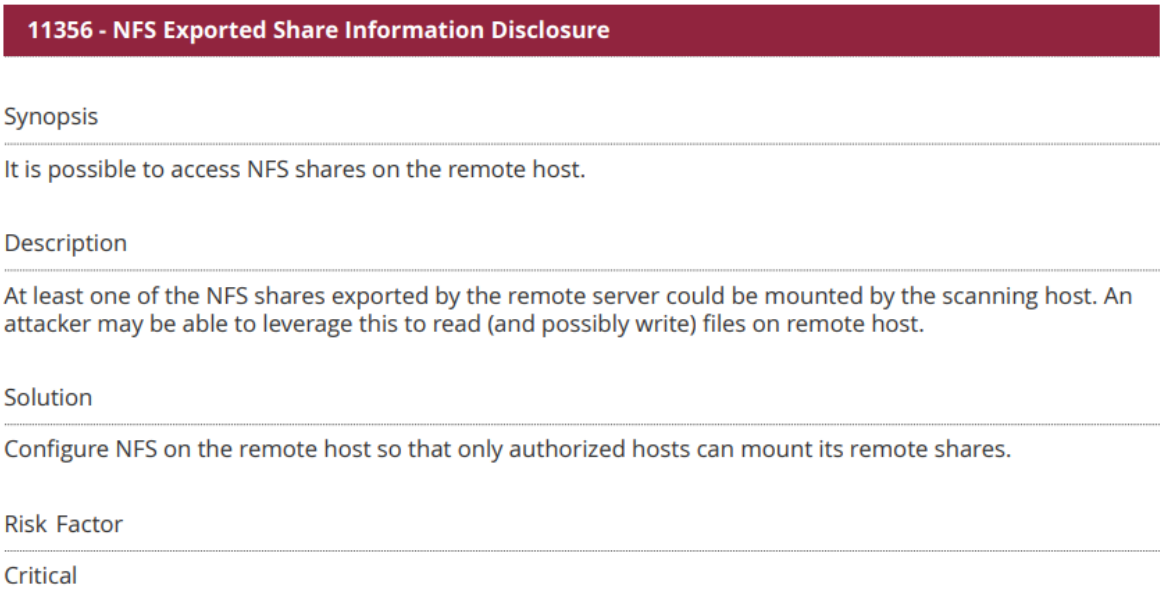
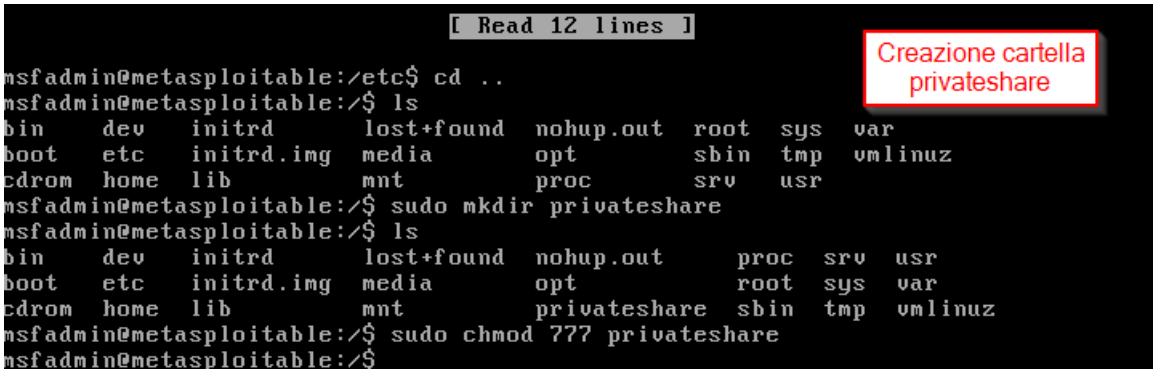
ESERCIZIO W12D4

La seconda parte del progetto di fine modulo verte sul risolvimento da 2 fino 4 vulnerabilità trovate con il Vulnerability scanner Nessus. Una volta conclusa la scansione, e esportato un report inziale, non ci resta apportare modifiche.

