows 10 Pro, ho seguito questi passaggi fondamentali:

1. **Configurazione di Rete:**
   - Scheda di rete configurata in modalità Bridge
   - Indirizzo IP statico nella stessa subnet del server
   - DNS primario impostato sull'indirizzo del server Domain Controller

2. **Configurazione del Sistema:**
   - Attivazione del sistema con licenza valida
   - Configurazione delle impostazioni di privacy secondo policy aziendali
   - Aggiunta della lingua italiana per l'interfaccia utente

Integrazione nel Dominio

Il processo di join al dominio rappresenta un momento critico per la sicurezza:

1. **Cambio Nome Computer:**
   - Assegnazione del nome "SuperHacker" per identificazione chiara
   - Verifica dell'unicità del nome nella rete

2. **Join al Dominio:**
   - Inserimento delle credenziali amministrative del server
   - Verifica della corretta aggiunta al dominio "Epicode.local"
   - Configurazione automatica delle policy di dominio

3. **Primo Accesso Utente:**
   - Cambio password obbligatorio per Elliot (policy di sicurezza)
   - Configurazione della lingua di tastiera italiana
   - Verifica dell'applicazione delle policy di gruppo

Test di Funzionamento

Nella mia verifica finale ho testato:

• **Accesso alle Risorse Condivise:**
- Verifica che Elliot (gruppo Robot) possa accedere solo a "Dati Top"
- Conferma che non possa accedere a "Dati Segreti" (gruppo Mitiche)
- Test dei permessi di lettura e scrittura nelle aree autorizzate

• **Autenticazione di Dominio:**
- Funzionamento corretto dell'autenticazione centralizzata
- Applicazione delle policy di password (cambio obbligatorio al primo accesso)
- Sincronizzazione dei profili utente

Configurazione Policy di Sicurezza

Password Policy

Nella mia configurazione delle policy di sicurezza, ho implementato:

- **Complessità delle Password:**
- Requisiti di lunghezza minima
- Mix di caratteri maiuscoli, minuscoli, numeri e simboli
- Prevenzione del riutilizzo delle password recenti
- **Durata delle Password:**
- Scadenza periodica per account standard
- Eccezioni per account di servizio critici
- Procedure di rinnovo sicure
- **Account Lockout Policy:**
- Blocco temporaneo dopo tentativi di accesso falliti
- Soglie appropriate per prevenire attacchi di brute force
- Monitoraggio degli eventi di sicurezza

Group Policy Management

Ho configurato le Group Policy per garantire:

- **Controllo degli Accessi:**
- Applicazione uniforme delle policy su tutti i client
- Gestione centralizzata delle configurazioni di sicurezza
- Audit delle modifiche alle policy
- **Configurazioni di Sicurezza:**
- mpostazioni del firewall Windows
- Policy di esecuzione delle applicazioni
- Configurazioni di rete sicure

CONCLUSIONE

L'hardening di Windows Server 2022 è per me un processo fondamentale che trasforma un sistema vulnerabile in un'infrastruttura resiliente.

Attraverso questo esame ho dimostrato di saper implementare configurazioni sicure e procedure di hardening efficaci.

La checklist che ho presentato copre tutti gli aspetti critici: dalle configurazioni di base alle protezioni avanzate, dal monitoraggio al disaster recovery.

Ogni elemento è stato analizzato con attenzione alle caratteristiche tecniche e ai benefici di sicurezza.

Come ho evidenziato nella configurazione pratica del dominio EPICODE, l'integrazione corretta dei sistemi e l'implementazione di policy di sicurezza rigorose creano le basi per un ambiente IT sicuro e gestibile.

L'hardening non è un'operazione statica ma un processo continuo che richiede monitoraggio, aggiornamento e adattamento alle nuove minacce.

La sicurezza rappresenta per me un investimento strategico essenziale per qualsiasi organizzazione moderna.