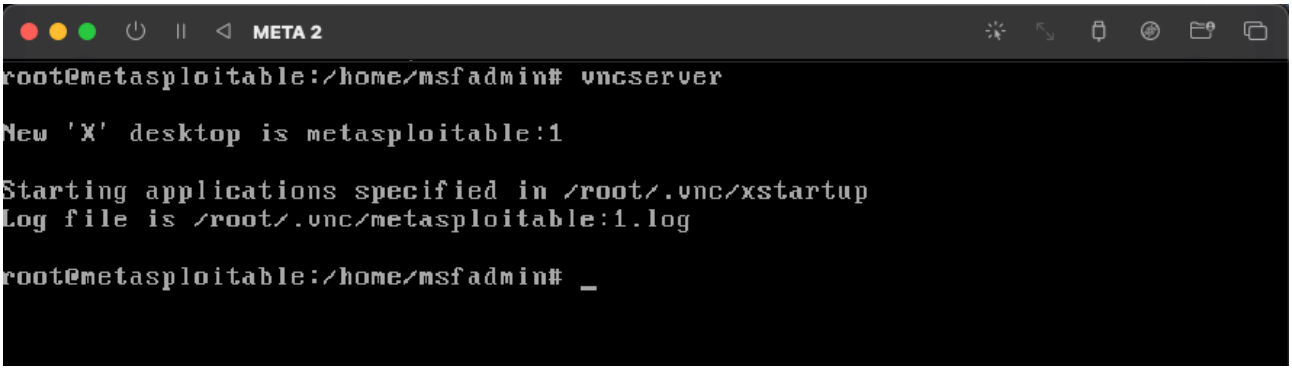
Edoardo Ceriani

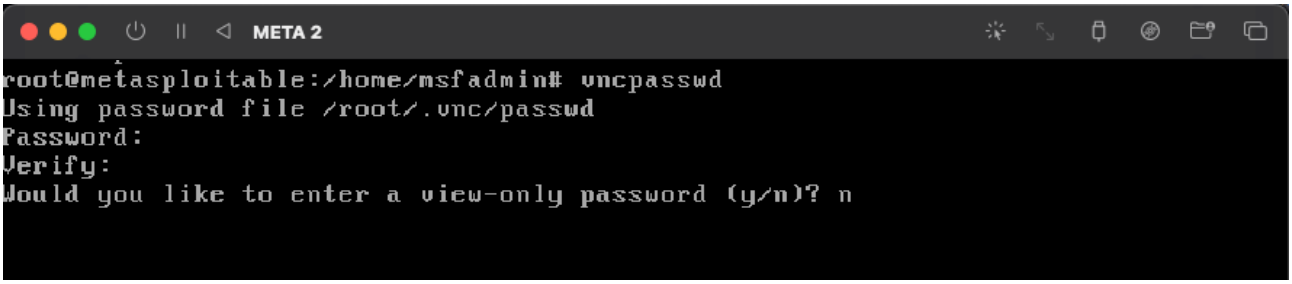
REMEDIATION

VNC SERVER 'PASSWORD' PASSWORD

Per risolvere questa vulnerabilità bisogna impostare una nuova password più sicura per il server VNC.

Per fare ciò, da terminale, eseguo il comando ‘sudo su’ per avere tutti i privilegi da amministratore; successivamente eseguo il comando ‘vncserver’ per avviare il server VNC.; a questo punto con il comando ‘vncpasswd’ mi viene data la possibilità di inserire una nuova password; scelgo quindi la password 9!*%38!B tramite un tool online di creazione password sicure che comprende numeri, simboli e caratteri. Avrei voluto inserire una password più lunga per avere una maggiore sicurezza, ma veniva accettata solo una password di massimo otto caratteri.

