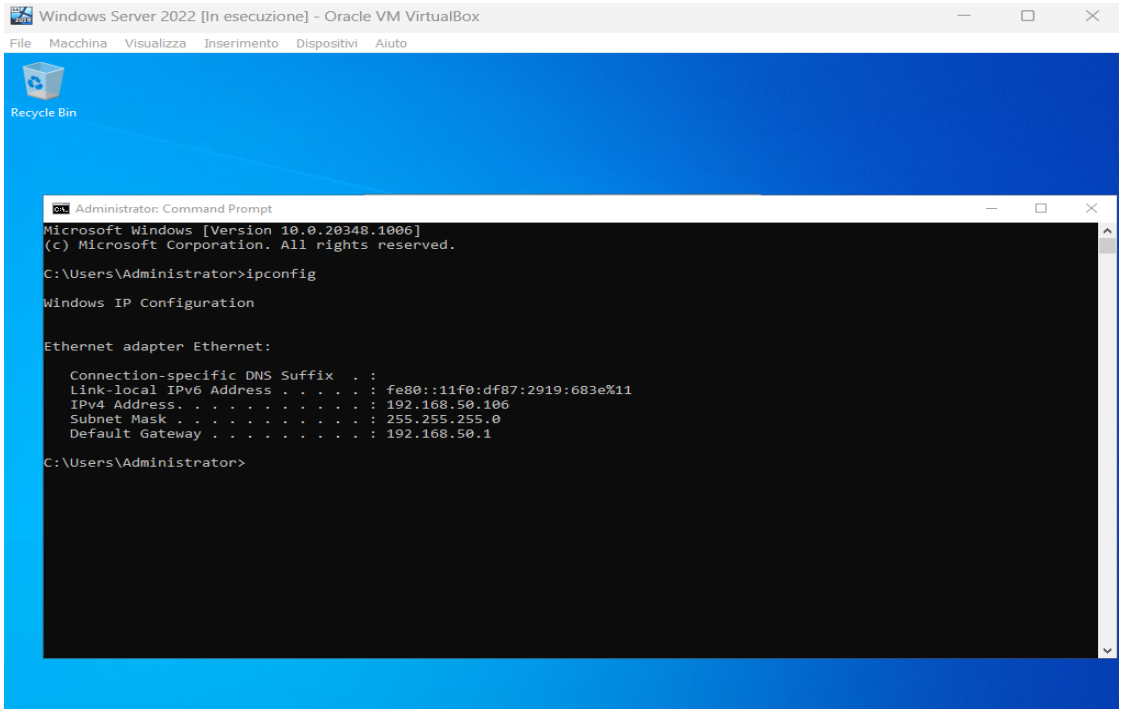
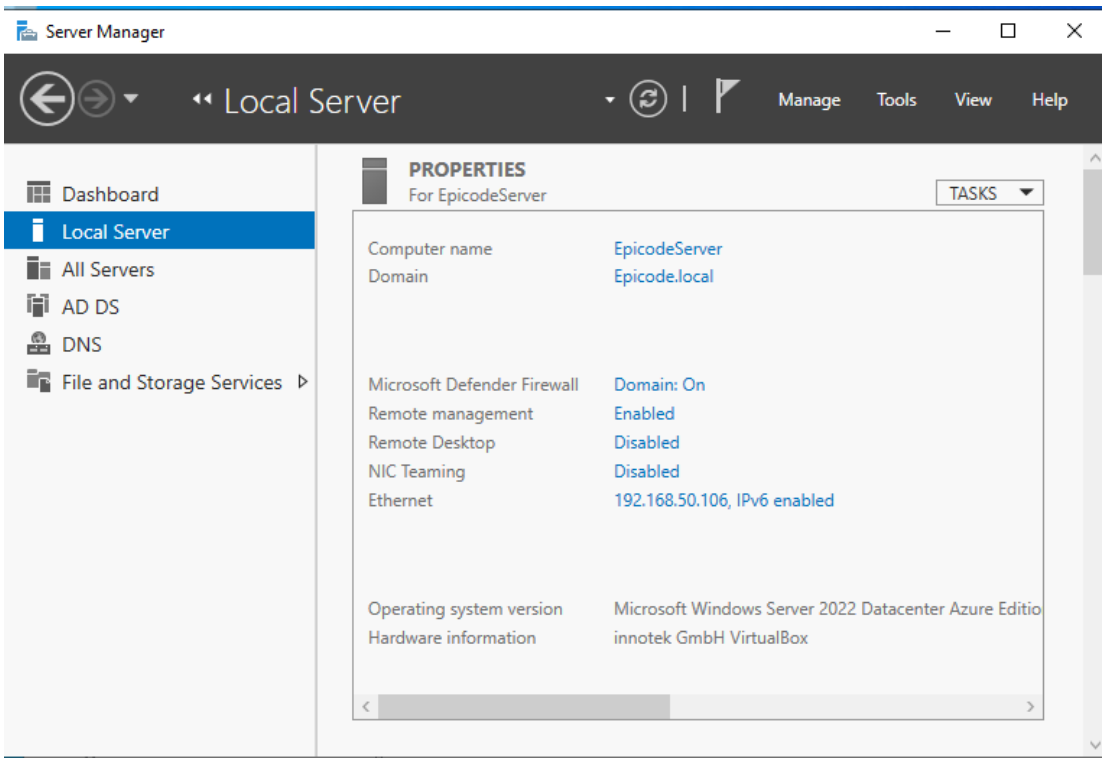
W23D1 – configurazione di Windows Server 2022

