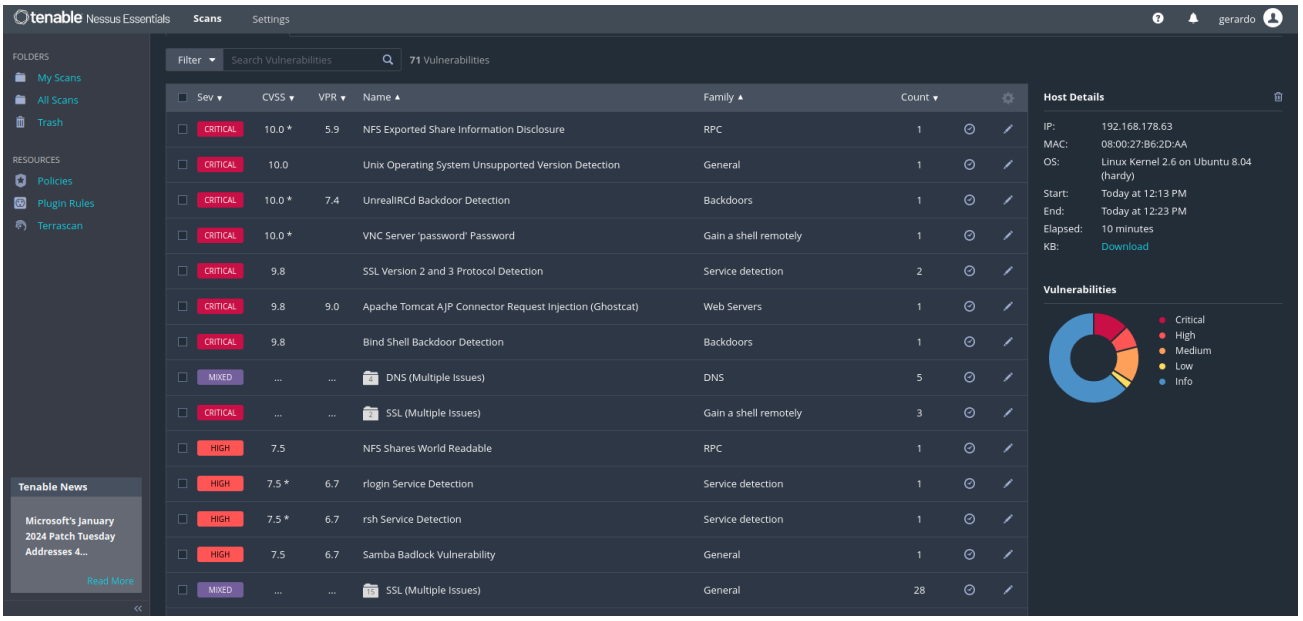
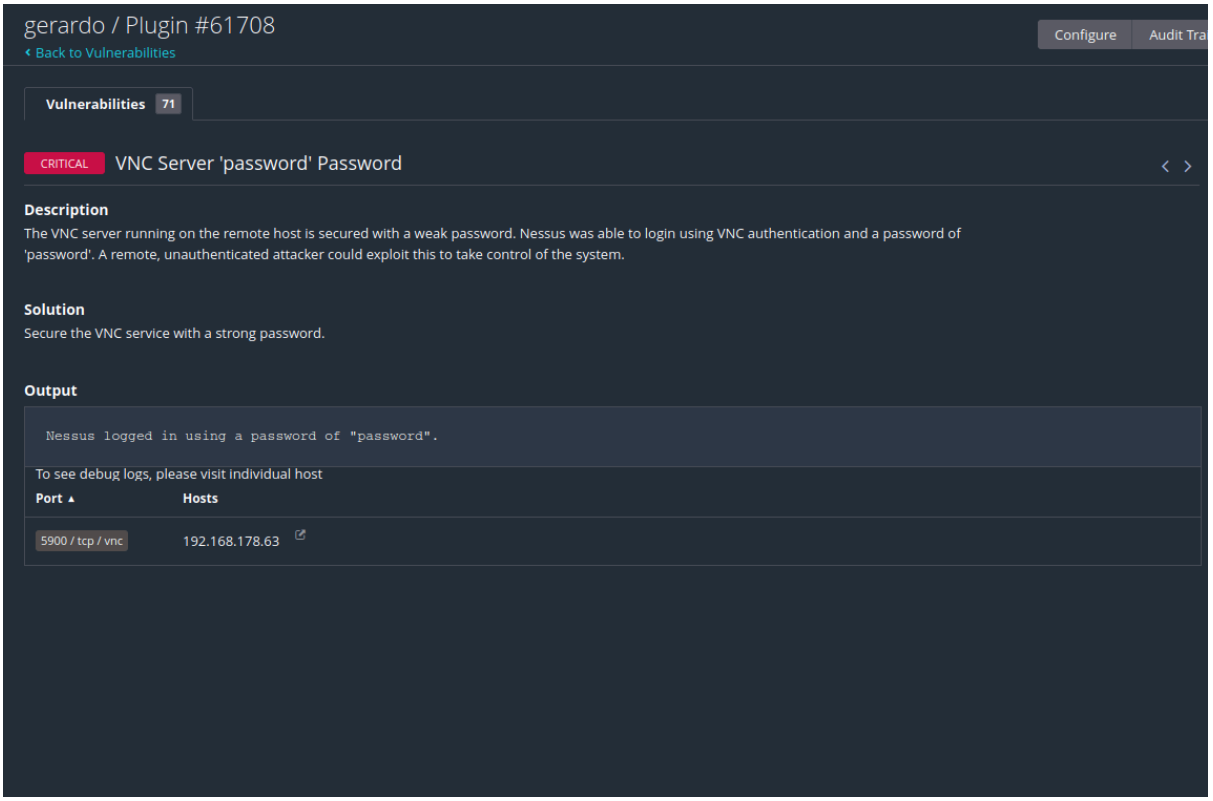
Progetto

