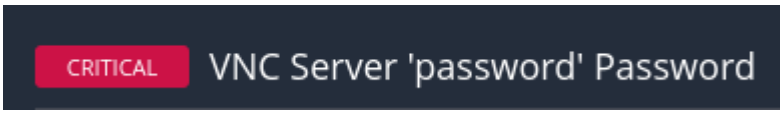
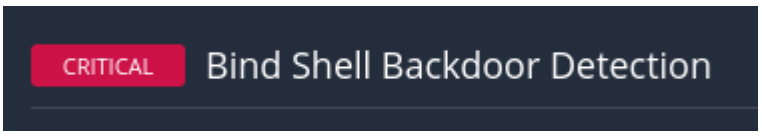
# *Vulnerability Test on Metaspoitable 2*

***Tramite l'uso del software Nessus su Kali(Linux) ho eseguito un vulnerability scan della macchina virtuale Metaspoitable 2 che ha dato come risultato il report che trovate in allegato su GitHub.***

***Successivamente ho preso in considerazione 2 vulnerabilità a rischio "Critico" e una a rischio "Alto" e ho analizzato essa e proposto una soluzione:***

1. 


   ***Descrizione:***
   *La password usata per il Server VNC e "password", una password troppo comune e facilmente scavabile.*
   ***Soluzione:***
   *Utilizzare una password più complessa alternando numeri, lettere e caratteri speciali.*

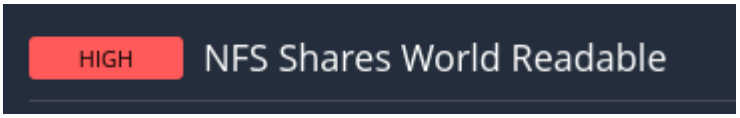
2. 


***Descrizione:***

*È presente una backdoor che permette ad un attaccante esterno di collegarsi e inviare comandi senza richiedere nessuna autenticazione.*

***Soluzione:***

*Chiudere la porta e/o terminare il processo legato alla shell in cui è presente la backdoor. E consigliato anche eseguire una scansione antivirus.*

3. 


***Descrizione:***

*Il server NFS remoto sta condividendo file o risorse in modo che chiunque possa accedervi senza restrizione specifiche.*

***Soluzione:***

*Modificare  la configurazione del server NFS per permettere l'accesso applicando restrizioni basate su IP.*