

Verifica 14/02/25

CONSEGNA

Esercizio di oggi: Creazione di Gruppi in Windows Server 2022 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.

1.

Preparazione:

- Accedi al tuo ambiente Windows Server 2022.
- Assicurati di avere i permessi amministrativi necessari per creare e gestire gruppi. Creazione dei Gruppi:

2.

- Crea due gruppi distinti.

Puoi scegliere i nomi che preferisci per questi gruppi, ma assicurati che i nomi siano significativi per riflettere la loro funzione o ruolo all'interno dell'organizzazione (ad esempio, "Amministratori", "UtentiStandard", "MarketingTeam", "Sviluppatori", ecc.).

3.

Assegnazione dei Permessi:

- Per ogni gruppo, assegna permessi specifici.

Puoi scegliere quali permessi concedere, ma assicurati di considerare i seguenti aspetti:

- Accesso ai file e alle cartelle.
- Esecuzione di programmi specifici.
- Modifiche alle impostazioni di sistema.
- Accesso remoto al server.

○ Documenta i permessi assegnati a ciascun gruppo, spiegando perché hai scelto tali permessi.
Verifica:

○ Una volta creati i gruppi e assegnati i permessi, verifica che le impostazioni siano corrette.

Puoi farlo:

- Creando utenti di prova e aggiungendoli ai gruppi.
- Verificando che gli utenti abbiano i permessi assegnati in base al gruppo a cui appartengono.

Documentazione:

- Scrivi un breve report che includa:
 - I nomi dei gruppi creati.
 - I permessi assegnati a ciascun gruppo.
 - I passaggi seguiti per creare e configurare i gruppi.

BONUS

(trovare versione sw)

SVOLGIMENTO

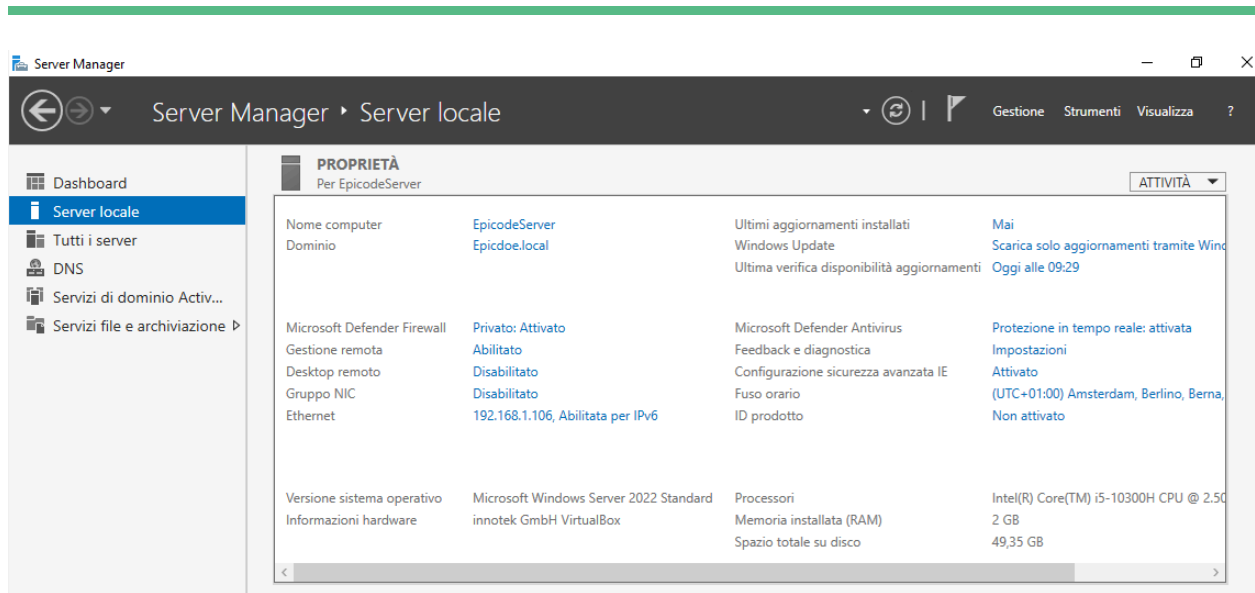
1.0

Per svolgere l'esercizio assegnato ci serviremo di due macchine virtuali:

-windows server 2022

-windows 10 pro

cominceremo andando a verificare le impostazioni di dominio e di active directory presenti sul nostro windows server



teniamo a mente le info importanti viste nell'immagine soprastante:

nome computer: **EpicodeServer**

nome dominio: **Epicdoe.local** (sì, ho sbagliato a scrivere :()

ora proseguiamo andando a creare sulla stessa macchina i gruppi relativi all'azienda. Ho scelto di simulare un'azienda del settore Tech/IT che comprenderà quattro gruppi:

1 Amministratori IT/server

2 Sviluppatori IT

3 Supporto Tecnico/risorse umane

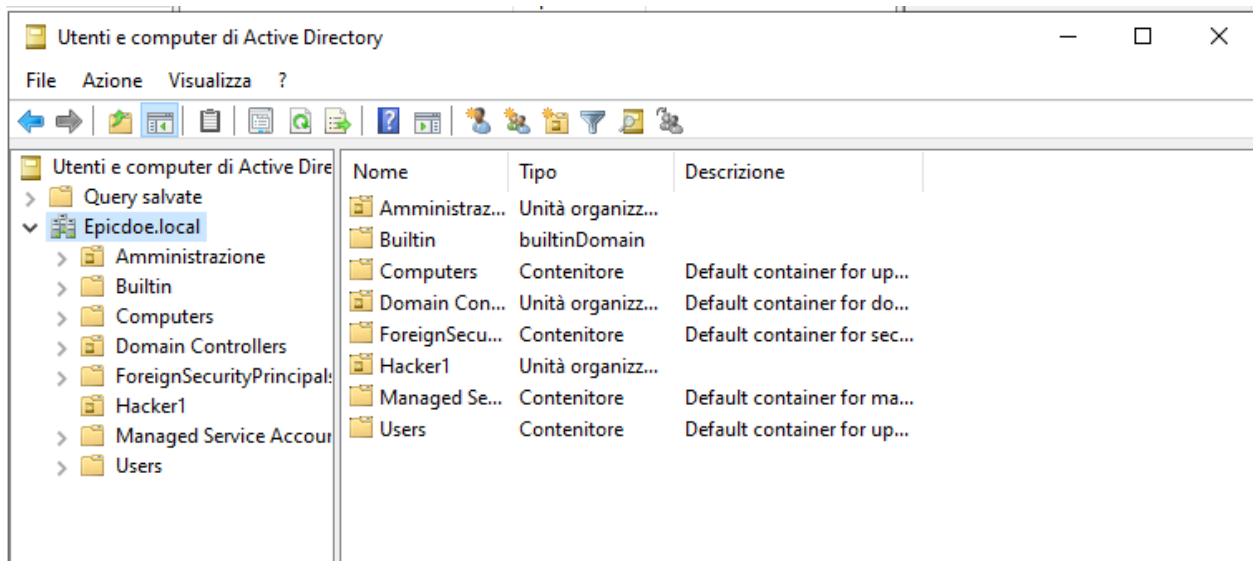
4 Marketing/commerciale

1.1 Creazione dei gruppi

Procediamo andando a creare il primo gruppo come segue;

Rechiamoci nella sezione

Domini e Trust di Active Directory



Andiamo a creare 4 unità organizzative

(ne utilizzeremo poi soltanto due, ma ci dà un'idea di suddivisione aziendale dei compiti più chiara)

dove successivamente inseriremo i gruppi

facciamo **'click'** col tasto destro sulla nostra **'active directory'** e selezioniamo

nuovo —> unità organizzativa

Nome	Tipo	Descrizione
Amministrat...	Unità organizz...	
Builtin	builtinDomain	
Computers	Contenitore	Default container for up...
Domain Con...	Unità organizz...	Default container for do...
ForeignSecu...	Contenitore	Default container for sec...
Hacker1	Unità organizz...	
Managed Se...	Contenitore	Default container for ma...
Users	Contenitore	Default container for up...
Amministrat...	Unità organizz...	
SviluppatoriIT	Unità organizz...	
Supporto	Unità organizz...	
Marketing	Unità organizz...	

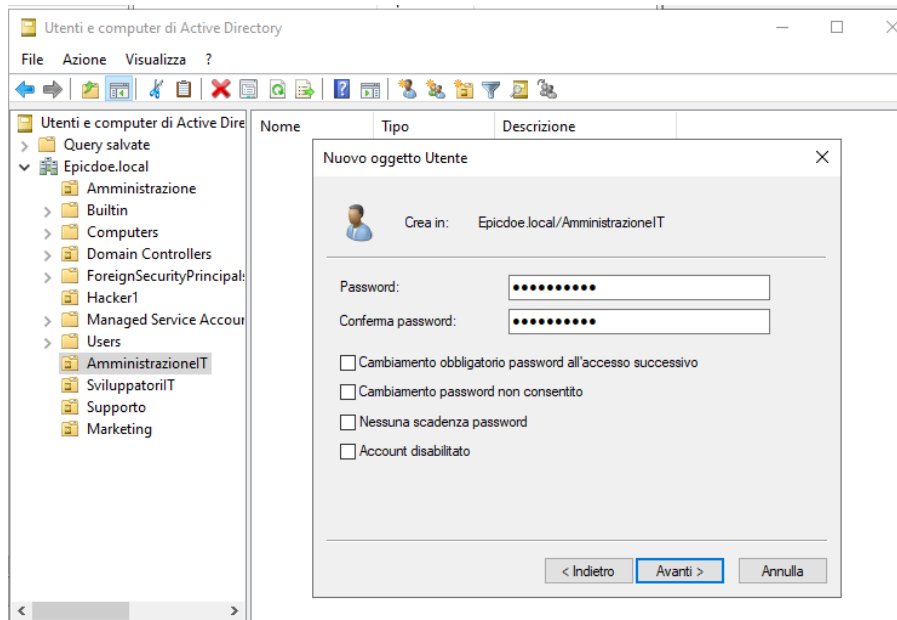
Procediamo selezionando la cartella Amministratori IT e andiamo a creare due utenti di esempio

