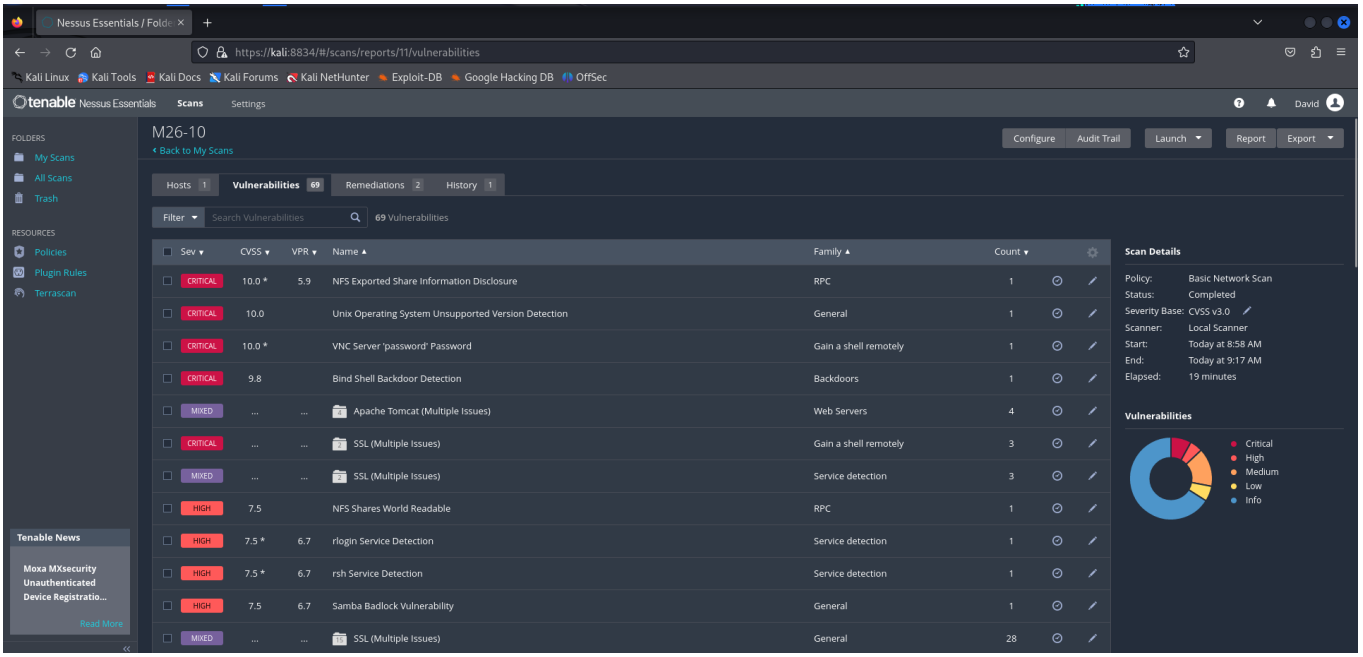
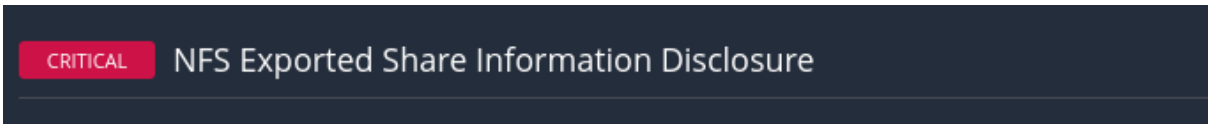
Report M26-10

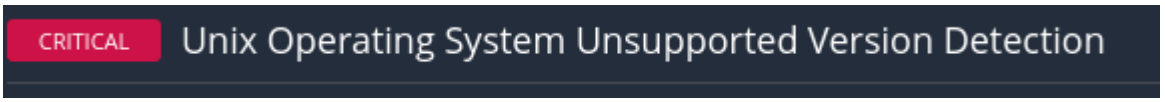


Abbiamo effettuato una scansione, con Nessus, sulla macchina Metasploitable indicando come target solo le parti comuni.
in questo caso troviamo 5 vulnerabilità critiche, di cui andremo tra poco a vedere il loro contenuto.

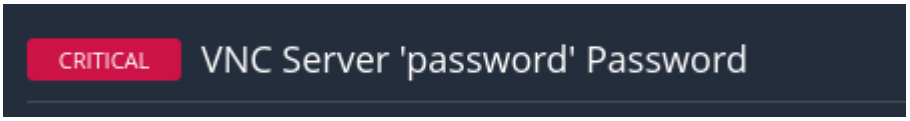
Vulnerabilità:



La prima vulnerabilità che troviamo è “NFS Exported share information Disclosure”, dove ci avvisa che un utente malintenzionato potrebbe accedere alla condivisione NFS sull’host in remoto.
Nessus ci suggerisce di configurare NFS in modo tale che solo host autorizzati possano accedervi.



La seconda vulnerabilità che vediamo è “Unix operating system unsupported version detection”, Nessus ci avvisa che la versione del sistema operativo Unix non è più supportato. Di conseguenza è probabile che contenga vulnerabilità per il fatto che non ci sono patch.
Ci suggerisce di eseguire un upgrade a una nuova versione del sistema operativo.



La terza vulnerabilità che vediamo invece è “VNC server ‘password’ password”. Ci avvisa dicendo che la password è debole e che potrebbero prendere controllo del sistema facilmente.
Così Nessus ci suggerisce di proteggere con una password complessa il servizio VNC.

L'ultima vulnerabilità che vediamo è “Bind shell backdoor detection”. Qui ci avvisa che un malintenzionato potrebbe collegarsi alla porta remota senza alcuna autenticazione.
Nessus ci suggerisce di controllare se l’host è stato compromesso e se necessario reinstallare il sistema.