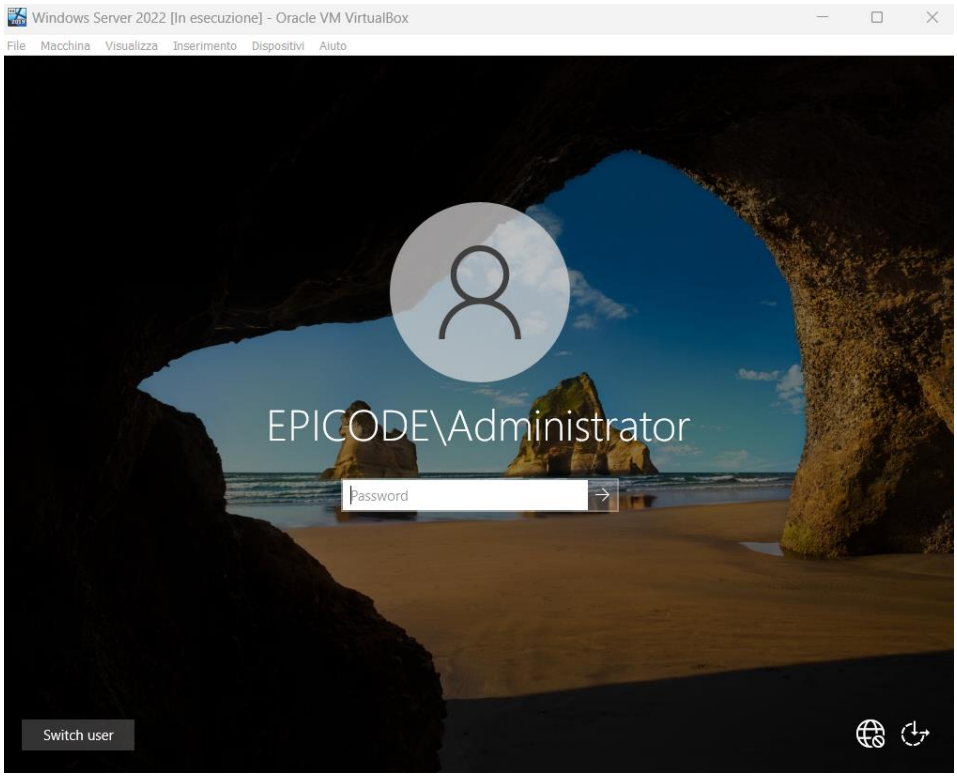
Esercizio obbligatorio.

