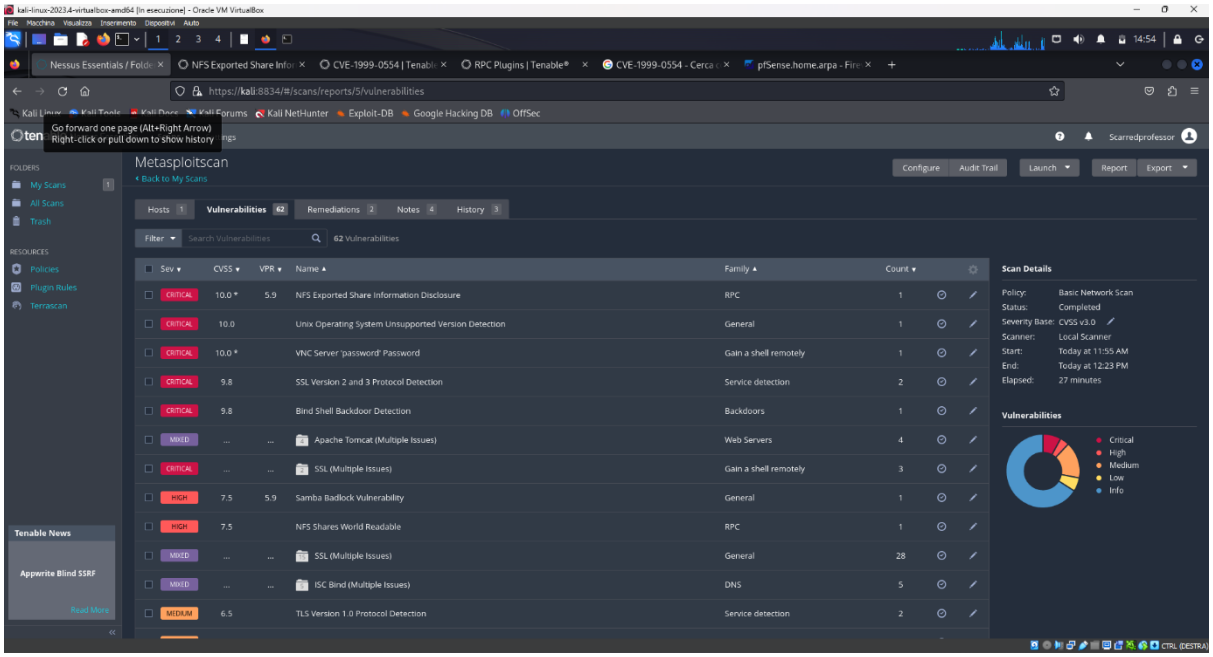
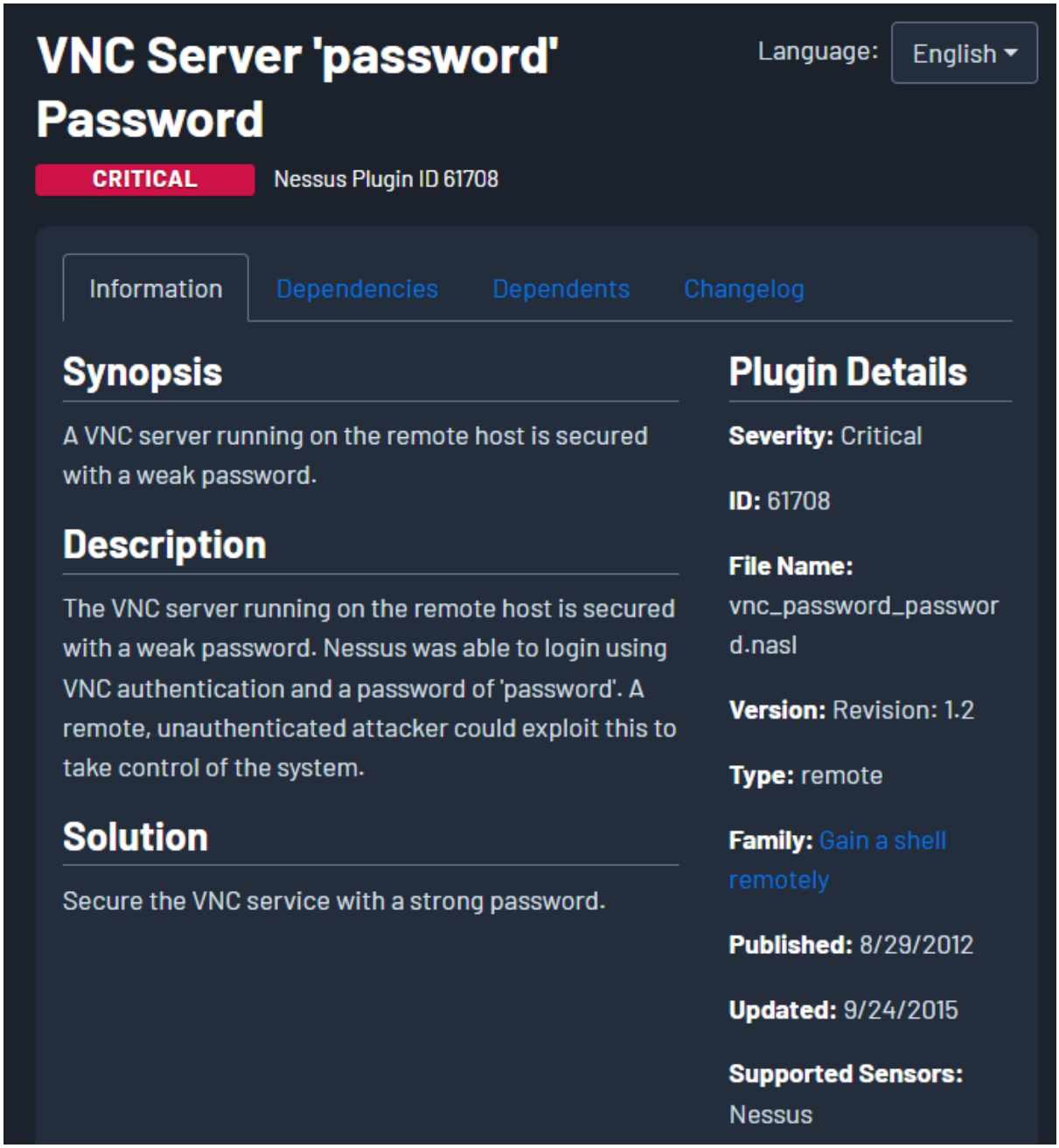
Exploit Critici post scansione con Nessus:



