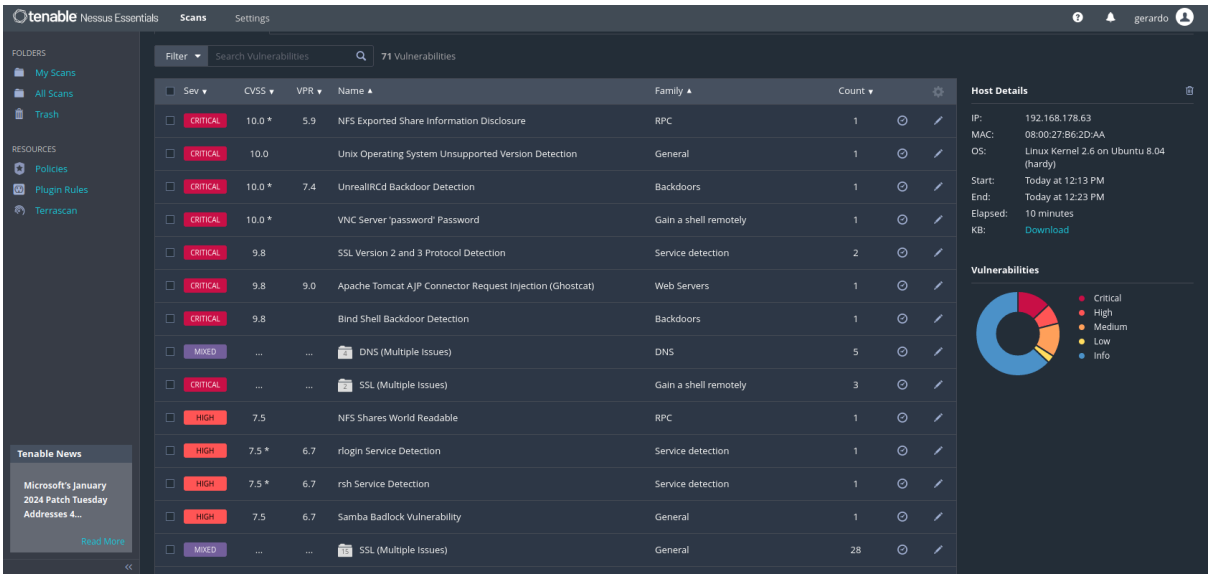
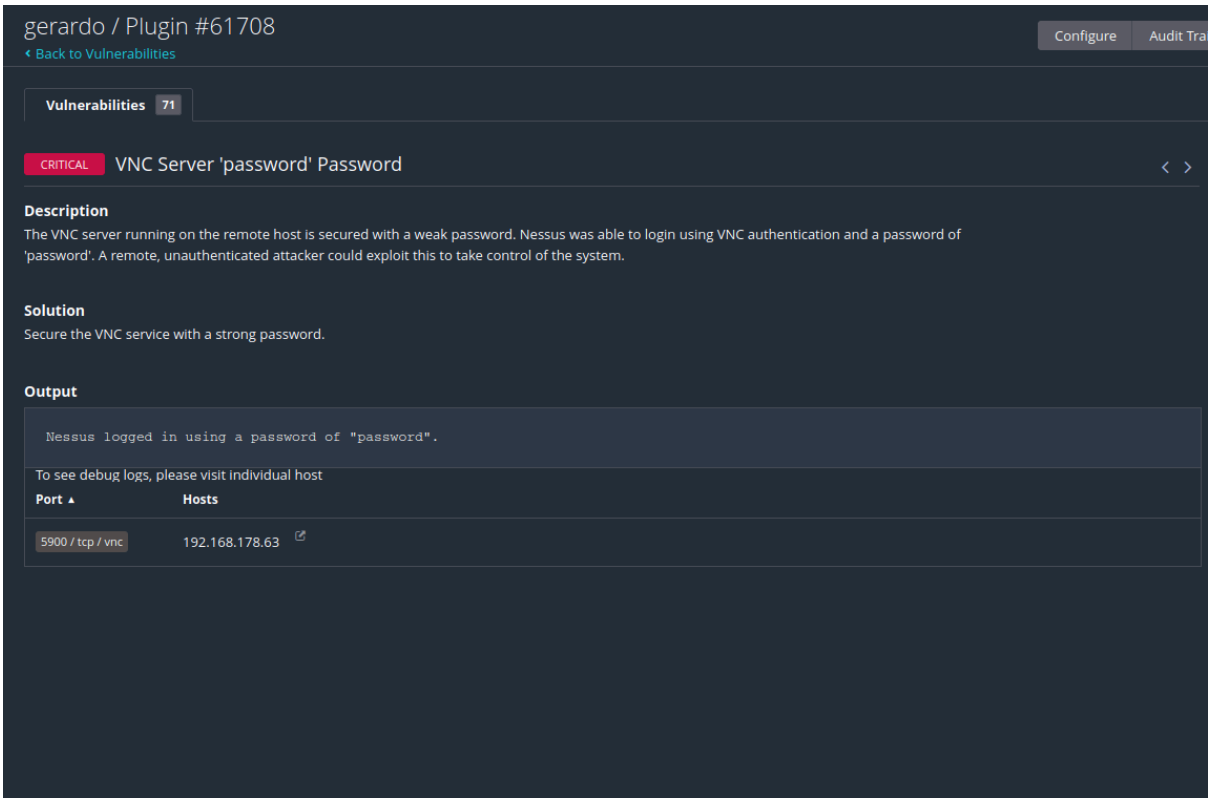
# SCAN CON NESSUS



