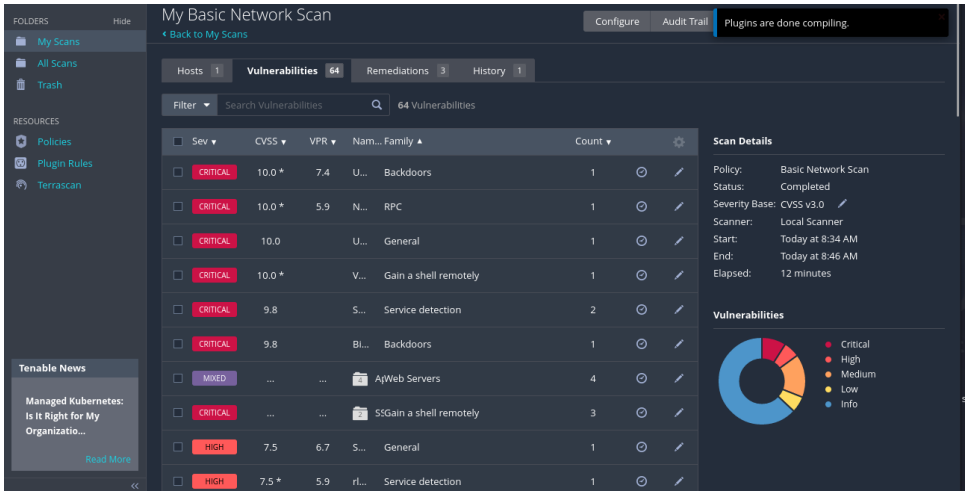
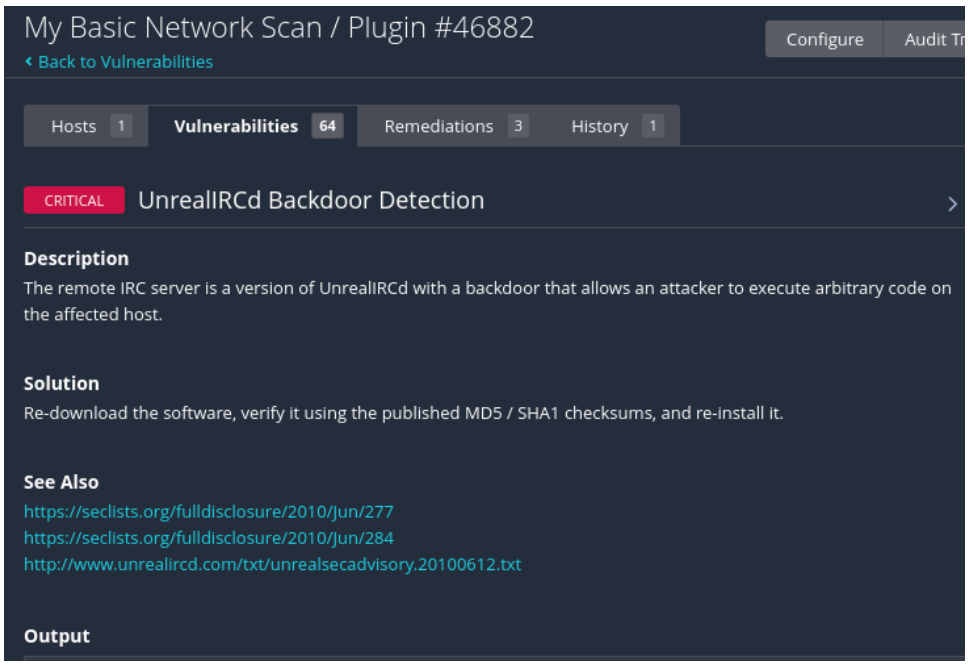
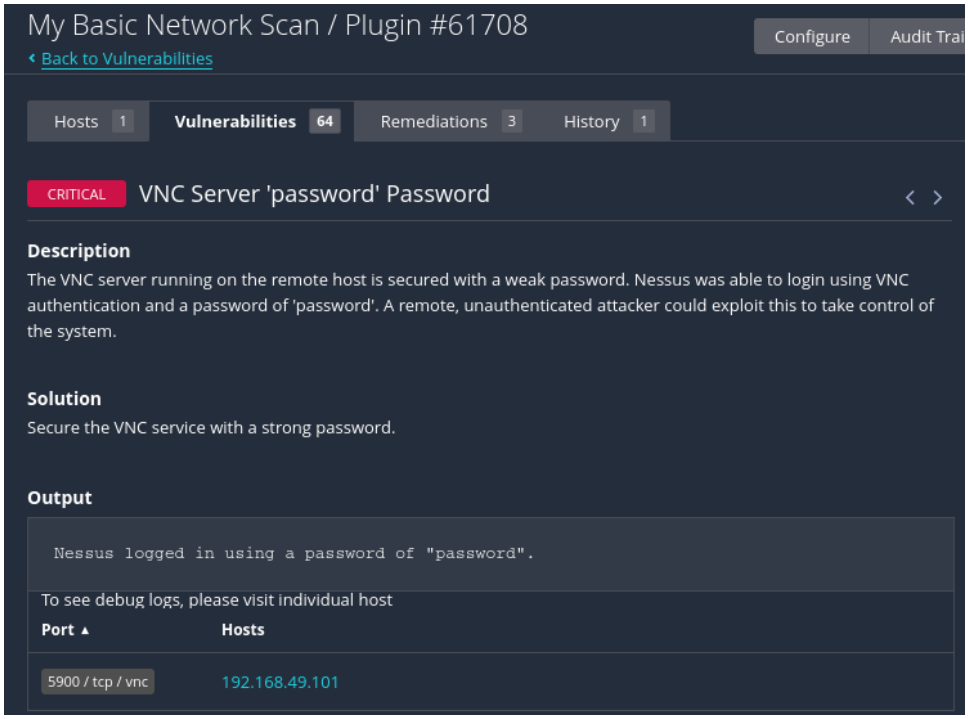