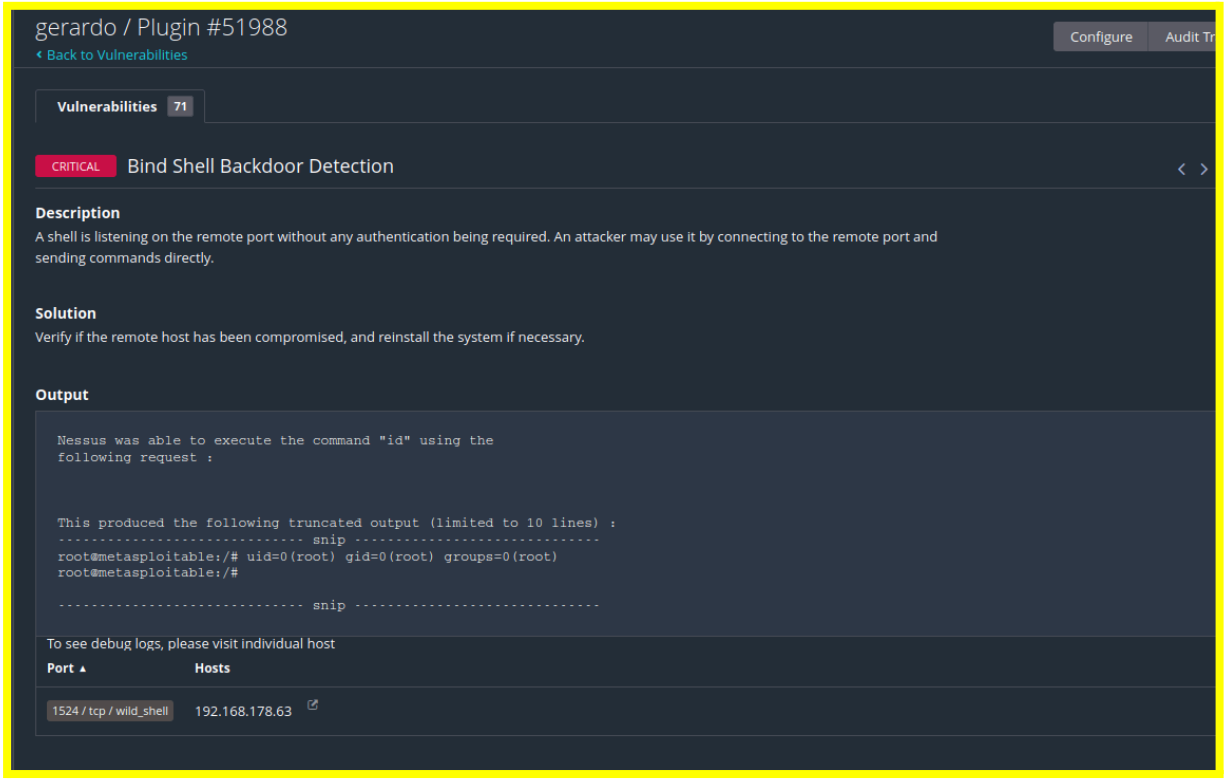
Eseguiamo tramite il tool “Nessus” una scansione sulla macchina macchina metasploitable (192.168.178.63)



come possiamo notare, abbiamo molte vulnerabilita’ critiche. Quindi procediamo per risolverne qualcuna.