Admin1

Admin2

per farlo clicchiamo col tasto destro sulla directory e selezioniamo

nuovo —> utente

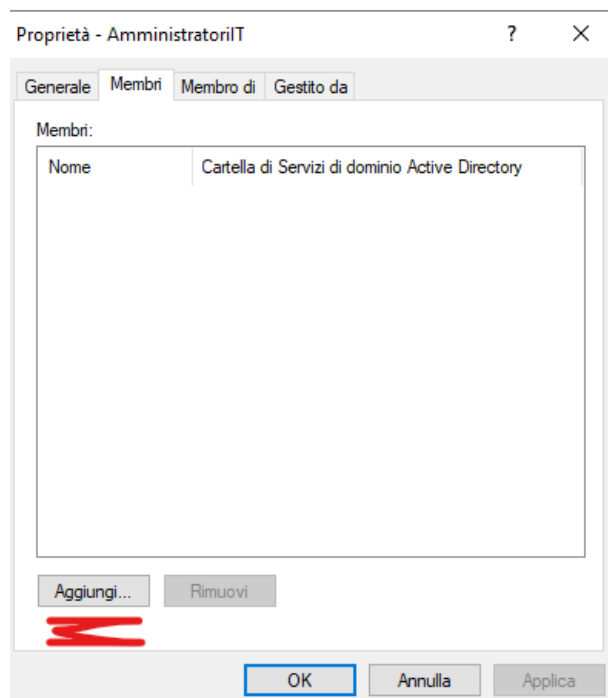
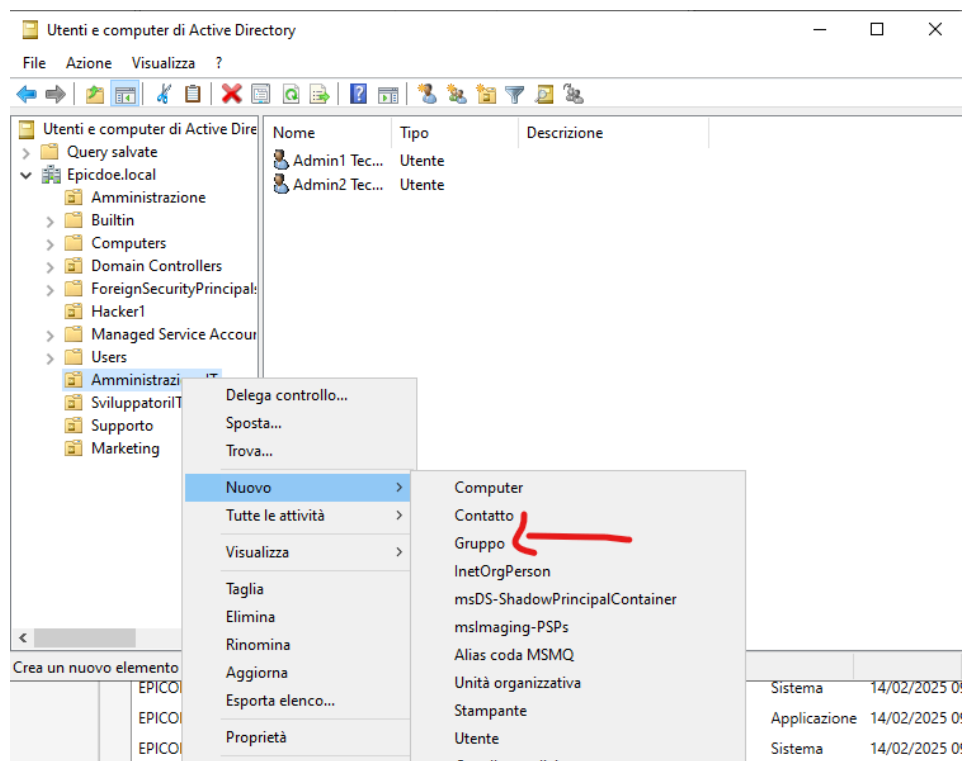


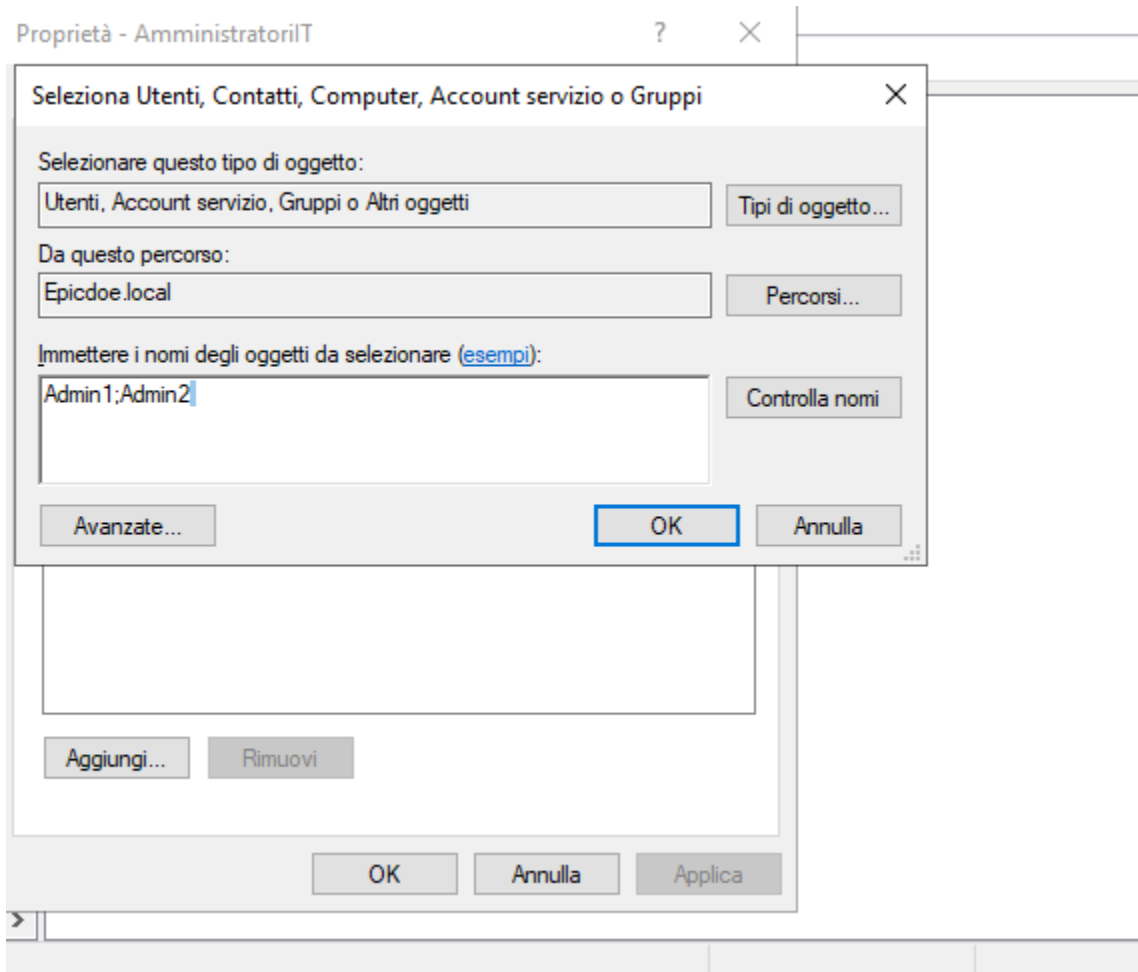
Utenti e computer di Active Dire	Nome	Tipo	Descrizione
Query salvate			
Epicdoe.local			
Amministrazione			
Builtin			
Computers			
Domain Controllers			
ForeignSecurityPrincipal			
Hacker1			
Managed Service Account			
Users			
AmministratoreIT			
SviluppatoriIT			
Supporto			
Marketing			

Nome	Tipo	Descrizione
Admin1 Tec...	Utente	
Admin2 Tec...	Utente	

procediamo andando a creare il **gruppo** vero e proprio e inseriamo i nostri utenti Admin al suo interno

chiameremo il gruppo: **AmministratoriT**





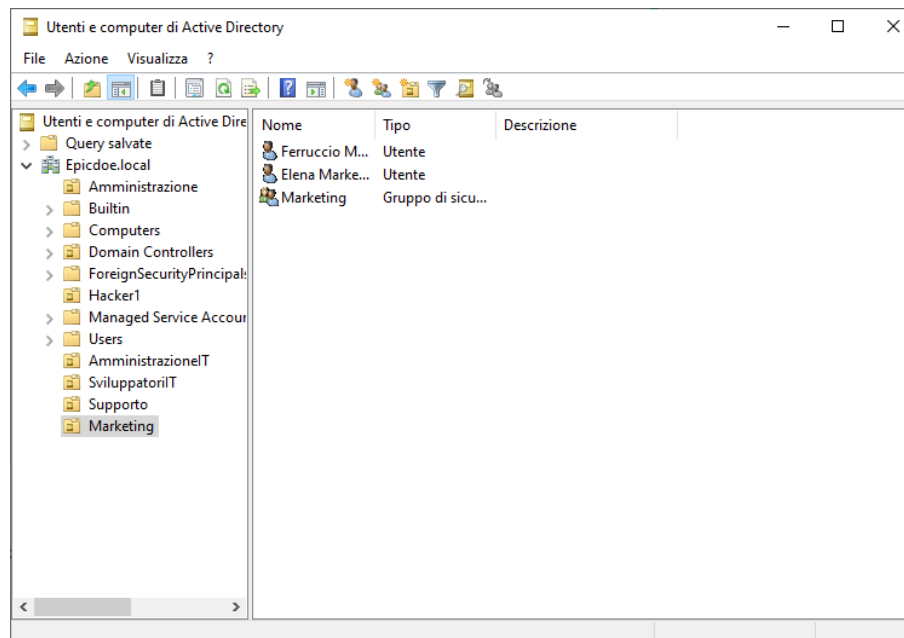
1.2 Creazione secondo gruppo (marketing)

Ripetiamo i passaggi precedentemente visti nel punto 1.1 per andare a creare prima due utenti esperti di marketing all'interno della nostra directory **Marketing**

Elena

Ferruccio

E poi procediamo con l'inserirli nel gruppo Marketing. la schermata finale dovrebbe essere come la seguente



1.3 Creazione cartelle di destinazione

Prima di procedere con la creazione delle regole/permessi da assegnare ai due gruppi, andremo a creare alcune repository che ci serviranno come esempio per testare la validità delle nostre regole di accesso ai dati presenti sul server.

ne creeremo 3:

-Dati SW e Manutenzione

questa repository ipoteticamente contiene un insieme di informazioni sui sistemi installati all'interno del nostro server, i quali comprendono SO, Impostazioni e configurazioni del server e di eventuali web app, tool utilizzati, framework, versioni dei singoli SW, licenze...

