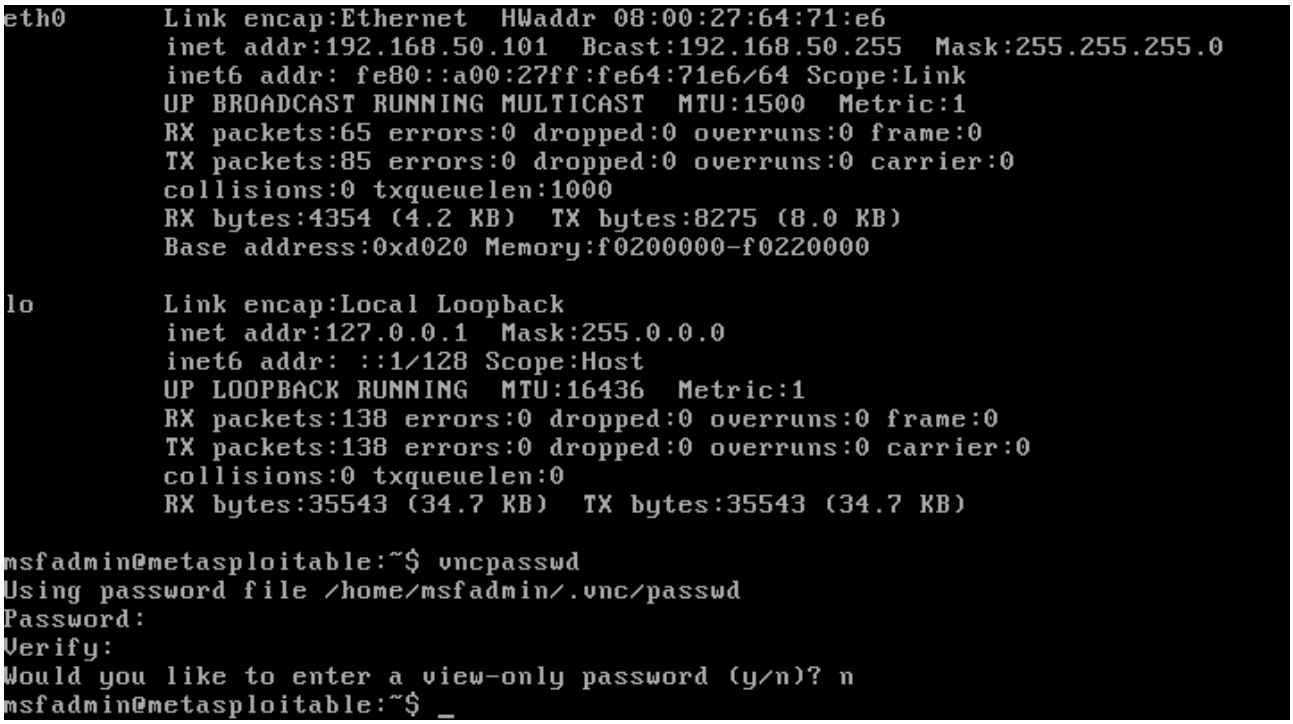
Report Esercizio REMEDIATION 01/06/2023

Ho avviato le macchine Kali Linux e Metasploitable, ho verificato pingassero, dopodichè ho fatto il login su Nessus e ho aggiunto una nuova scansione. Ho deciso di utilizzare la Basic Scan, dove ho impostato i paramentri di scan su tutte le porte. Ho avviato la scansione e a fine processo, dopo aver individuato le vulnerabilità critiche presenti in lista vulnerabilità di Nessus, ho provveduto ad iniziare la fase di Remediation.

Per prima cosa ho cambiato la password VNC.



Secondo step è stata l'eliminazione della backdoor entrando nel file sudo nano /etc/inetd.conf, ho eliminato l'ultima stringa che consentiva l'accesso.

Terzo step ho modificato i privilegi del server NFS entrando nel file sudo nano /etc/exports dove ho eliminato la stringa tra parentesi tonde, che permetteva l'accesso da remoto a qualsiasi root user.