Ho installato Windows Server 2022, le guest additions ed ho impostato l'indirizzo IP statico 192.168.50.106 del server. Come richiesto dall'esercizio, ho inserito anche la data e l'ora corrette.

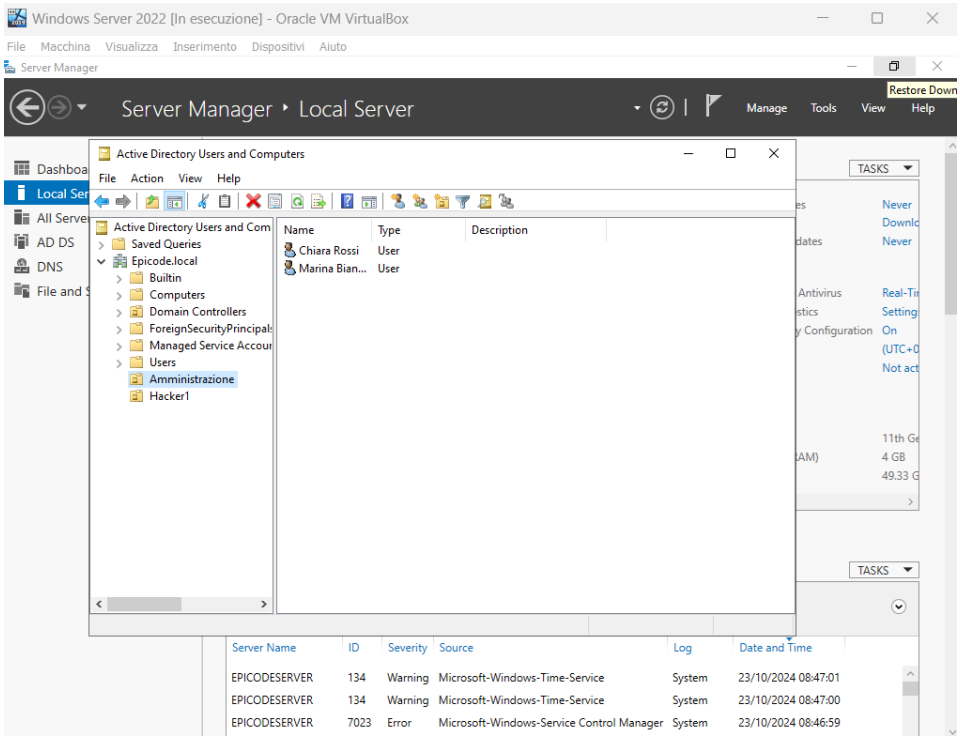


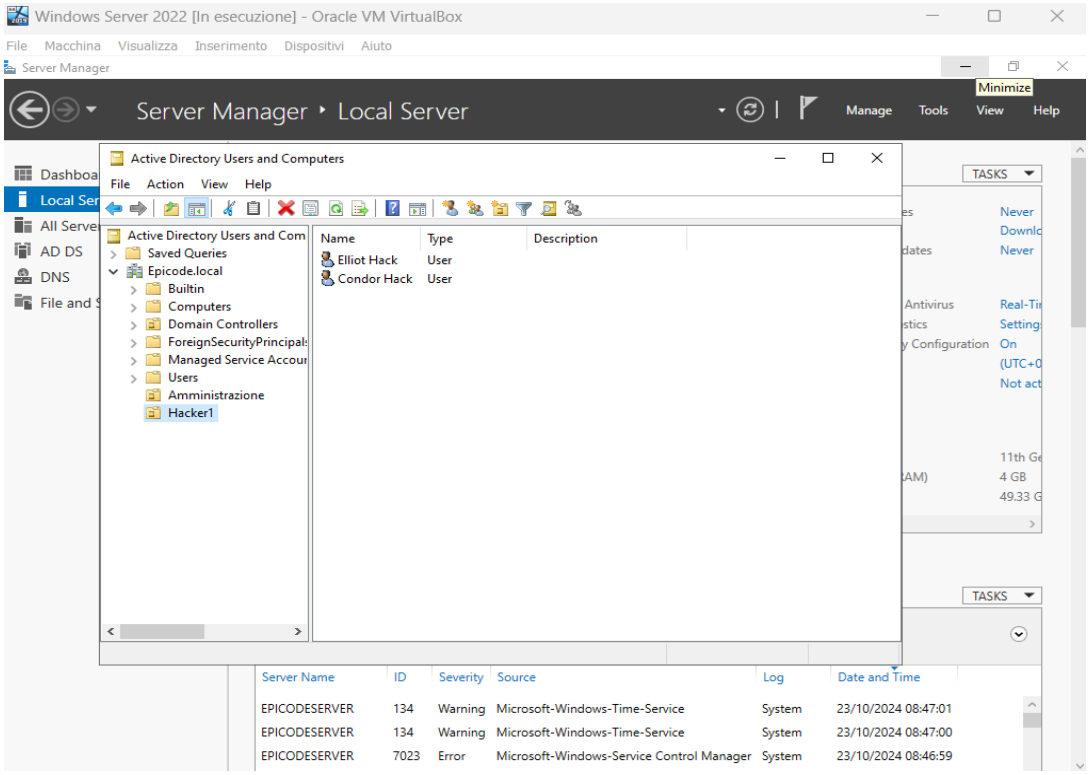
Ho cambiato il nome del server in EpicodeServer, ho creato la Active Directory ed ho creato la foresta epicode.local. Il tutto è andato a buon fine.