NFS Exported Share Information Disclosure

Per risolvere questa vulnerabilità, l'unica possibilità che non sono andato a testare sarebbe aggiornare il sistema applicando la patch NFS jumbo (Patch-ID# 100173-13), disponibile sul sito Web di Sun Microsystems.

VNC Server 'password' Password

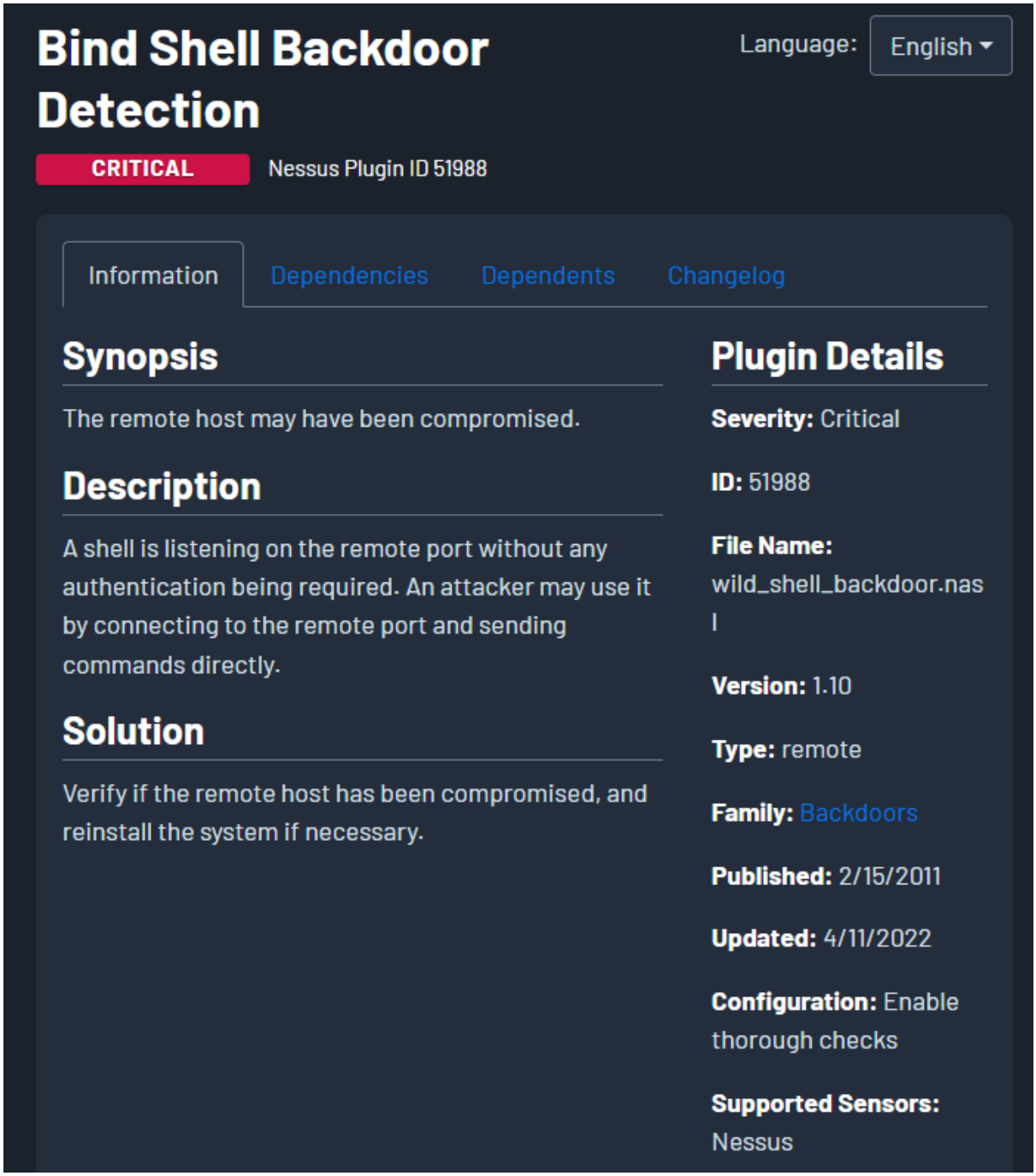


Il problema in questione è CHE la password utilizzata per autenticarsi su un server VNC è “Password”.
Il VNC, acronimo di Virtual Network Computing, è un protocollo che consente di controllare e visualizzare il desktop di un computer da un altro
Per risolvere abbiamo cambiato semplicemente la Password da linea di commando usando

il comando “vncpasswd”.