-Dati di Vendita

contiene i report di vendita dell'azienda, con informazioni riguardo la situazione economica attuale, i rapporti commerciali, idee di brand, strategie di marketing..

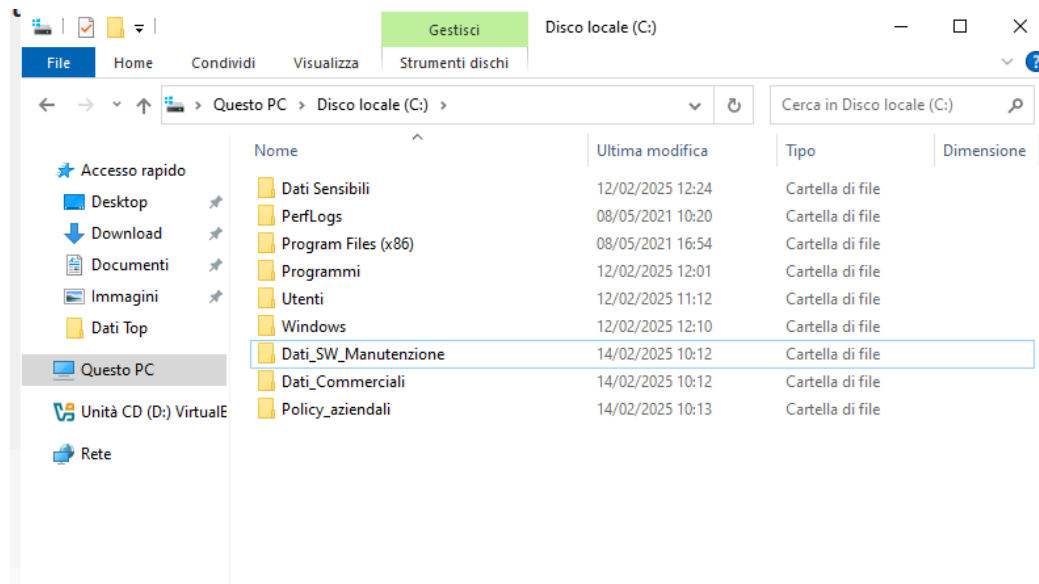
-Policy aziendali e Best Practice

Una raccolta delle principali best practice e delle regole fondamentali di utilizzo e gestione, messa a disposizione dei dipendenti dell'azienda per fornire linee guida efficaci e trasparenti.

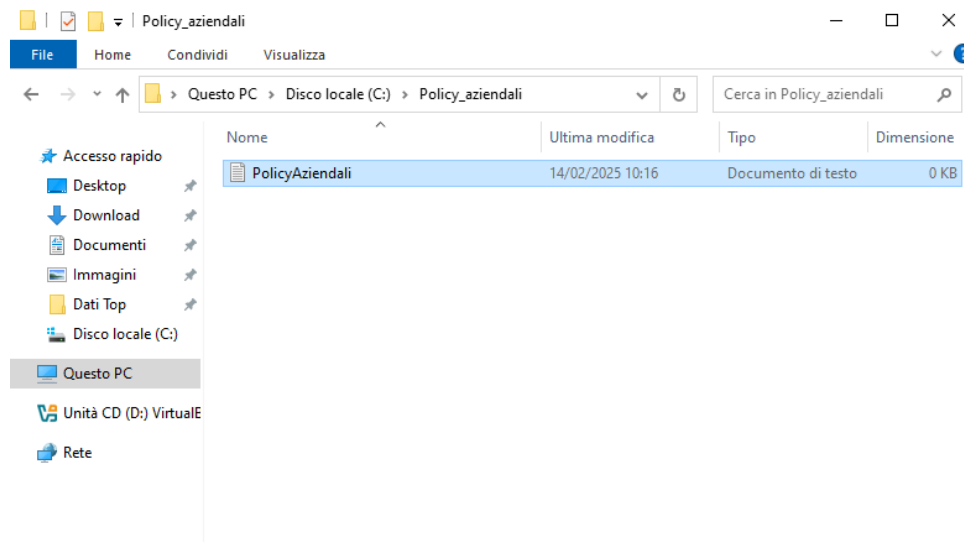
Per creare le cartelle ci basta recarci sul percorso

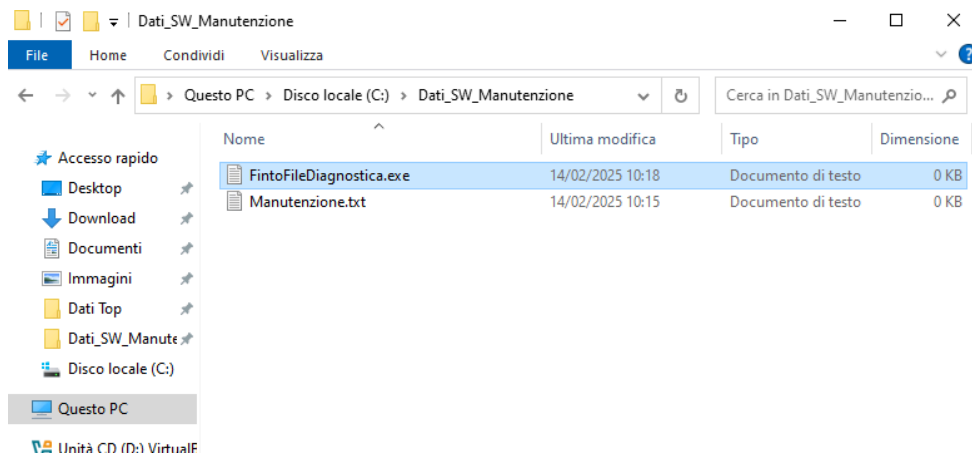
Questo PC → Disco Locale

e procedere cliccando col tasto destro e selezionando 'nuova cartella'



(Inseriamo successivamente dei file .txt in ciascuna cartella solo per avere dei target di riferimento nel nostro esempio)





1.4 Valutazione dei permessi

Ora siamo arrivati al 'core' del nostro esercizio, andiamo a configurare i permessi di accesso alle nostre repository basandoci sulla logica aziendale di accesso ai dati sensibili/non sensibili.

Sarà infatti opportuno definire quali tipi di permessi concedere ad ogni gruppo di utenti, nel nostro caso specifico assegneremo:

-al gruppo Amministratori IT:

l'accesso completo a tutte le cartelle, trattandosi di personale specializzato e incaricato di gestire la manutenzione e il corretto funzionamento del server aziendale, non ritengo opportuno negare all'amministratore stesso l'accesso ai dati di alcun tipo. Pertanto tutte e tre le directory avranno attive i permessi di **lettura, scrittura ed esecuzione**.

-al gruppo Marketing:

negheremo l'accesso in maniera totale alla directory contenente i dati e i file inerenti la manutenzione (Dati_Sw_Manutenzione)

permetteremo l'accesso completo (**scrittura, lettura, esecuzione**) ai dati riguardanti la vendita e le strategie di marketing (Dati_Commerciali).

daremo accesso di **sola lettura** per quanto riguarda le policy aziendali, in modo che queste non possano essere modificate inadeguatamente.

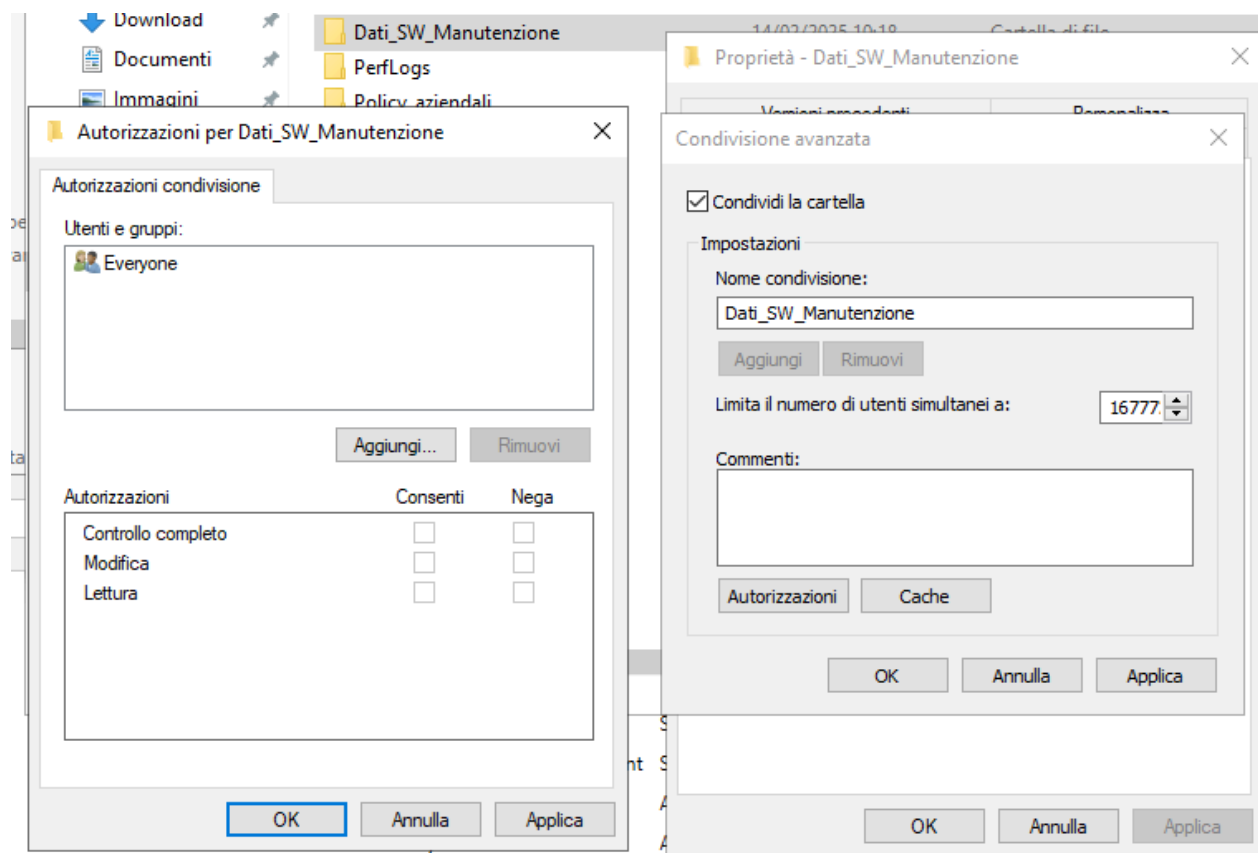
IMPORTANTE!

