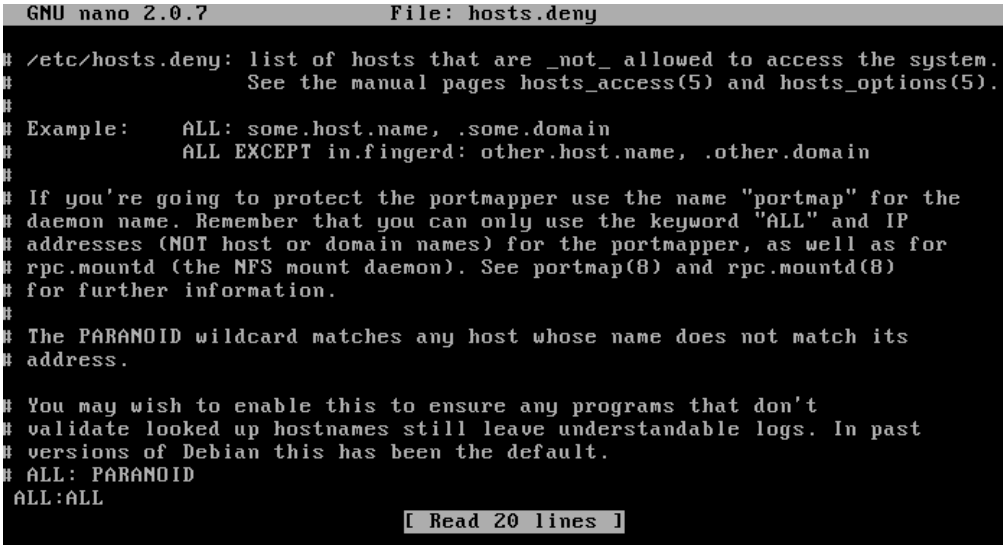
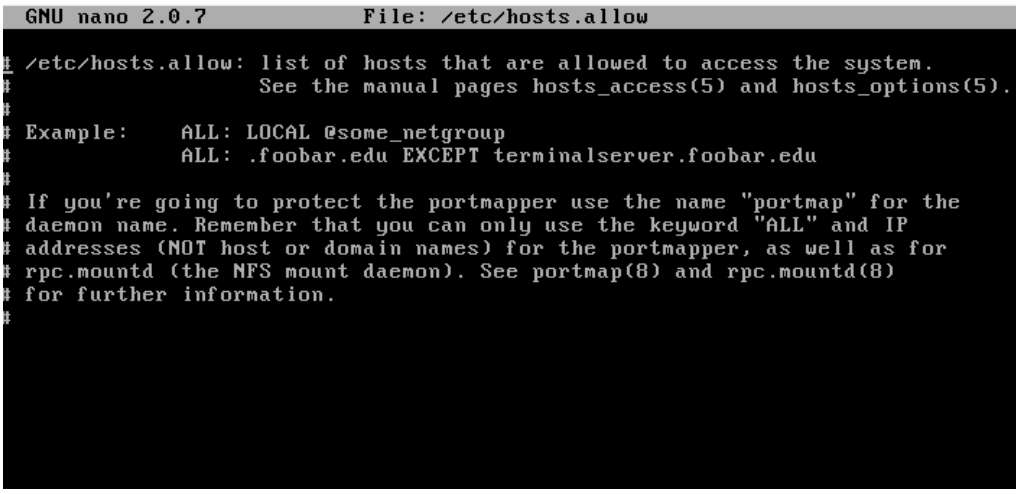
REPORT REMEDIATION

11356 - NFS Exported Share Information Disclosure

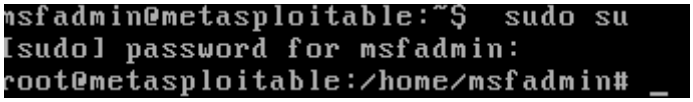
Per risolvere questa criticità sono andato a modificare il file hosts.deny ed il file hosts.allow nella cartella etc che controllano i TCP Wrappers, un insieme di funzioni utili per gestire gli accessi al vostro sistema dall'esterno. In questo caso ho modificato le regole cancellando nel file allow il ALL:ALL che permetteva a tutti gli host di accedere e mettendo ALL:ALL in deny per proibire a qualunque host di connettersi. Ovviamente in ottica aziendale i file aziendali verranno modificati per permettere a chi ha il permesso di accedere.



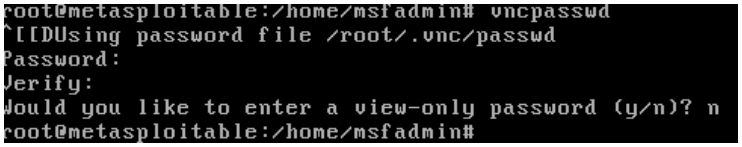


61708 - VNC Server 'password' Password

Seguendo le indicazioni indicazioni risolutive scritte nel report di Nessus sono andato a cambiare la password del servizio VNC che era molto debole. Per prima cosa ho fatto sudo su per avere i privilegi di root:

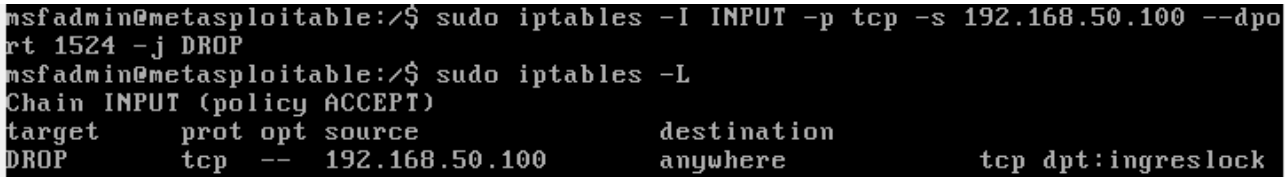


Dopodichè ho lanciato il comando vncpasswd per potere cambiare la password e sono andato ad inserire la nuova password più sicura:



51988 - Bind Shell Backdoor Detection

Per ovviare al problema della backdoor sono andato a modificare le firewall policies di meta tramite il comando iptables:



In questo modo la macchina Metasploitable non accetta comunicazioni in entrata provenienti dall'IP 192.168.50.100 per il protocollo TCP sulla porta 1524.