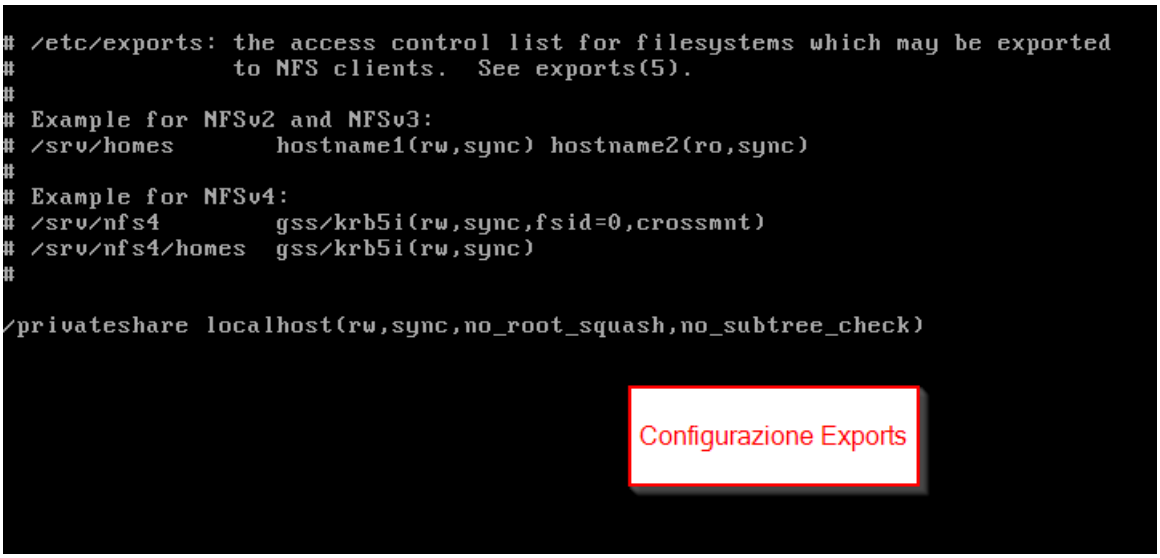
Prima vulnerabilità



Secondo lo scanner, il servizio NFS espone gran parte delle directory, rendendole di fatto montabili su sistemi client esterni. Non dovrebbero essere accessibili da tutti, ma solo dall'utenza autorizzata. Per correggere questa vulnerabilità andiamo a cambiare la configurazione del servizio NFS direttamente da dentro Metasploitable. Andremo a creare una cartella privata con mkdir e la renderemo visibile solo da localhost.



Una volta fatto, accediamo al file di testo localizzato in /etc/exports. Usiamo sudo nano per aprire il foglio e specifichiamo la cartella privateshare come usufruibile solo da Metaploitable.



Salviamo le nuove impostazioni e riavviamo Metaploitable2. Piu tardi useremo un'altra volta il Vulnerability Scanner, ma ci accertiamo lo stesso della scongiurata vulnerabilità, andando ad effettuare un tentativo di montaggio sulla macchina attaccante. Creiamo una cartella mount per la condivisione, dentro la directory temp.

sudo mount -t nfs 192.168.50.100:/privateshare /tmp/mount -nolock è la sintassi che ci consentirà di tentare un montaggio di rete:

- mount viene utilizzato per montare un file system
- -t nfs indica il tipo di file system da montare, in questo nfs
- 192.168.50.100:/privateshare specifica l'indirizzo IP del server NFS e la directory condivisa da montare.
- /tmp/mount specifica il punto di mount locale in cui verrà montata la cartella condivisa.
- -nolock specifica che il mount deve essere effettuato senza il lock manager NFS.

Da come si evince dallo screenshot, non è stato possibile completare il montaggio di rete perché il server ha vietato l'accesso alla macchina attaccante.