Al fine della scansione è stato generato anche un report con le vulnerabilità.



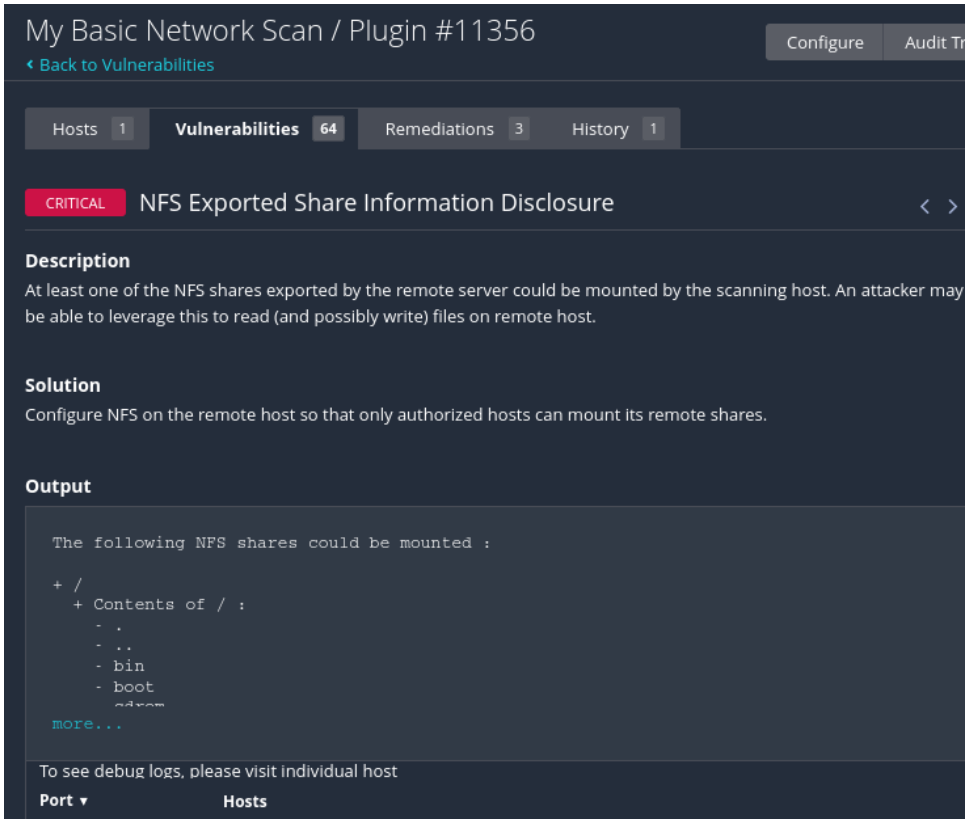
Prendiamo come esempio questa criticità UnrealIRCd Backdoor Detection
Aprendo il primo link possiamo dedurre che la versione 3.2.8.1 di UnrealIRCd è stata compromessa con una backdoor, come rivelato da una comunicazione inviata alla lista di distribuzione "irc-security". Questo errore consente a un aggressore di eseguire comandi arbitrari sul sistema ospitante il server IRC, ponendo a rischio la sicurezza e la privacy degli utenti.



Analizziamo quest altro errore critico, VNC Server ‘password’ Password

In pratica, ci dice che il server VNC è protetto da una password debole, in quanto quest’ultima è ‘password’ ed un attaccante potrebbe facilmente entrare.

Per risolvere l’errore è consigliabile: Modificare immediatamente la password predefinita del server VNC utilizzando una password robusta e unica. La password dovrebbe essere lunga, complessa e contenere una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali.



Osservando questa criticità *(*NFS Exported Share Information Disclosure*)*
osserviamo che almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere "montato" dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) file sull'host remoto.

Per risolvere questo errore è consigliabile: Modificare la configurazione di NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote. Questo può essere realizzato tramite l'implementazione di restrizioni di accesso basate su indirizzi IP o domini.