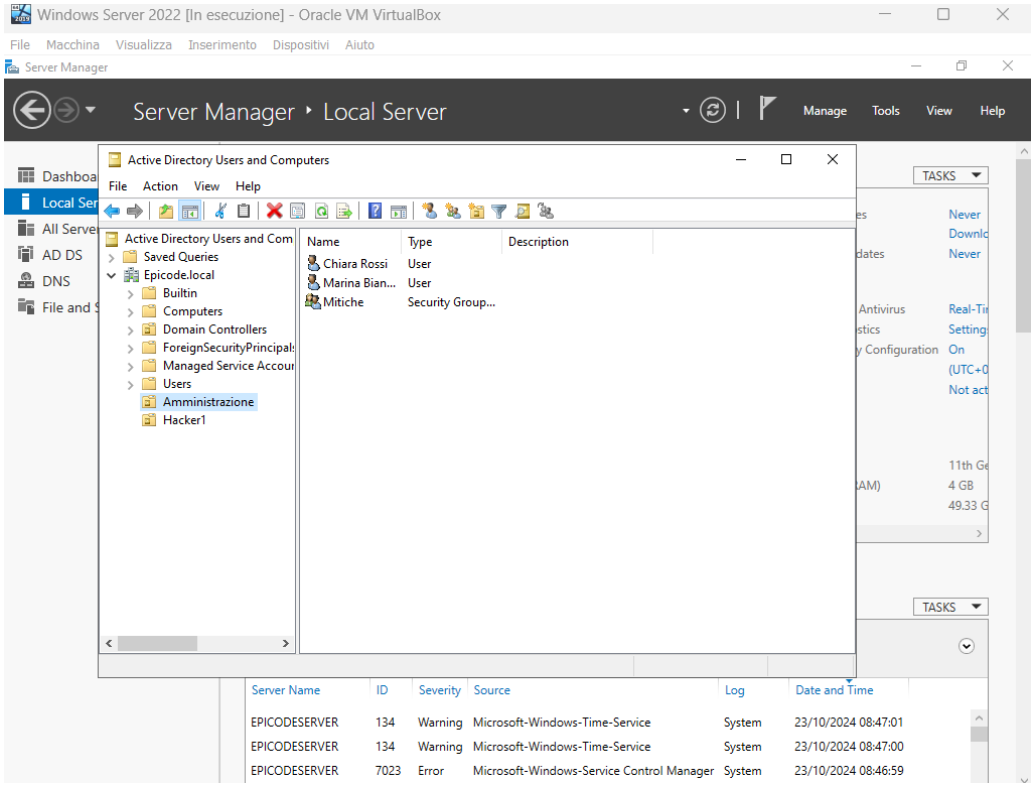


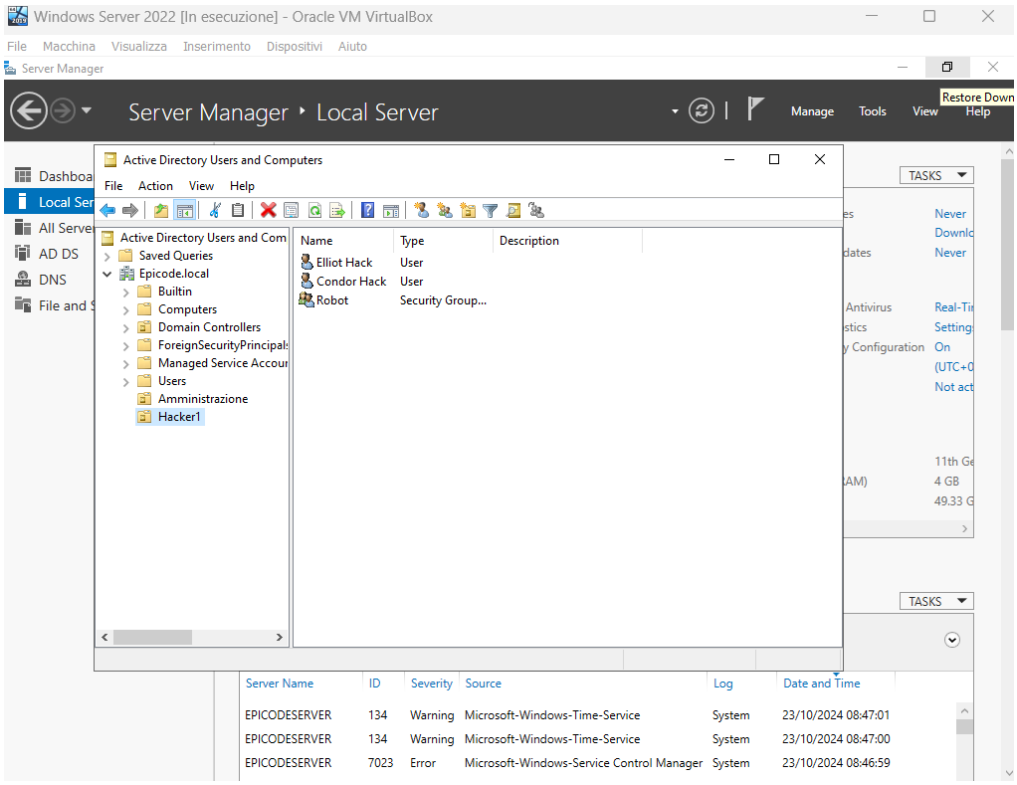
Ho creato le Unità Organizzative Amministrazione ed Hacker1 e gli utenti Chiara, Marina, Elliot e Condor.