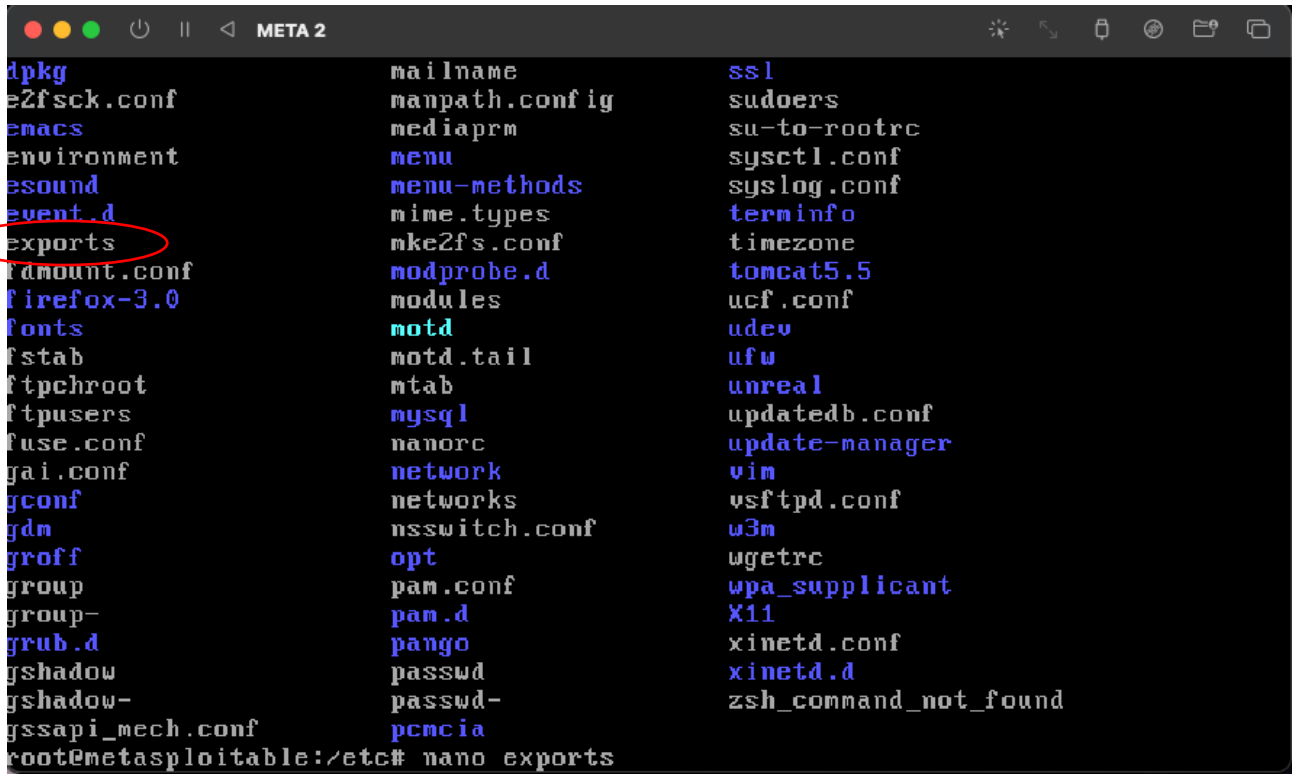


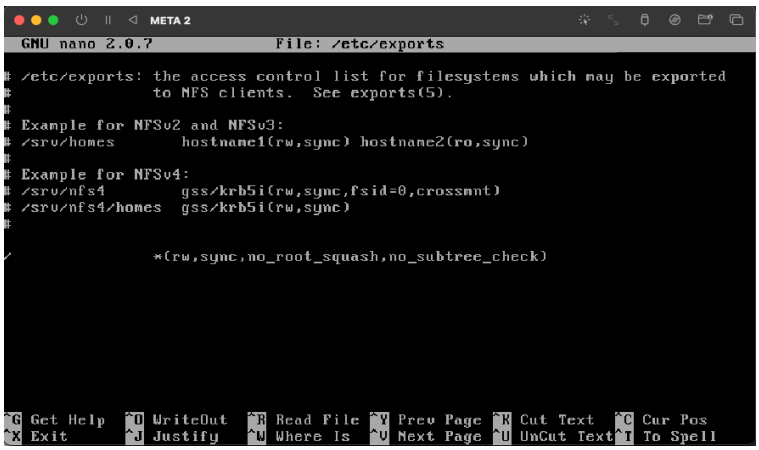


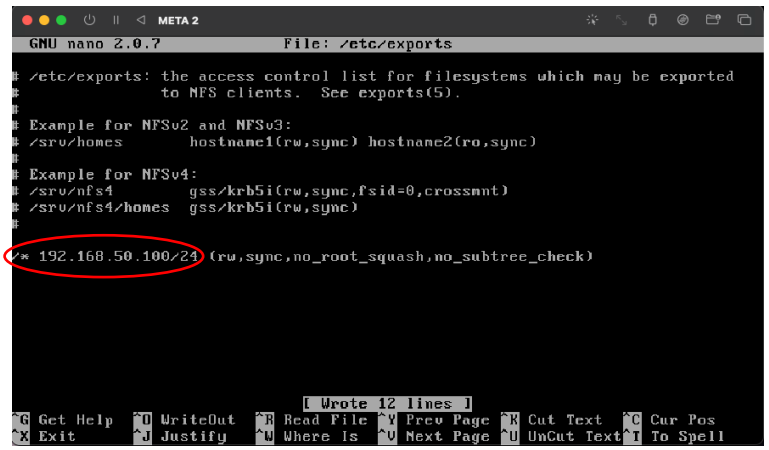
NFS EXPORTED SHARE INFORMATION DISCLOSURE

Per risolvere questa vulnerabilità bisogna limitare gli host che possono accedere alle cartelle condivise.

Per fare ciò, tramite il comando ‘cd /etc’ mi sposto nella directory etc e guardo tutte le directory/file presenti al suo interno con il comando ‘ls -A’; apro quindi il file exports per poterlo modificare con il comando ‘nano exports’; nell’ultima riga aggiungo ‘192.168.50.100/24’ per far sì che solo la rete interna possa accedere alle cartelle esportate e salvo il file modificato.







BIND SHELL BACKDOOR DETECTION

Per risolvere questa vulnerabilità bisogna chiudere la porta a cui è associato il servizio incriminato. Per fare ciò, guardando il report della scansione di Nessus, noto che la porta da chiudere è la 1524; per una ulteriore verifica, da Kali eseguo una scansione con nmap sulla porta 1524 con il comando 'nmap -sV -p 1524 192.168.50.101' che mi conferma quanto riportato da Nessus riportando inoltre il servizio e la sua versione; a questo punto, da terminale su Meta eseguo il comando 'iptables -I INPUT -p tcp –dport 1524 -j DROP' per aggiungere una nuova regola di firewall per bloccare il traffico in entrata sulla porta 1524 utilizzando il firewall di linux iptables; eseguo quindi il comando 'iptables -L' per verificare la presenza della nuova regola. Per avere una verifica prima di eseguire una nuova scansione con Nessus, eseguo nuovamente nmap su Kali che, correttamente, mi restituisce lo stato della porta come filtrata e non fornisce informazioni riguardo il servizio in ascolto.