Ricordiamoci nella nostra configurazione di rimuovere il permesso **'Everyone'** che windows server imposta di default per la sola lettura dei file. altrimenti le nostre policy di accesso risulteranno inefficaci.

1.5 Configurazione dei permessi

Procediamo quindi a configurare i permessi, rechiamoci sulla prima cartella (Dati_SW_Manutenzione) e clicchiamo col tasto destro su 'proprietà'

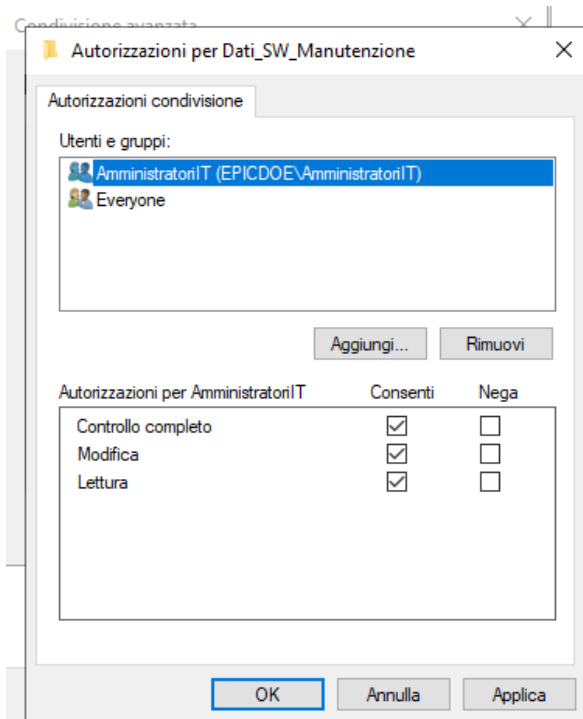
da qui selezioniamo le impostazioni avanzate di condivisione e andiamo a rimuovere il flag da 'solo lettura' impostato per il gruppo **'Everyone'**



Successivamente clicchiamo su 'Aggiungi' ed inseriamo

Amministratori IT

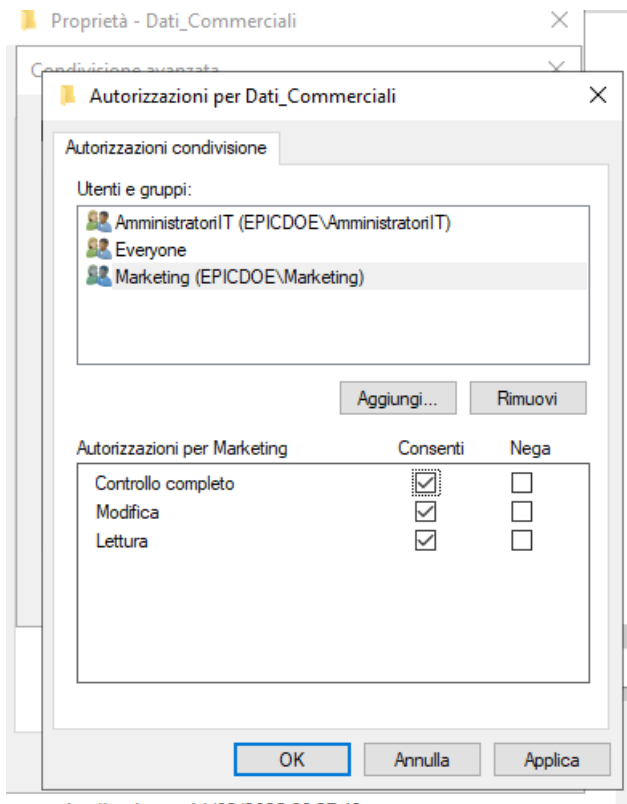
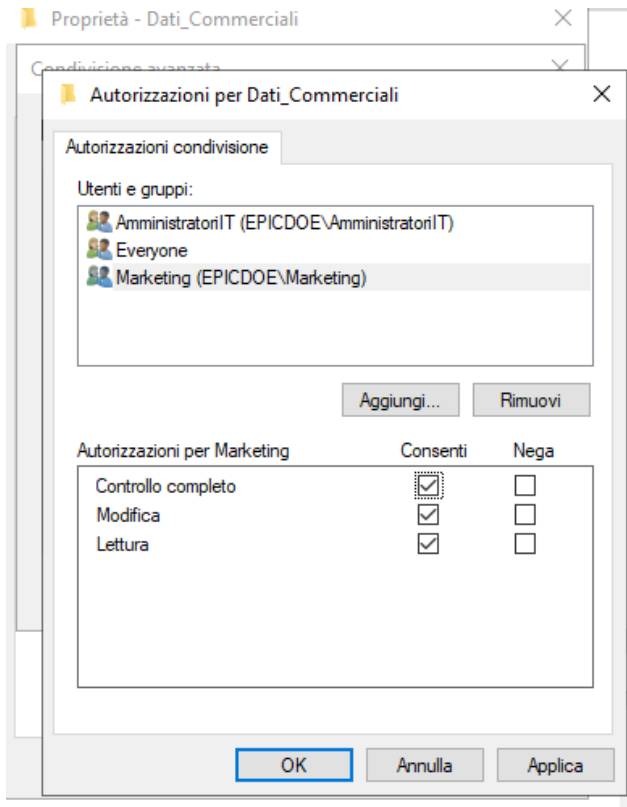
come gruppo, poi selezioniamo tutti i tipi di permessi e clicchiamo su **'Applica'**



non vi è bisogno di configurare l'accesso senza permessi al secondo gruppo in quanto, non avendo nessun tipo di accesso, staremo ancora più sicuri senza condividere nemmeno la cartella

Proseguiamo come abbiamo appena visto, andando a configurare i permessi anche per le altre due cartelle create nei confronti del gruppo '**AmministratoriIT**'

E approfittiamo anche per impostare i permessi relativi al gruppo '**Marketing**', che come prima accennato deve avere permessi totali solo nei confronti della cartella inerente i dati commerciali, e di sola lettura per quanto riguarda le policy aziendali