(VNC “password’Password) questa è una vulnerabilità,la quale indica che la password impostata sul server VNV è molto debole e può essere scoperta facilmente.
Come seconda vulnerabilità troviamo la seguente:



Questa invece ci indica che sulla porta 1524 si trova una backdoor che può essere sfruttata per connettersi al server ed eseguire comandi da remoto.

SOLUZIONE

Sono andato ad impostare le rules nel firewall della macchina metasploitable (iptables),limitando il traffico sulle porte 1524 e 5900.

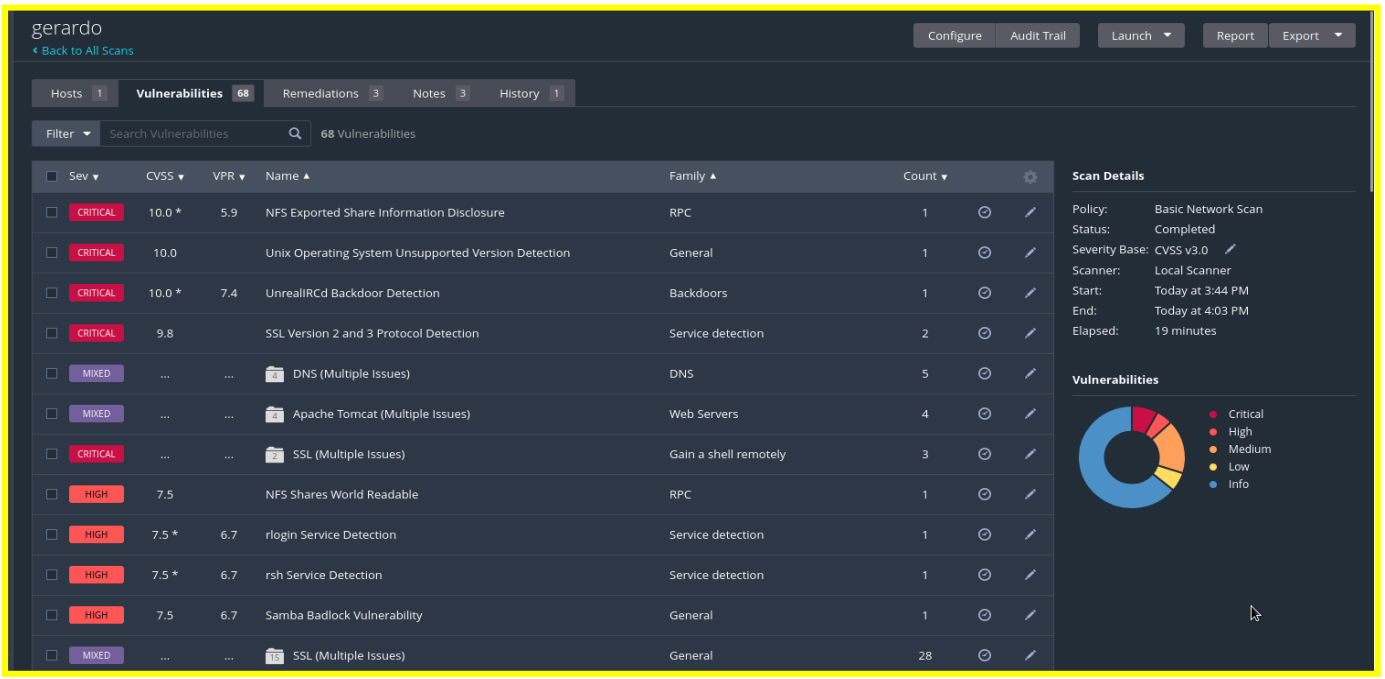
sudo iptables -A INPUT -p tcp --dport 1524 -j DROP
sudo iptables -A INPUT -p tcp --dport 5900 -j DROP
questo comando spiegato brevemente,aggiunge una regola per il protocollo tcp sulla porta 1524 istruendo il firewall a scartare tutti i pacchetti che arrivano su quella porta

```
Try `iptables -h' or 'iptables --help' for more information.
root@metasploitable:/home/msfadmin#  iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere            tcp dpt:5900
DROP       tcp  --  anywhere             anywhere            tcp dpt:ingreslock
DROP       tcp  --  anywhere             anywhere            tcp dpt:ingreslock

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@metasploitable:/home/msfadmin#
```

Scansione finale



come possiamo notare le due vulnerabilità non vengono riscontrate dal programma