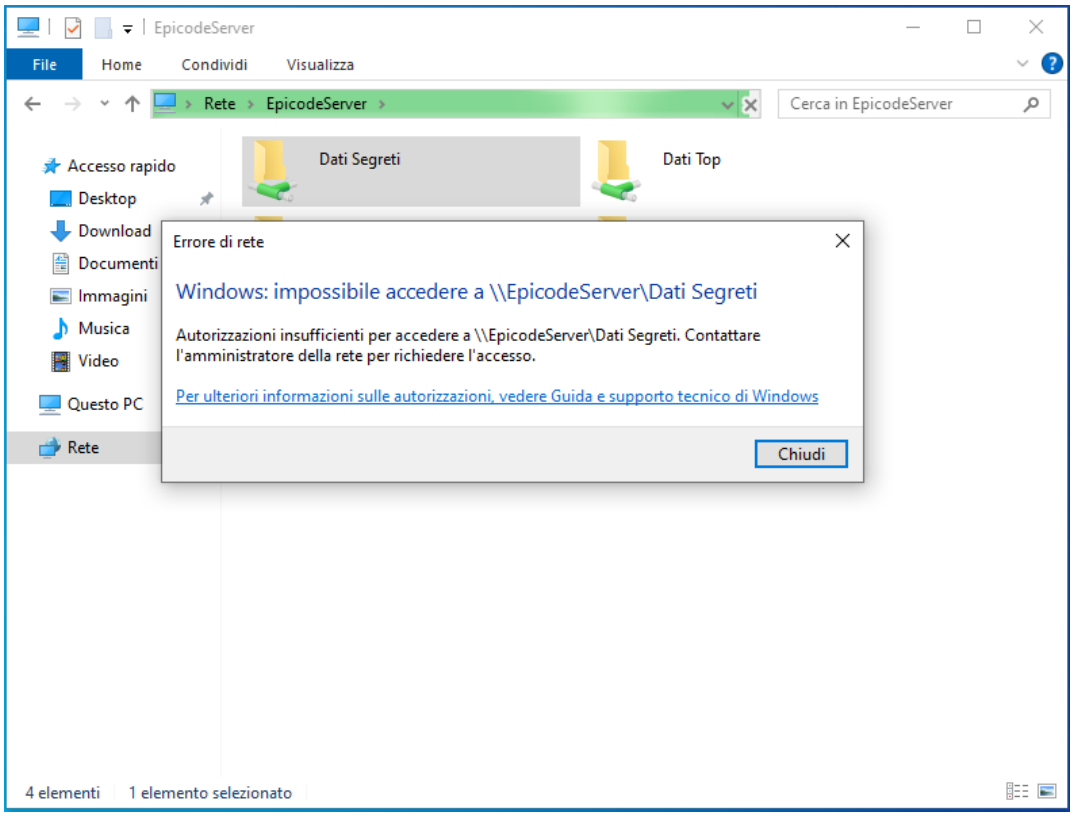


Ho poi creato i due gruppi, ovvero Mitiche e Robot, come richiesto dall'esercizio.

