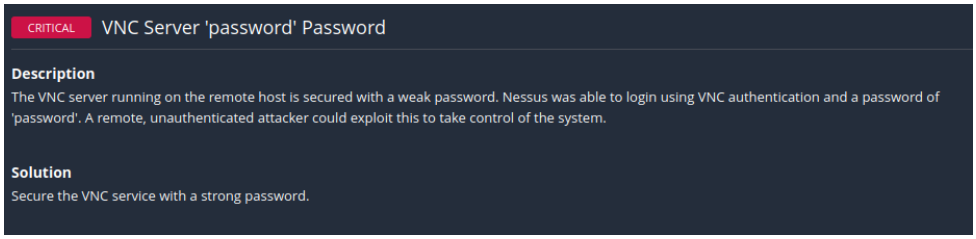
S5 L4 NESSUS

In questo esercizio, abbiamo utilizzato l'applicativo NESSUS.

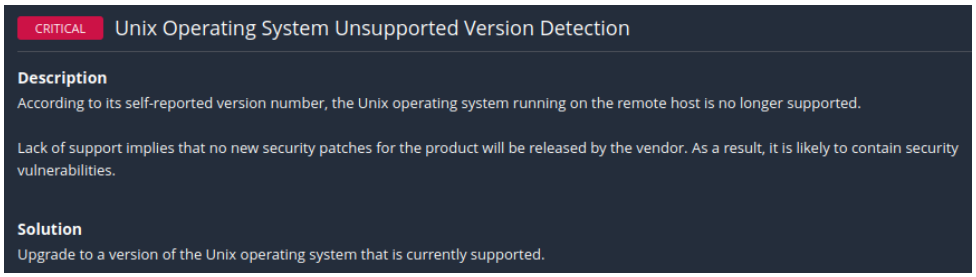
Abbiamo effettuato una "BASIC NETWORK SCAN", delle well know ports verso l'ip di metasploit.

Ottenendo come risultato delle vulnerabilità, divise per gravità.

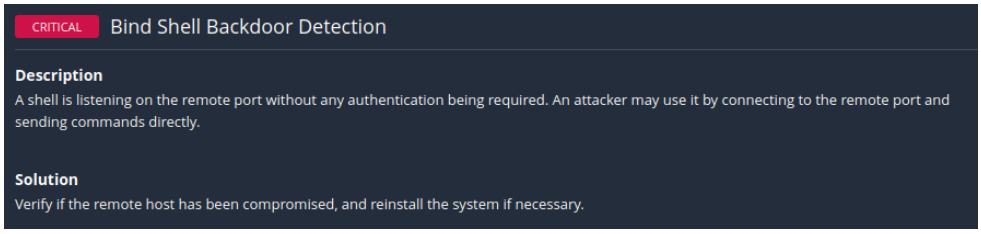
Sotto riportiamo 4 delle più gravi.



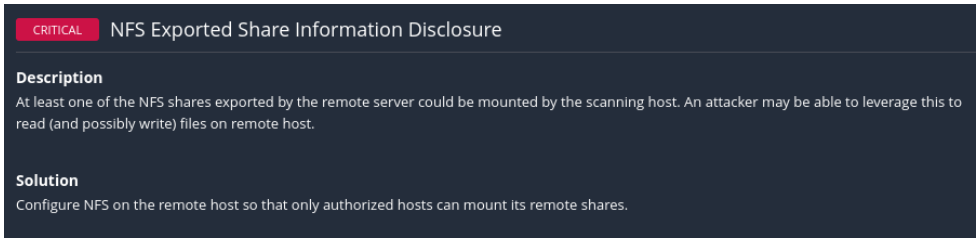
Il servizio VNC, permette il controllo remoto di un host. In questo caso, ci indica di utilizzare un password più efficace, poiché un malintenzionato, potrebbe prendere facilmente controllo dell'host in questione.



Qui indica, invece, che stiamo utilizzando una versione di Unix non recente, pertanto, consiglia di aggiornarla in modo tale da avere le ultime patch di sicurezza disponibili.



Bindshell permette di accedere all'host senza bisogno di alcuna autenticazione.



NFS(NETWORK FILE SHARING), riguarda la possibilità, di condividere file e cartelle con altri client linux nella rete. Pertanto rende facile, attivare la condivisioni di file e quindi rubarne il contenuto.