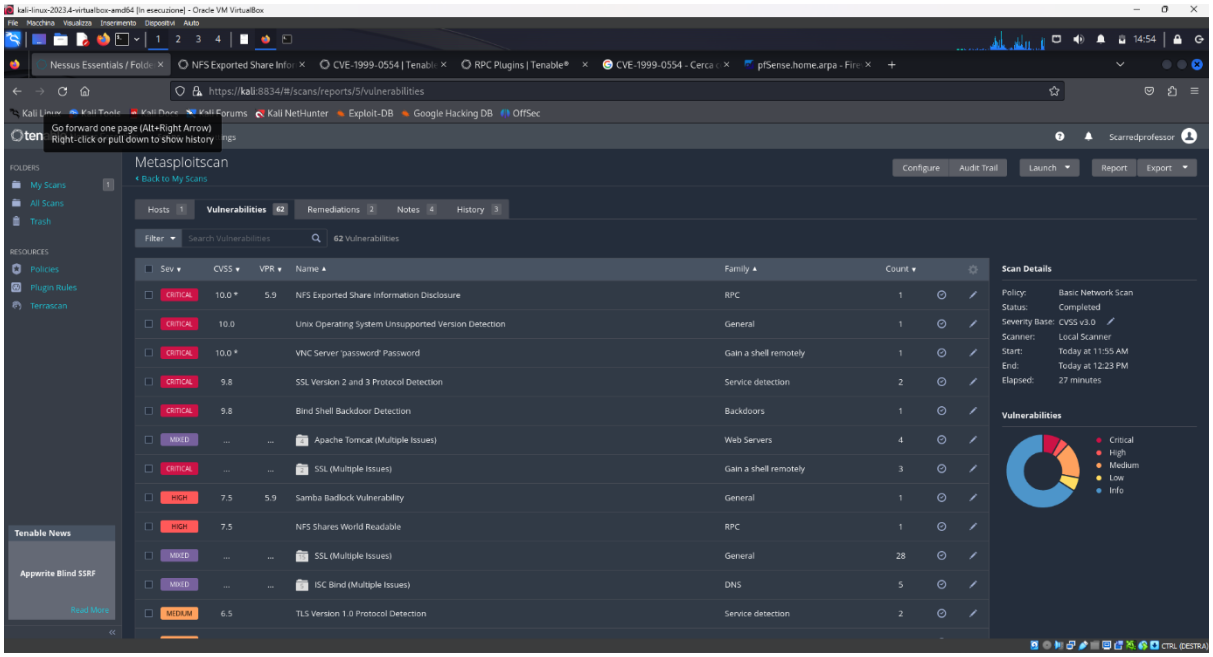
Dopo il Sistema chiederà due volte di inserire la password per conferma e basterà inserire una nuova password e premere invio.