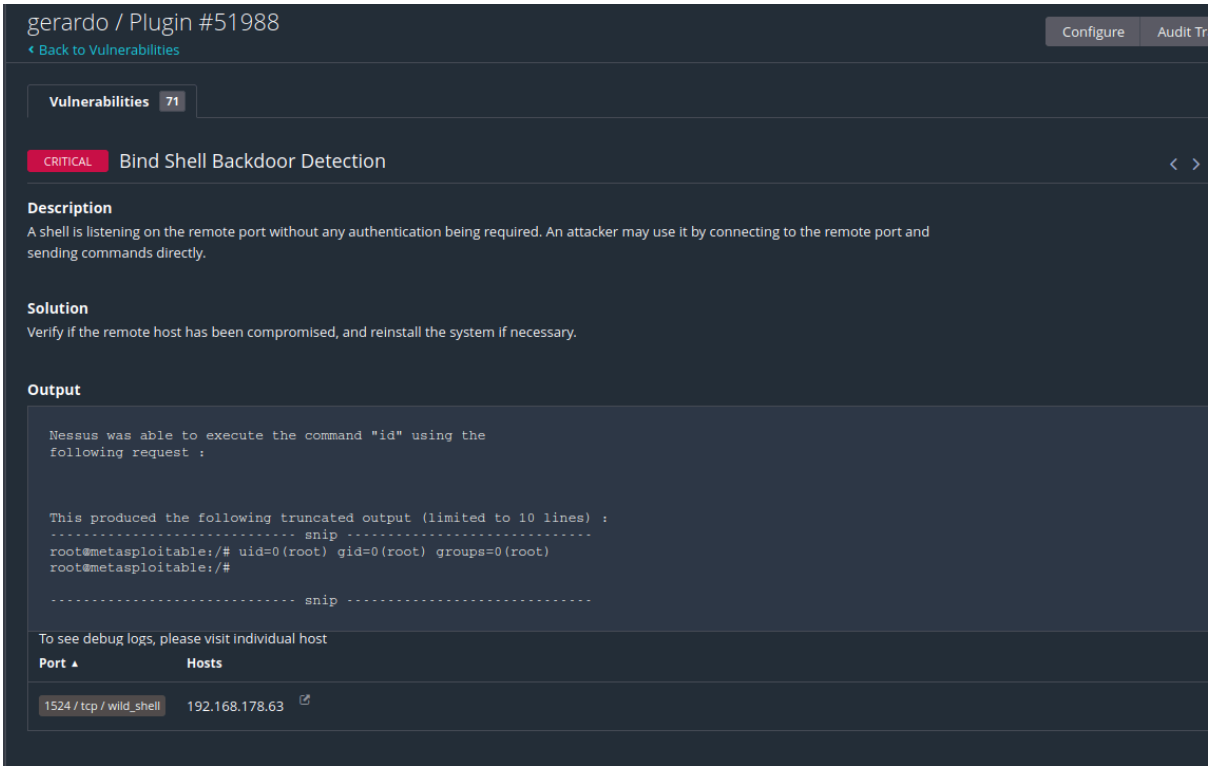

# 1 VULNERABILITA’




**Il messaggio indica che il server VNC su un computer remoto ha una password molto debole e Nessus è riuscito ad accedere usando la password 'password'. Questa situazione è pericolosa perché significa che chiunque, da remoto e senza autenticazione, potrebbe sfruttare questa debolezza per prendere il controllo completo del computer.**