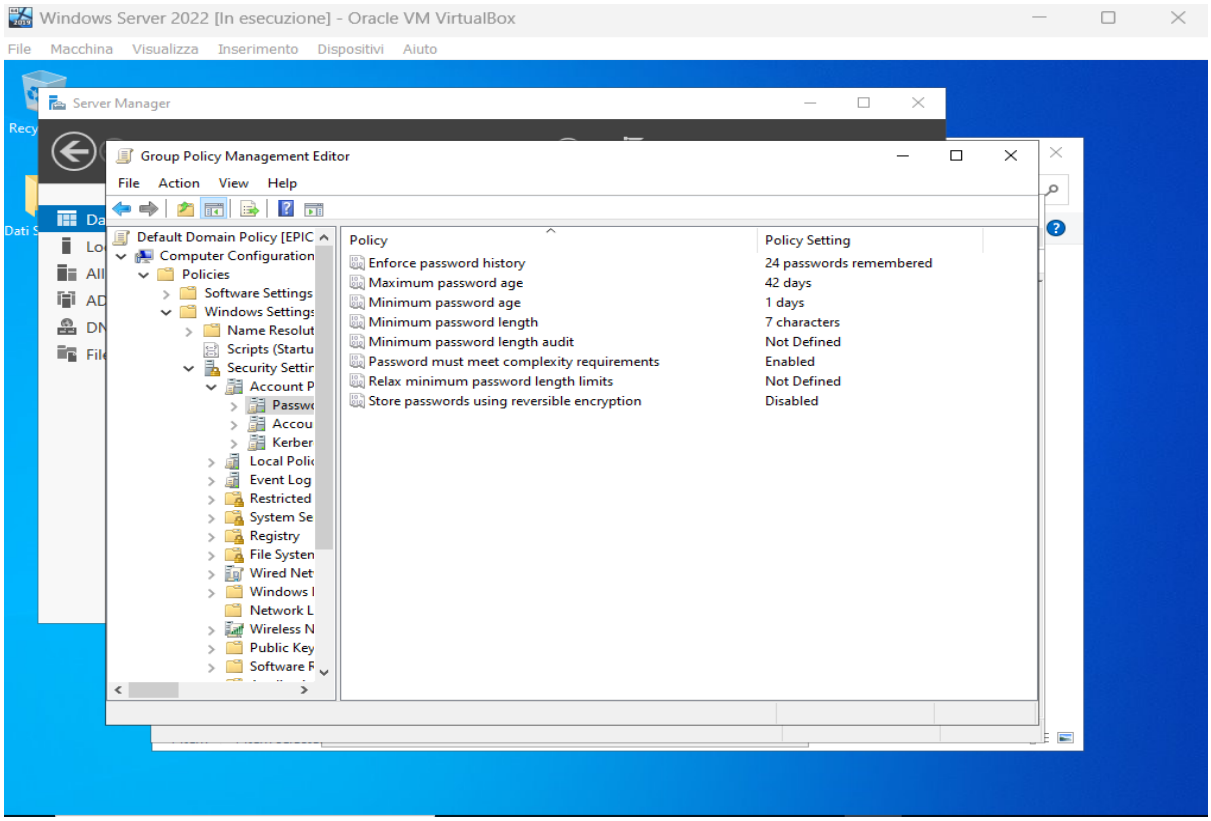




Ho seguito la procedura dell'esercizio, creando la cartella "Dati Segreti" a cui possono accedere gli utenti del gruppo Mitiche e la cartella "Dati Top" a cui possono accedere gli utenti del gruppo Robot. Ho collegato il computer client Windows 10, settando correttamente la rete, al dominio epicode.local ed ho eseguito l'accesso come Elliot Hacker, utente del gruppo Robot. Per verificare che i permessi siano stati inseriti correttamente, ho provato ad accedere come Elliot alla cartella "Dati Segreti" e l'accesso è stato negato, proprio perché solo gli utenti del gruppo "Mitiche" possono accedere a questa cartella. I permessi sono quindi stati settati correttamente e funzionano per evitare che un utente non autorizzato acceda a dati a lui non riservati.



Sono riuscita anche ad accedere alle impostazioni delle password dal server, per poter cambiare le policy delle password, ad esempio riguardo alla lunghezza.



Esercizio extra

Hardening dei sistemi implica un lavoro sulla configurazione di un sistema per renderlo più sicuro e ridurre la superficie vulnerabile ad un attacco. Ad esempio vengono disabilitati servizi non più utilizzati, vengono rimossi utenti che non servono più, vengono aggiornati i software e rimossi i software non più utilizzati. Si tratta di un'ottimizzazione delle configurazioni per puntare solo su ciò che è veramente necessario e concentrarsi sulla protezione di ciò che davvero serve, eliminando elementi superflui che possono diventare pericolosi.

