## **Nessus**

A seguito di una scansione delle vulnerabilità di un sistema Metasploitable sono state trovate svariate vulnerabilità alcune più critiche altre meno

Nel documento successivo analizzeremo 3 di queste criticità e cercheremo di mitigare il rischio di questecriticità

La prima criticità in questione è legata al Server VLC



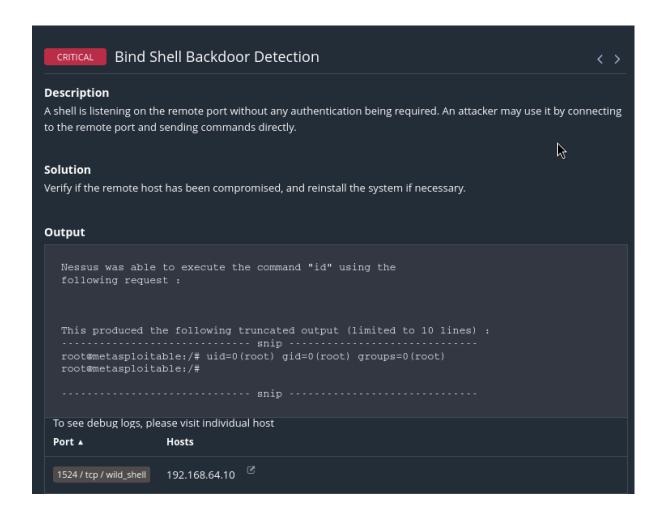
Come è possibile notare attraverso nessus è stato molto semplice exploitare la password del server.

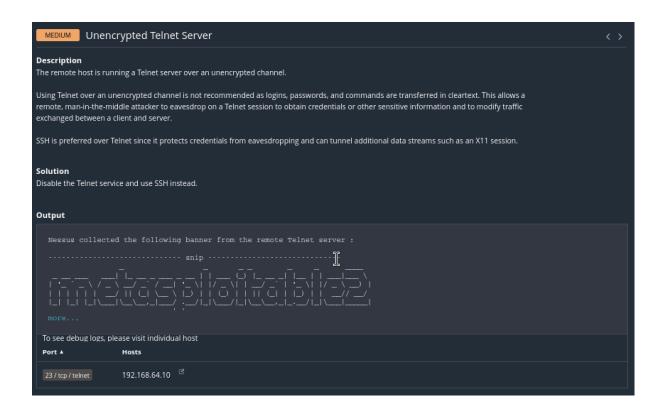
La soluzione a questo tipo di criticità è l'utilizzo di una password più sicura.

Nel report viene evidenziata un'altra criticità importante, una backdoor.

Questa porta potrebbe essere inutilizzata, se questo è il caso per limitare il rischio di un possibile exploit attraverso questa porta l'ideale sarebbe disattivarla.

Questo tipo di criticità è possibile evidenziarla anche attraverso il software nmap, individuando esattamente la backdoor aperta ovvero la 1524.





Questo tipo di vulnerabilità è dovuta al fatto che la comunicazione attraverso questa porta non è criptata quindi è preferibile disattivarla oppure utilizzare una porta criptata come la SSH. Non essendo una porta criptata trasmette tutte le informazioni in chiaro, quindi è possibile che vengano trasmessi dati sensibili in chiaro.