**SOLUZIONE: cambiare la password con una piu forte oppure controllare l'accesso,ovvero impostare il server in modo tale che solo alcuni pc possono accedere.**

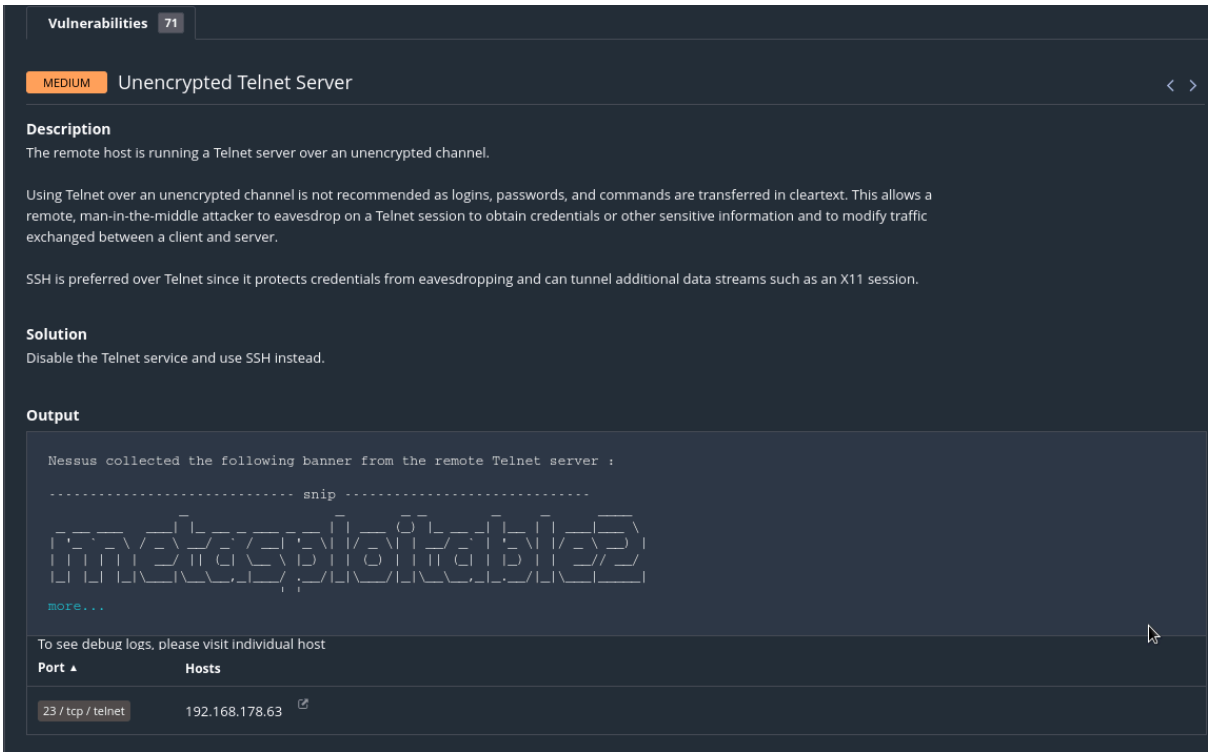
# 2 VULNERABILITA’




**Su una porta (1524)remota del sistema, c'è una shell in ascolto senza richiedere alcuna autenticazione. Questo significa che chiunque, senza dover fornire alcuna credenziale, potrebbe connettersi a questa porta e inviare comandi direttamente al sistema.**

**SOLUZIONE: chiudere la porta in questione oppure impostare un sistema di autenticazione su questa porta in modo da limitarne l'accesso**

# 3 VULNERABILITA’




**Sul computer remoto è attivo un servizio  Telnet su un canale non crittografato(porta 23). L'utilizzo di Telnet su un canale non crittografato non è consigliato perché le informazioni di accesso: password e comandi vengono trasferite in chiaro. Questo significa che un attaccante remoto, posizionato nel mezzo della comunicazione (man-in-the-middle), potrebbe intercettare una sessione Telnet per ottenere credenziali o altre informazioni sensibili e anche modificare il traffico tra il client e il server.**
**SOLUZIONE:utilizzare un servizio SSH poichè protegge le credenziali da intercettazioni**