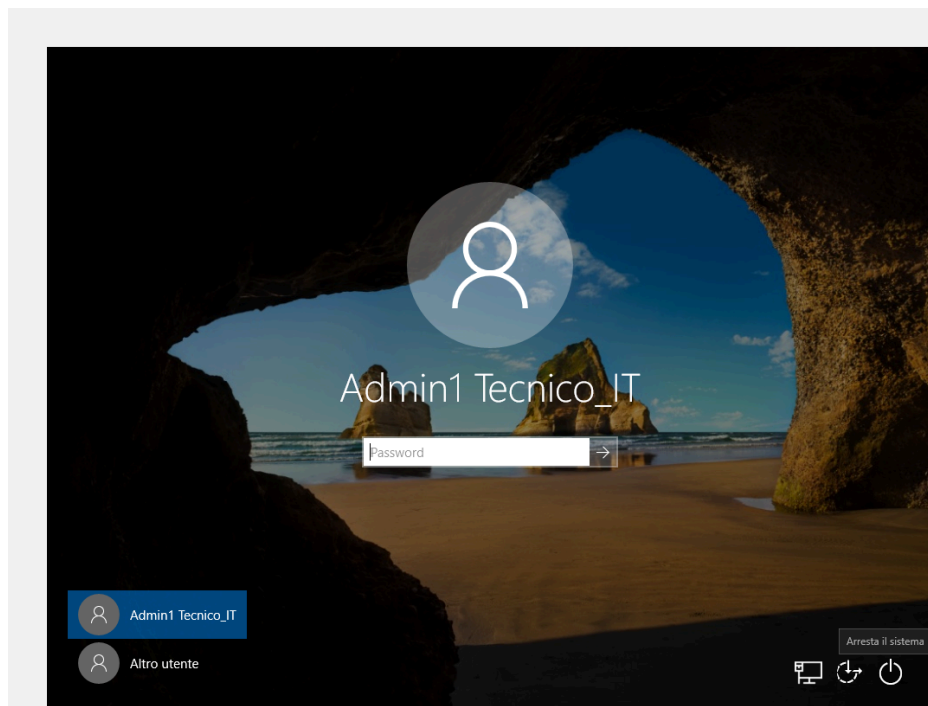


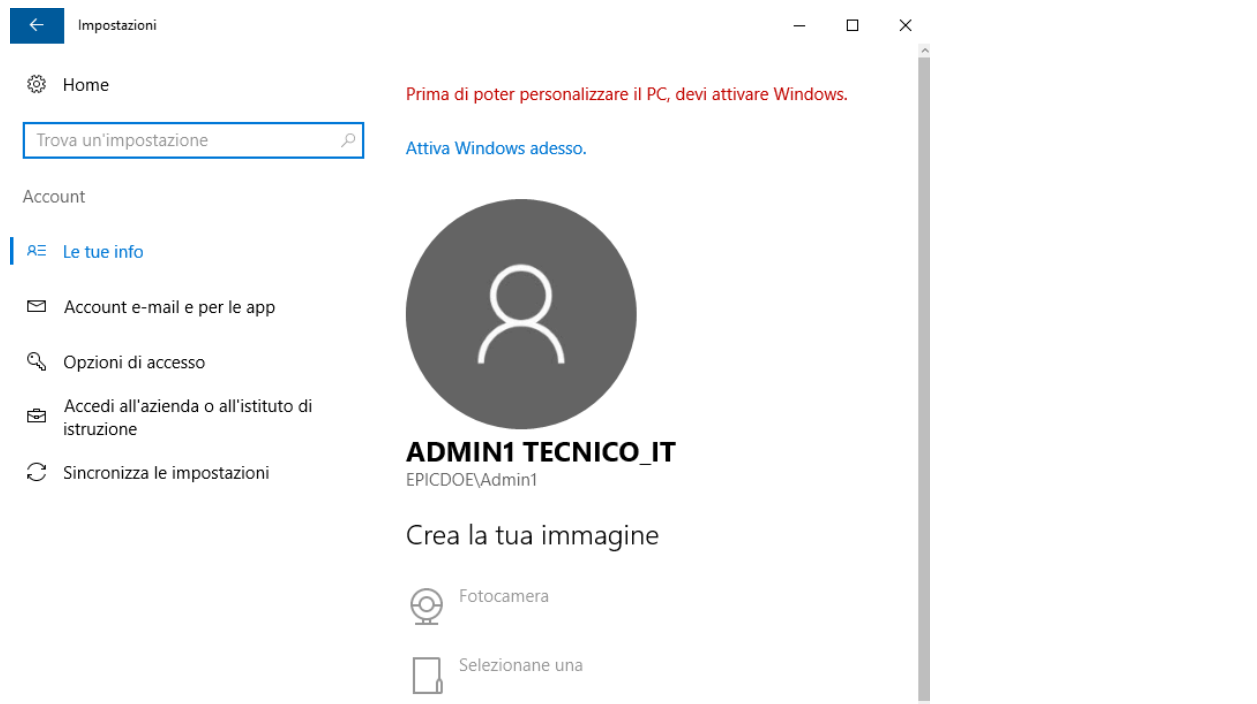
1.6 Verifica Admin1

Non ci resta che testare quanto fatto fin ad ora, andiamo ad effettuare l'accesso al nostro pc Windows 10

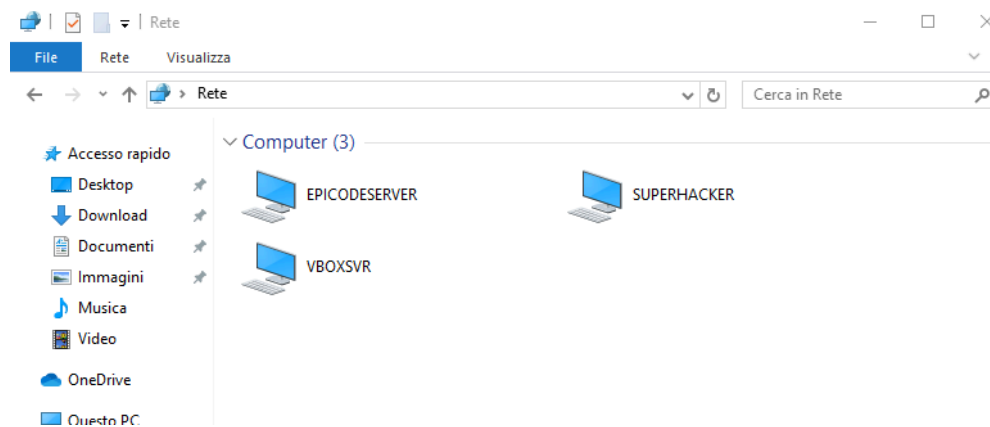
(precedentemente impostato per connettersi al dominio del nostro server)

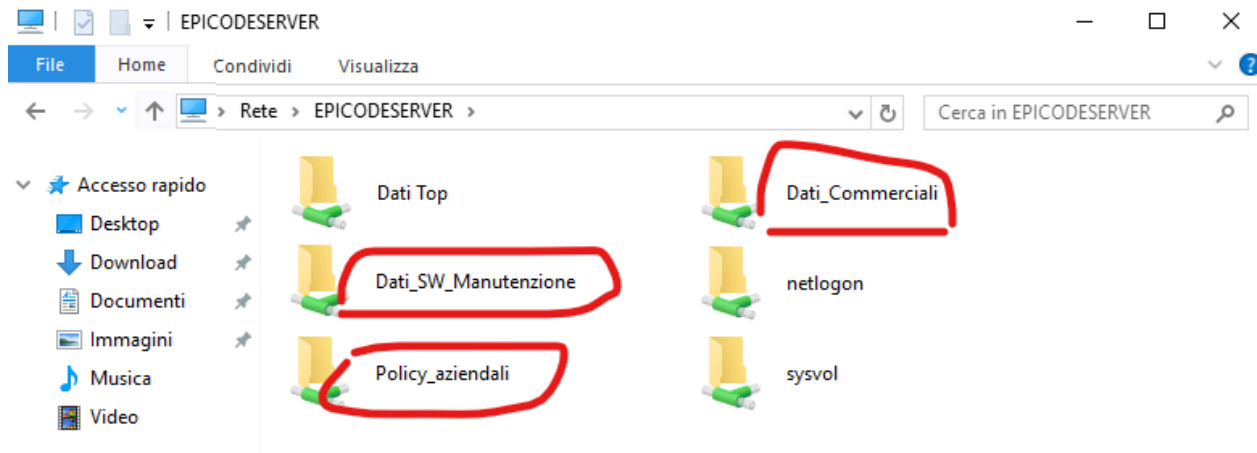
con l'utente **Admin1** e verifichiamo che questi sia in grado di visualizzare e modificare i file condivisi



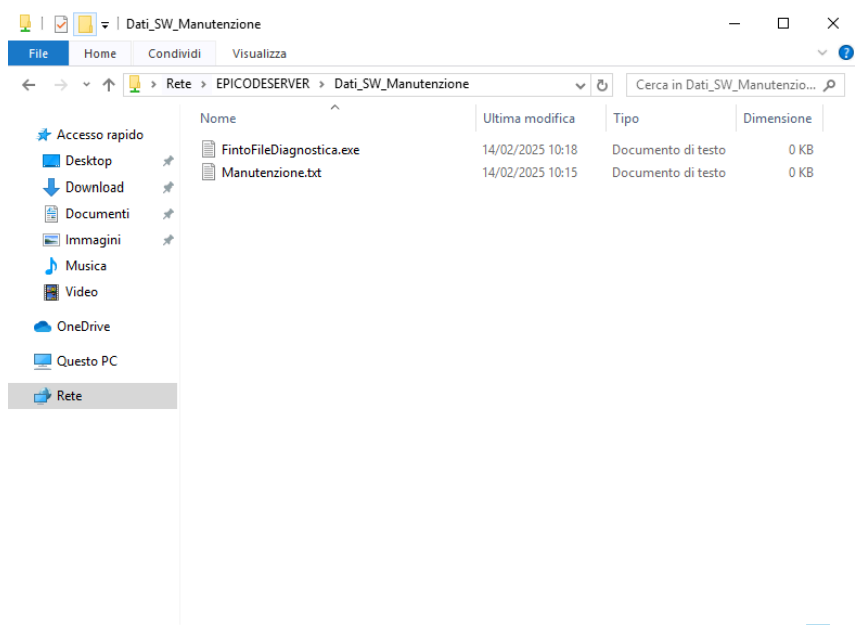


accendiamo alla sezione **rete** e visualizziamo il nostro server, facendo doppio click potremo vedere tutte le cartelle in esso condivise

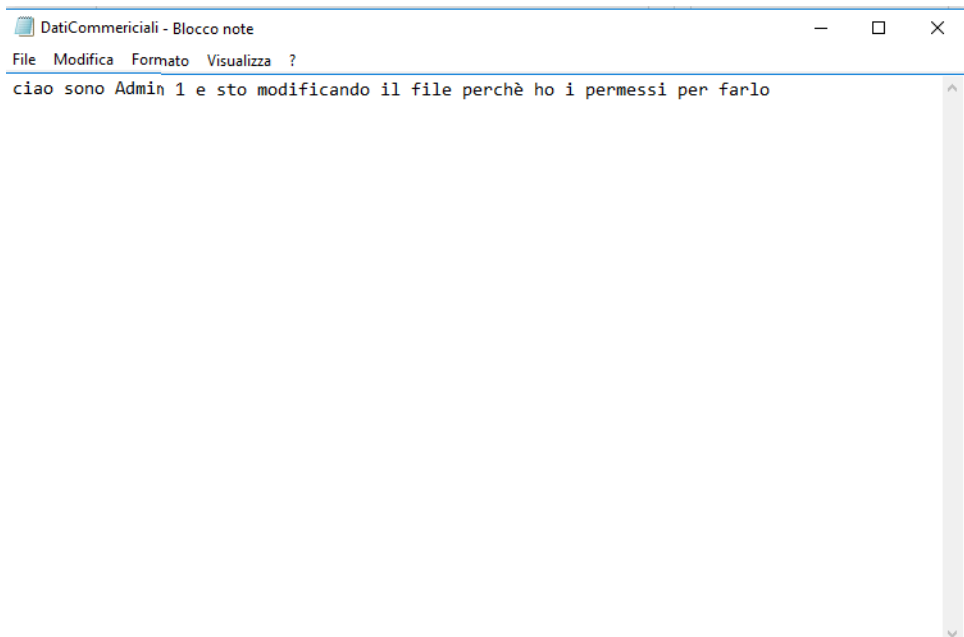




Ora effettuiamo l'accesso alla cartella riservata agli Amministratori (Dati_SW_Manutenzione) per verificare che le nostre policy di accesso siano corrette:

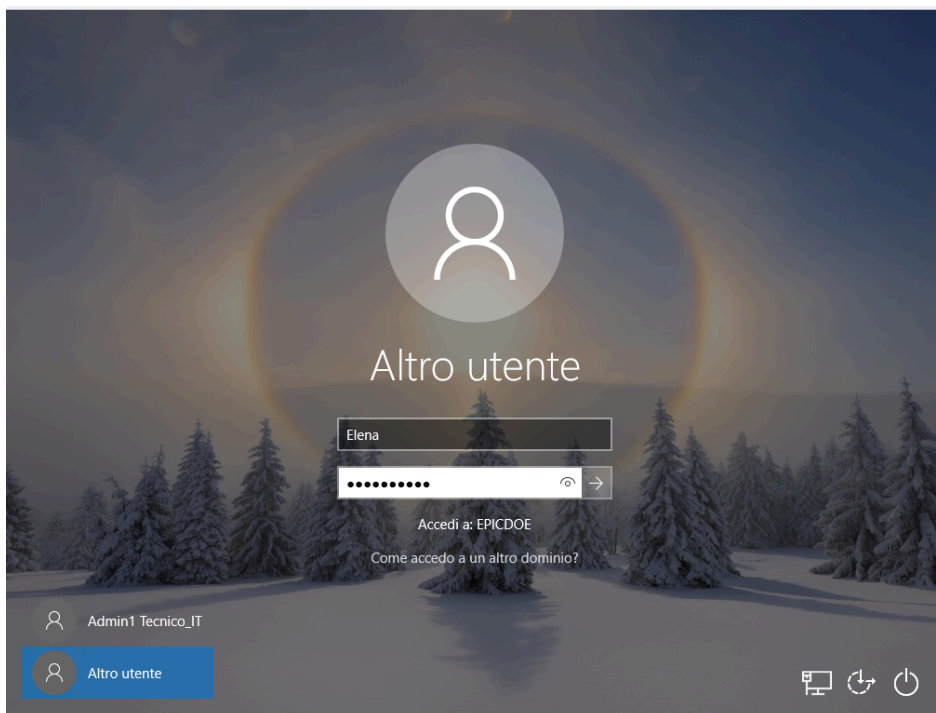


ora modifichiamo il file contenuto nella cartella Dati Commerciali per eseguire una verifica anche ai permessi di scrittura/modifica

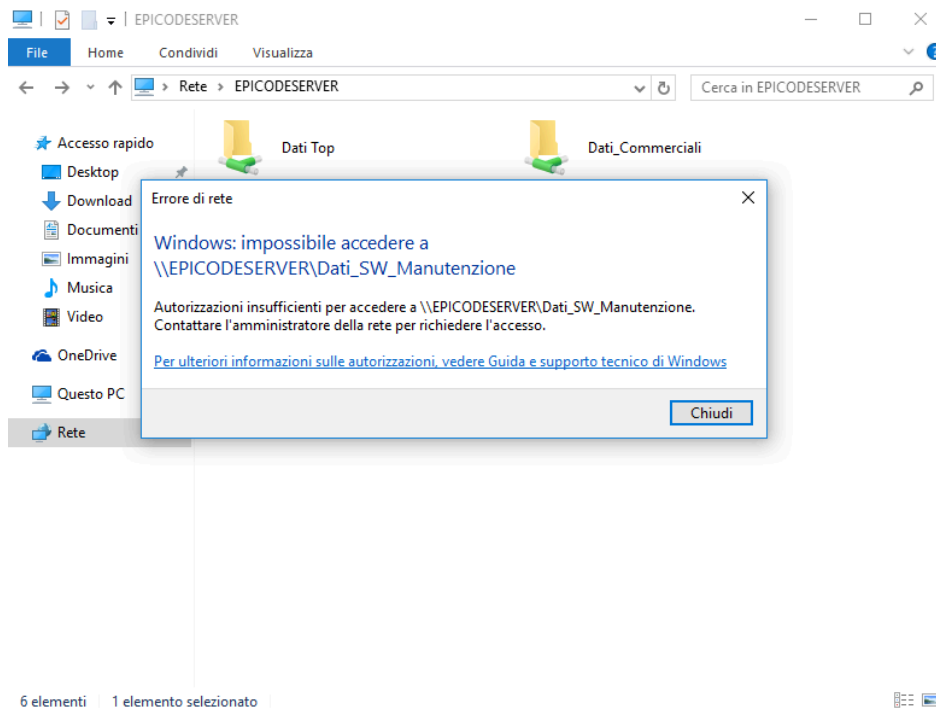


1.7 Verifica Utente Marketing

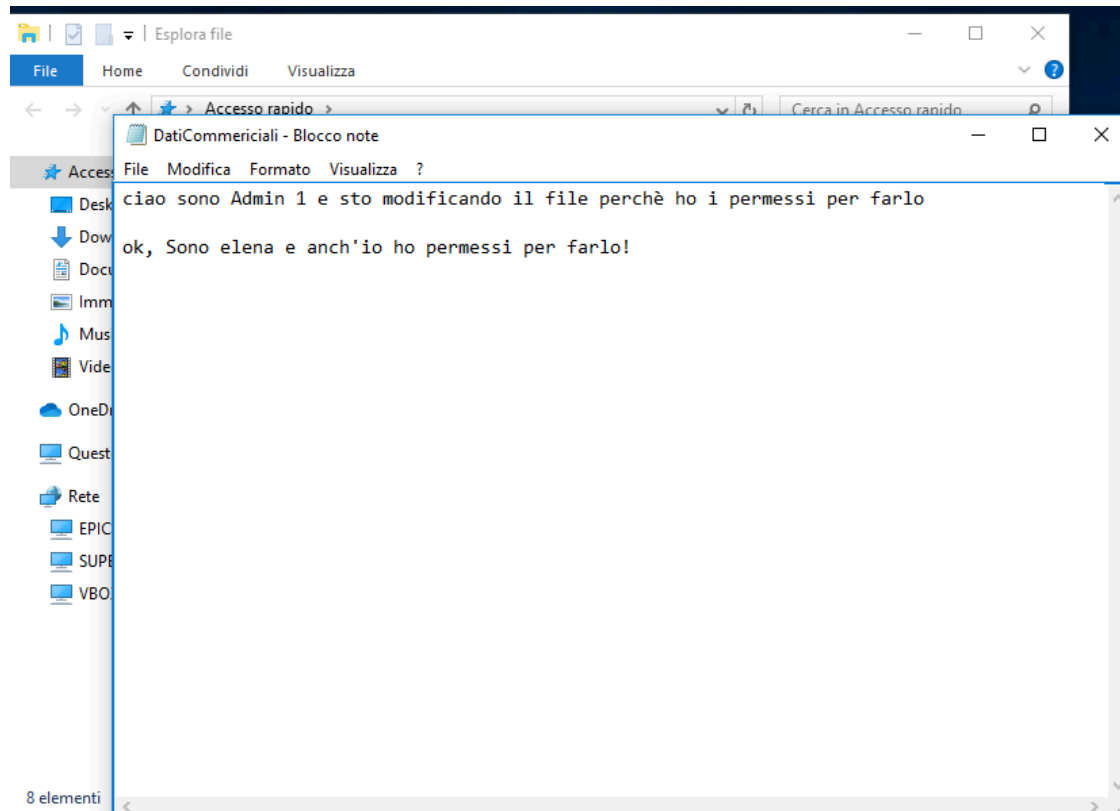
Per avere un doppio riscontro ora procederemo come appena visto, ma utilizzando un utente del gruppo Marketing, **Elena**



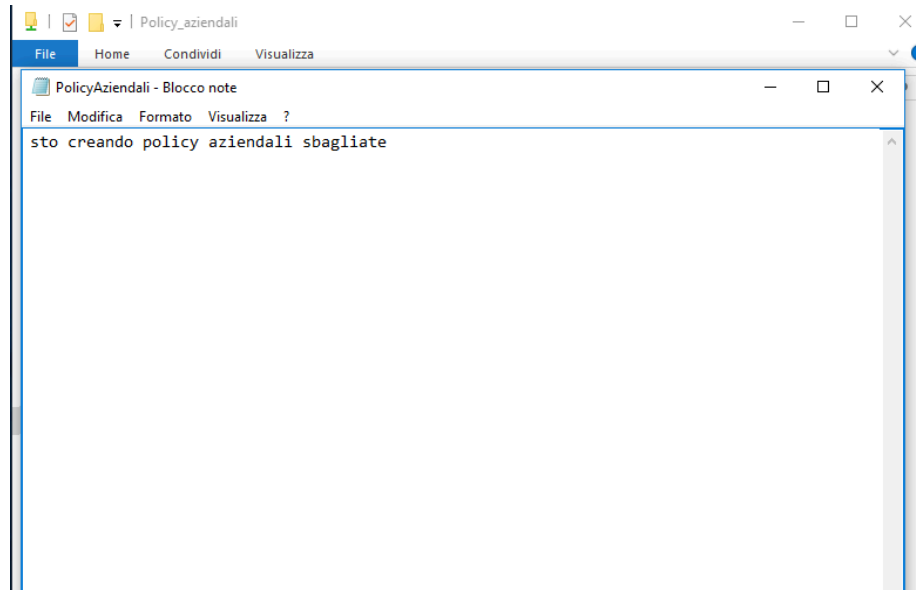
Proviamo ad accedere con questo utente alla cartella riservata agli amministratori IT