Al primo posto di una checklist per l'hardening di Windows Server 2022 si trova un effettivo patch management, per assicurarsi che le patch di sicurezza vengano scaricate regolarmente per contrastare le vulnerabilità note e corrette dal vendor. Per agevolare l'operazione si può usare Windows Server Update Services, anche per automatizzare gli aggiornamenti nel server e nei vari workgroup. È necessario poi disabilitare i servizi che non vengono effettivamente utilizzati, magari quelli legati al fax, che non sono sfruttati per l'operatività ma che possono essere sfruttati da un attaccante per penetrare nel sistema. È necessario poi concentrarsi sugli utenti e sui ruoli assegnati, disabilitando i ruoli non necessari, riducendo i privilegi al minimo e verificando la sicurezza delle password, in modo che siano abbastanza complesse da non essere scoperte facilmente con un attacco brute-force. Si possono applicare delle account lockout policies, per cui dopo un certo tempo e dopo un certo numero di tentativi di login falliti l'account viene temporaneamente bloccato, per evitare che si tenti di scoprire la password per un accesso malevolo. È bene verificare che sia implementata l'autenticazione a più fattori in tutti gli account per aggiungere un maggiore livello di sicurezza oltre alla semplice password. Passando poi alle misure per la sicurezza della rete, il primo passo per l'Hardening prevede un'attenta configurazione del firewall, per il filtraggio delle connessioni e soprattutto la disabilitazione di porte notoriamente non sicure o non utilizzate. Le porte associate ad SMBv1, Telnet e NETBIOS sono porte ben note e spesso sfruttate per attacchi ed anche chiudere le porte non utilizzate riduce notevolmente la superficie di attacco. È necessario anche controllare che la segmentazione della rete sia implementata correttamente e che i livelli di sicurezza siano adeguati in base alle necessità dei vari segmenti. A questo punto bisogna controllare l'accesso da remoto, disabilitando RDP, ossia remote desktop protocol se non è veramente necessario ed eventualmente implementare una whitelist per controllare che gli IP che lo utilizzano siano solo quelli autorizzati e fidati. Se non si può disabilitare completamente RDP è possibile abilitare la network level authentication NLA, che richiede l'autenticazione dell'utente, possibilmente a più fattori, prima dell'inizio di una sessione di remote desktop. Anziché Telnet è preferibile usare SSH per una migliore crittografia e si può richiedere di collegarsi a remote desktop solo tramite una VPN. Il prossimo passo per l'hardening consiste nel controllo dei meccanismi di logging e monitoring, abilitando Windows Event Logging per una raccolta centralizzata dei log, abilitando i log per tutte le attività che richiedono privilegi di amministratore ed abilitando un logging dettagliato per la PowerShell, spesso sfruttata in varie tipologie di attacchi. Una checklist per l'hardening deve prevedere delle azioni concrete

contro i malware, abilitando Windows Defender ed Exploit Protection, assicurandosi che vengano svolte delle scansioni in tempo reale e che tutti gli strumenti siano debitamente aggiornati e configurati. Per quanto riguarda la sicurezza del file system, serve verificare con attenzione i permessi, soprattutto i permessi NTFS, dando i minimi privilegi possibili agli utenti ed abilitare AppLocker e Windows Defender Application Control per limitare il numero di applicazioni e script che possono essere eseguiti sul server. Infine è necessario abilitare BitLocker per una migliore crittografia dei dischi fisici del server. Per una maggiore sicurezza, serve disabilitare i servizi non utilizzati o notoriamente vulnerabili, come SMBv1. Infine, è bene configurare correttamente anche le group policies, per applicare in maniera centralizzata delle configurazioni di sicurezza ed anche controllare i privilegi degli amministratori, cercando di contenerli solo al necessario. Infine, l'ultimo passo un buon hardening è un controllo e un rafforzamento delle politiche di backup, utili in caso di incidente e questi backup devono essere testati per essere sicuri di poter contare su di loro in caso di problemi per ripristinare i dati.