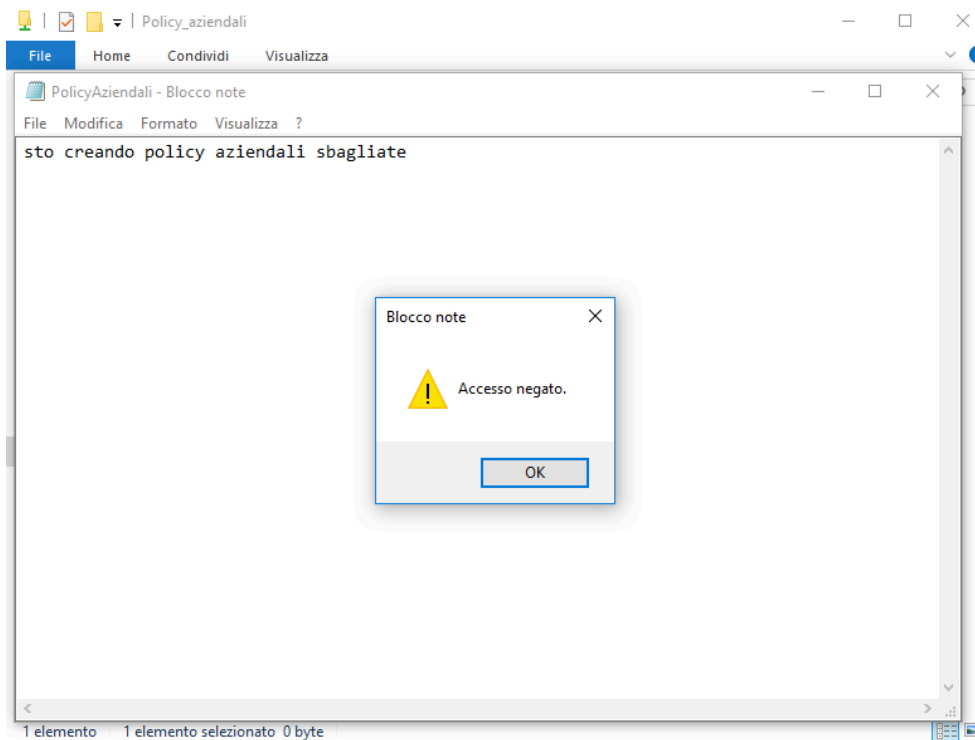
come da programma, ci viene negato l'accesso, ora andiamo a testare il permesso di lettura sul file precedentemente modificato nella sezione '**marketing**'



come vediamo il file era stato correttamente modificato e salvato, concludiamo andando a verificare i permessi di lettura e scrittura per le policy aziendali, Elena infatti dovrebbe essere in grado di vedere e leggere il file, ma non di modificarlo



proviamo a salvare le modifiche



L'accesso è stato correttamente **negato** a causa della mancanza del permesso di **modifica**.

Possiamo quindi considerare completato l'esercizio

BONUS

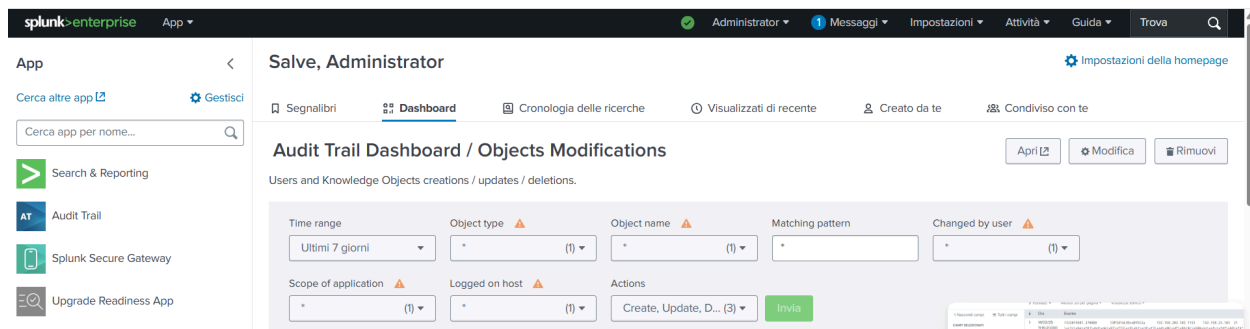
Bonus Obiettivo Lo scopo di questo esercizio è analizzare il seguente file di log con Splunk e :

1. Notare e documentare evidenze di anomalie o attacchi Esercizio Esercizio
2. Preparare un report TECNICO DETTAGLIATO per spiegare le remediation (non voglio tipo "installare MFA" ma voglio dei passi per implementare una soluzione, a livello pratico).

3. Creare una conclusione PER I MANAGER che indica brevemente le anomalie/attacchi coprire le situazioni (descritte dal file log).

SVOLGIMENTO

Per analizzare il file fornito utilizzeremo splunk enterprise, precedentemente installato, avviamo splunk



carichiamo il file direttamente dalla directory di destinazione

Input locali		
Tipo	Input	Azioni
Raccolta di log eventi locale Raccogliere log eventi da questo computer.	-	Modifica
Raccolte di log eventi remoti Raccogliere log eventi da host remoti. Nota: utilizza WMI e richiede un account di dominio.	1	+ Aggiungi nuovo/a
File e directory Indicizzare un file locale o monitorare un'intera directory.	19	+ Aggiungi nuovo/a
Monitoraggio prestazioni locali Raccogliere dati sulle prestazioni del computer locale.	0	+ Aggiungi nuovo/a
Monitoraggio prestazioni remoto Raccogliere informazioni su prestazioni ed eventi di host remoti. Sono necessarie le credenziali di dominio.	0	+ Aggiungi nuovo/a
Raccolta eventi HTTP Ricevere dati su HTTP o HTTPS.	0	+ Aggiungi nuovo/a

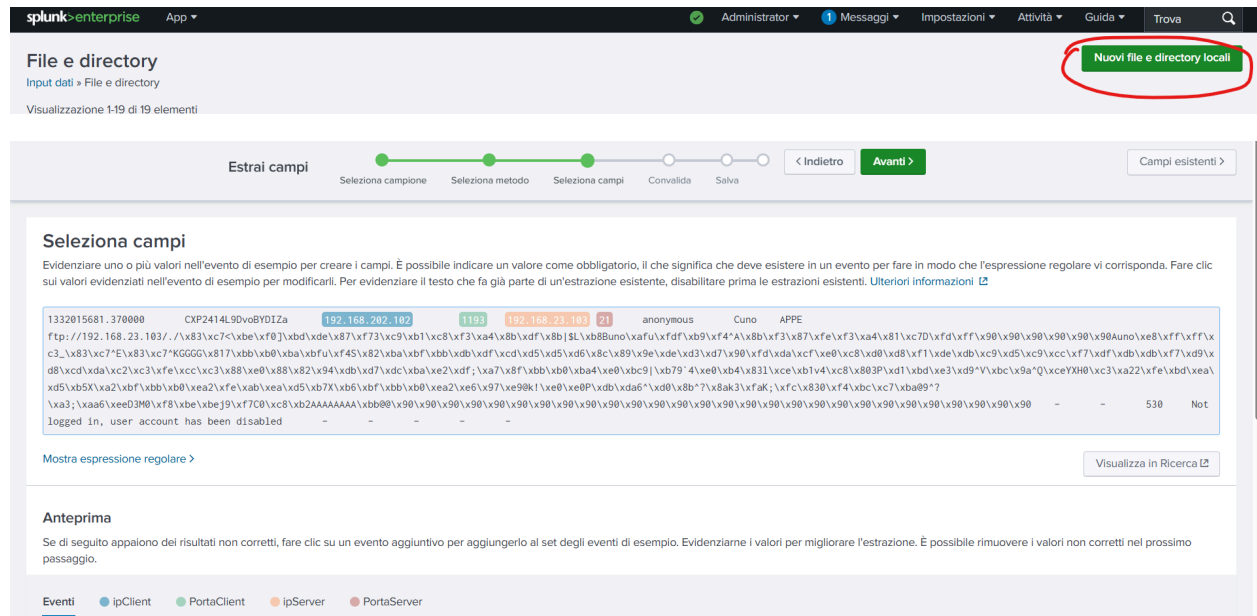
una volta avviata la ricerca possiamo istituire le nostre query per analizzare il file, ma per renderci più semplice il compito andiamo a creare/modificare i campi di ricerca e inseriamo

ipClient

ipServer

PortaClient

PortaServer



The screenshot shows the Splunk Enterprise interface. At the top, the navigation bar includes 'splunk>enterprise', 'App', and user roles like 'Administrator'. The main header is 'File e directory' with a sub-header 'Input dati > File e directory'. A red circle highlights the 'Nuovi file e directory locali' button. Below the header, a progress bar shows the steps: 'Seleziona campione', 'Seleziona metodo', 'Seleziona campi' (active), 'Convalida', and 'Salva'. The 'Seleziona campi' step is expanded, showing a list of fields with their values. The fields include IP addresses like '192.168.202.102' and file paths like 'CXP2414L9DvoBYDIZa'. The 'Mostra espressione regolare' button is visible. At the bottom, there is a legend for 'Eventi' with categories: 'ipClient', 'PortaClient', 'ipServer', and 'PortaServer'.

ora possiamo analizzare preventivamente con maggior facilità il file con il menù a tendina laterale,

notiamo subito che l'indirizzo IP

192.168.202.102

ha effettuato un totale di 5478 connessioni, il che lo rende sospetto, lo identificheremo da qui in poi come 'attaccante'

mentre il bersaglio sembra essere il server con IP

192.168.28.101

< Nascondi campi

Tutti i campi

CAMPI SELEZIONATI

a host 1

CAMPI INTERESSANTI

a index 1

a ipClient 15

a ipServer 21

linecount 1

PortaClient 95

PortaServer 1

a punct 100+

a source 1

a sourcetype 1

a splunk_server 1

a timestamp 1

+ Estrai nuovi campi

ipClient

15 Valori, 100% di eventi

Selezionato

Si

No

Report

Primi valori

Primi valori nel tempo

Valori rari

Eventi con questo campo

Primi 10 valori	Conteggio	%	
192.168.202.102	5.478	94,513%	
192.168.202.94	209	3,606%	
192.168.202.138	55	0,949%	
192.168.204.45	14	0,242%	
192.168.202.108	7	0,121%	
192.168.202.118	5	0,086%	
192.168.202.79	4	0,069%	
192.168.202.96	4	0,069%	
192.168.203.45	4	0,069%	
192.168.25.100	4	0,069%	

< Nascondi campi

Tutti i campi

CAMPI SELEZIONATI

a host 1

CAMPI INTERESSANTI

a index 1

a ipClient 15

a ipServer 21

linecount 1

PortaClient 95

PortaServer 1

a punct 100+

a source 1

a sourcetype 1

a splunk_server 1

a timestamp 1

+ Estrai nuovi campi

ipServer

21 Valori, 100% di eventi

Selezionato

Si

No

Report

Primi valori

Primi valori nel tempo

Valori rari

Eventi con questo campo

Primi 10 valori	Conteggio	%	
192.168.28.101	1.547	26,691%	
192.168.27.101	780	13,458%	
192.168.21.101	778	13,423%	
192.168.22.101	774	13,354%	
192.168.23.101	774	13,354%	
192.168.24.101	774	13,354%	
192.168.25.101	258	4,451%	
192.168.23.103	55	0,949%	
192.168.28.103	13	0,224%	
192.168.202.92	10	0,172%	

filtriamo quindi la nostra query per isolare le comunicazioni tra le due macchine

index=*_ OR index=* sourcetype=file_verifica ipClient="192.168.202.102" ipServer="192.168.28.101"

Ultime 24 ore

1.544 eventi (13/02/25 13:00:00,000 - 14/02/25 13:50:37,000)

Nessun campionamento degli eventi

Processo

Modalità interattiva

Eventi (1.544)

Pattern

Statistiche

Visualizzazione

Formato timeline

Zoom indietro

Zoom area selezionata

Deseleziona

Time Filter

Formato

Mostra: 20 per pagina

Visualizza: Elenco

< Prec

1

2

3

4

5

6

7

8

...

< Nascondi campi

Tutti i campi

AMPI SELEZIONATI

host 1

AMPI INTERESSANTI

index 1

ipClient 1

ipServer 1

linecount 1

PortaClient 2

PortaServer 1

punct 35

source 1

sourcetype 1

i	Ora	Evento
>	14/02/25 11:16:21,000	1331909396.160000 CVHmp01B6y1GqaAJje 192.168.202.102 4970 192.168.28.101 21 ftp password@example.com PASV - 227 Entering Passive Mode (192,168,28,101,190,7). T 192.168.202.102 192.168.28.101 48647 FymT07Uu2XCIsuux2 host = host_diagnosi
>	14/02/25 11:16:21,000	1331909396.160000 CVHmp01B6y1GqaAJje 192.168.202.102 4970 192.168.28.101 21 ftp password@example.com STOR ftp://1 1/dept/env/lib/python2.7/site-packages/flask/testsuite/test_apps/moduleapp/apps/admin/static/css/.ftpd854Us - - 550 /dept/e n2.7/site-packages/flask/testsuite/test_apps/moduleapp/apps/admin/static/css/.ftpd854Us: Operation not permitted - - T07Uu2XCIsuux2 host = host_diagnosi
>	14/02/25 11:16:21,000	1331909396.160000 CVHmp01B6y1GqaAJje 192.168.202.102 4970 192.168.28.101 21 ftp password@example.com PASV - 227 Entering Passive Mode (192,168,28,101,188,200). T 192.168.202.102 192.168.28.101 48328 FymT07Uu2XCIsuux2 host = host_diagnosi

andando a verificare i log con una breve analisi notiamo che il nostro presunto attaccante lancia principalmente tre tipi di operazioni

PASV

ovvero il tentativo di aprire una connessione ‘passiva’ sulla porta 21, questi tentativi sembrano andare a buon fine, il server infatti apre una connessione su una porta specifica che viene comunicata al presunto attaccante al fine di trasmettere traffico via tcp

STORE

questo comando serve a trasferire dati tramite protocollo ftp, non conosciamo la natura di questi ma siccome siamo in ambito di sicurezza informatica e conosciamo l’anomalia riguardo il numero di tentativi, possiamo presumere si tratti di malware o altre applicazioni pericolose.

DELE

questo comando serve ad eliminare file da una specifica directory, con una breve ricerca su google possiamo vedere come questo tipo di comportamento sia tipico degli hacker o degli script da loro utilizzati, che prima caricano un file sul pc target e poi lo eliminano

(magari dopo averlo eseguito, o al solo scopo di vedere se l'upload funziona) al fine di eliminare qualsiasi traccia in attesa dell'attacco vero e proprio.

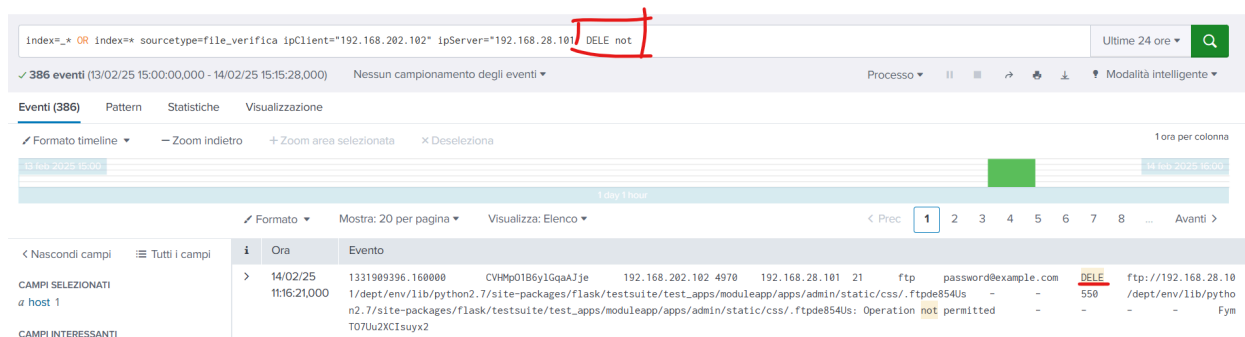
CONCLUSIONI

il comportamento del nostro presunto attaccante risulta notevolmente sospetto e ci lascia concludere che si tratti con ogni probabilità di un tentativo di hacking al server **192.168.28.101**

operato dalla macchina attaccante

192.168.202.102

Per completezza analizzando le operazioni eseguite e inserendo come filtro **STOR** o **DELE** uniti alla parola 'not' possiamo notare come il numero delle richieste risulti sempre 368, il che significa che nessun tentativo dell'hacker di caricare i file potenzialmente malevoli ha avuto successo.



MITIGAZIONI POSSIBILI A COSTO 0

Come possibili mitigazioni mi limiterò ad elencare quelle facilmente eseguibili/gestibili senza l'impiego di costi aggiuntivi, esclusi quelli per il tecnico che esegue l'operazione in caso l'azienda non ne disponga di uno.

1. monitoraggio porta target e blocco IP

Come abbiamo notato l'attaccante prende di mira esclusivamente la porta FTP, i tentativi di stabilire una connessione vengono realizzati con successo perciò, oltre a banalmente **bloccare l'accesso da parte di quel determinato IP al server**, bisognerebbe effettuare un futuro monitoraggio delle connessioni al servizio per identificare altri comportamenti sospetti o frequenti che potrebbero indicare la presenza di uno o più attacchi e permettere all'azienda di rispondere tempestivamente o adottare misure più restrittive, nel caso non si tratti di un caso isolato

per bloccare l'accesso all'IP incriminato è sufficiente escluderlo dalla regola di traffico lecito presente nel firewall, il processo differisce a seconda del firewall utilizzato.

2. Modifica e revisione dei permessi

Il motivo per il quale il nostro attaccante non è riuscito nell'intento è probabilmente perché non possiede i permessi per caricare o cancellare file nella directory bersagliata. Si consiglia all'azienda di rivedere con cura le policy di utilizzo dei dati sensibili e delle directory poste in condivisione. Anche se per ora ha funzionato, non significa che l'hacker non riesca in futuro a trovare il metodo per caricare i file in altre directory che magari hanno l'accesso di default al gruppo 'everybody', come abbiamo visto nei giorni precedenti. Consiglierei anche di valutare il livello di sicurezza in merito agli attacchi noti inerenti le privilege escalation, nel caso l'hacker decidesse in futuro di tentare questa strada.

Nello specifico, la cartella di destinazione identificata dal report va esclusa **ASSOLUTAMENTE** con i procedimenti visti nel primo esercizio, dalla possibilità di essere modificata da alcun utente che non ne abbia strettamente necessità di modifica per scopi aziendali.

possiamo completare l'operazione interamente dalla gestione del server con un utente Admin.

3. Potenziamento sicurezza delle password utenti

L'Hacker era in grado di connettersi al servizio tramite password, perciò, anche se non conosciamo il modo in cui ne è venuto in possesso, possiamo comunque preventivamente rinforzare la sicurezza andando ad aumentare i criteri di sicurezza richiesti nella scelta delle password da parte dei dipendenti, e formare inoltre, su come queste non debbano essere assolutamente condivise in maniera inappropriata CON NESSUNO al fine di prevenire il furto delle credenziali anche per via 'non informatica'.

i criteri uniformemente più utilizzati per rendere maggiormente sicura una password sono:

- l'inserimento di numeri e simboli
- lunghezza di almeno 16 caratteri
- deve contenere lettere maiuscole e minuscole,

4. Verifica integrità del server

il log che abbiamo analizzato **non** mostra l'intero storico della vita della macchina in questione, perciò potrebbe essere opportuno effettuare una scansione approfondita delle directory e servizi del server target, al fine di escludere che la macchina non sia già stata **precedentemente infettata** in passato con malware che potrebbero consentire accessi esterni o peggio.

5. Modifica delle regole del firewall

Se l'azienda ha già implementato un firewall allora vanno riviste le impostazioni dello stesso ed eventualmente rese più restrittive per consentire l'accesso esclusivamente agli utenti autorizzati secondo i criteri di preferenza. Oltre all'esclusione dell'ip come già menzionato, possiamo ridurre la gamma di utenze concesse al server e/o impostare delle regole

specifiche per bloccare indirizzi con comportamenti particolari, come l'invio di moltissime richieste ad una singola porta o server.

MITIGAZIONI CONSIGLIATE

Nel caso si tratti di un'azienda con disponibilità economica sufficiente, la mia raccomandazione primaria sarebbe quella di instaurare un

IPS

ossia un sistema di monitoraggio e prevenzione **in tempo reale** che non solo permetta una più tempestiva analisi dei log effettuati, ma sia anche in grado di, ad esempio, bloccare un indirizzo IP consecutivamente ad un elevatissimo numero di richieste, proprio come nel nostro caso, anche se a discapito di un possibile rallentamento delle comunicazioni server-client

DANIELE BALANI