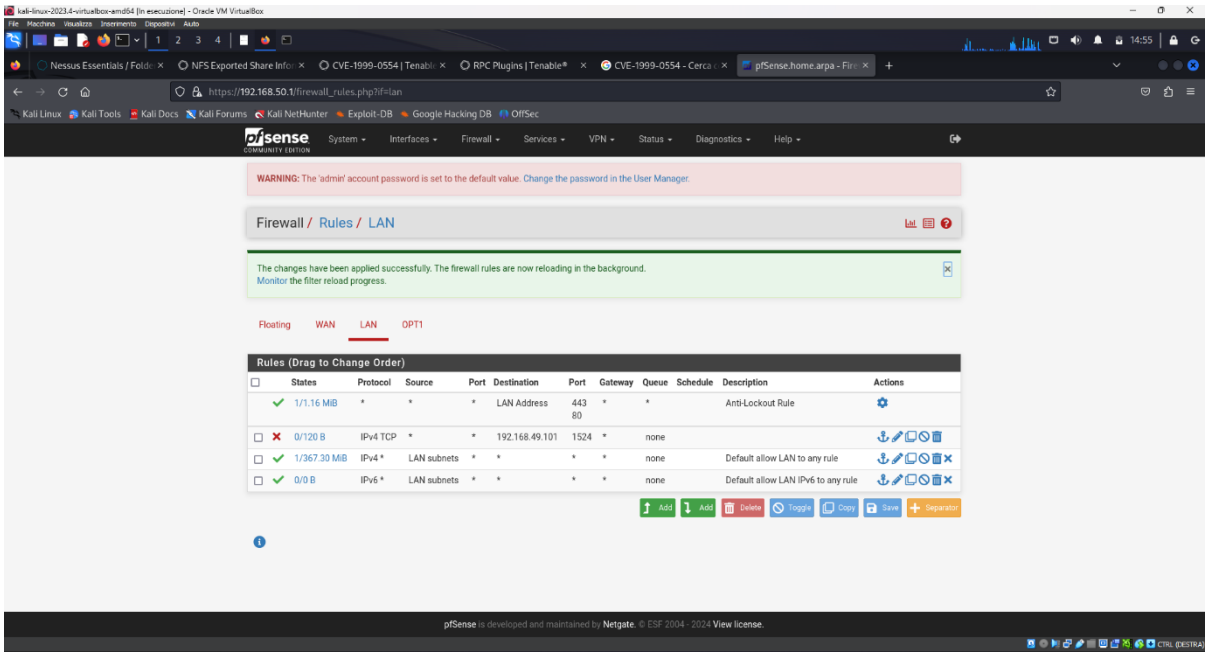
Bind Shell Backdoor Detection

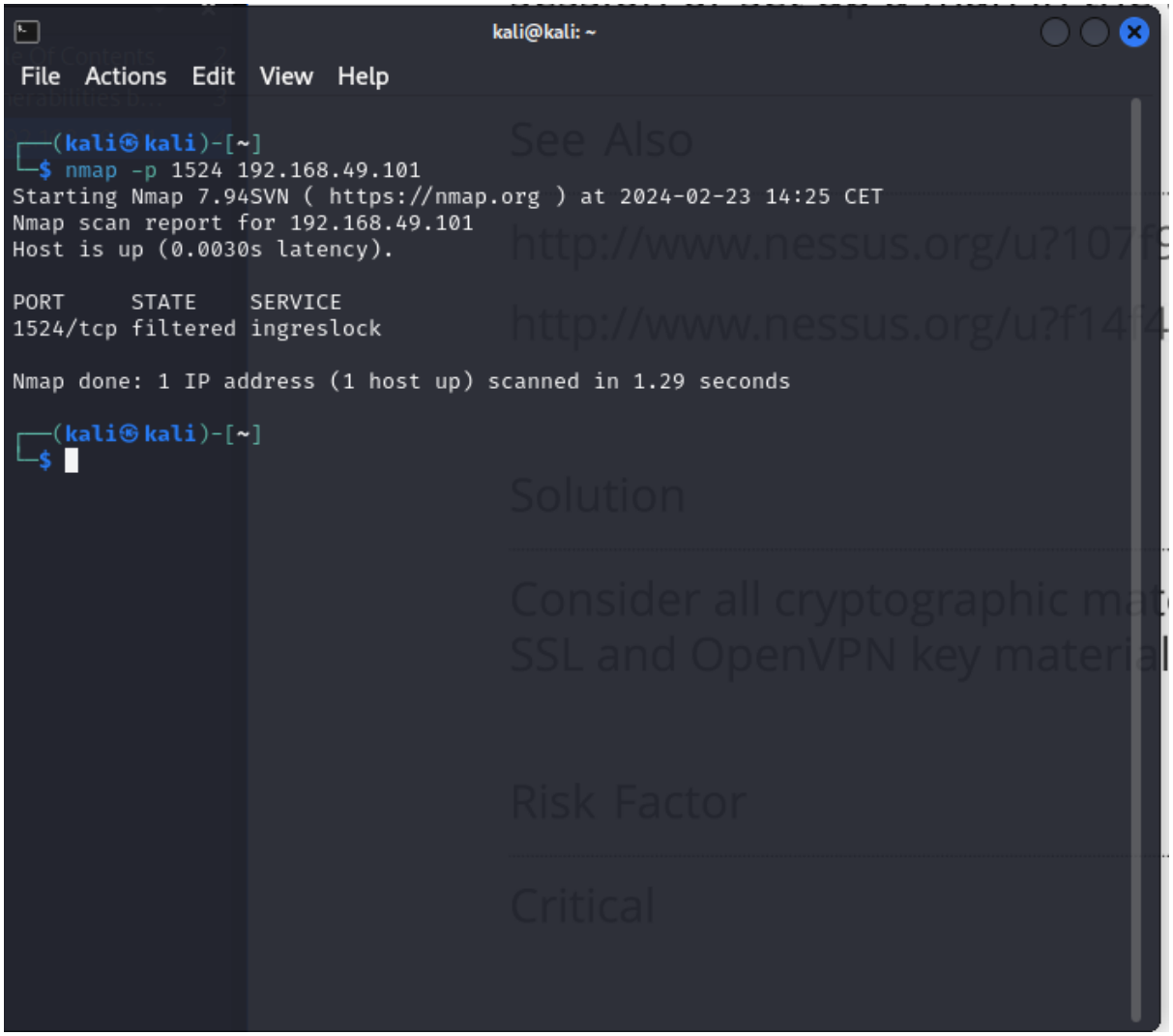


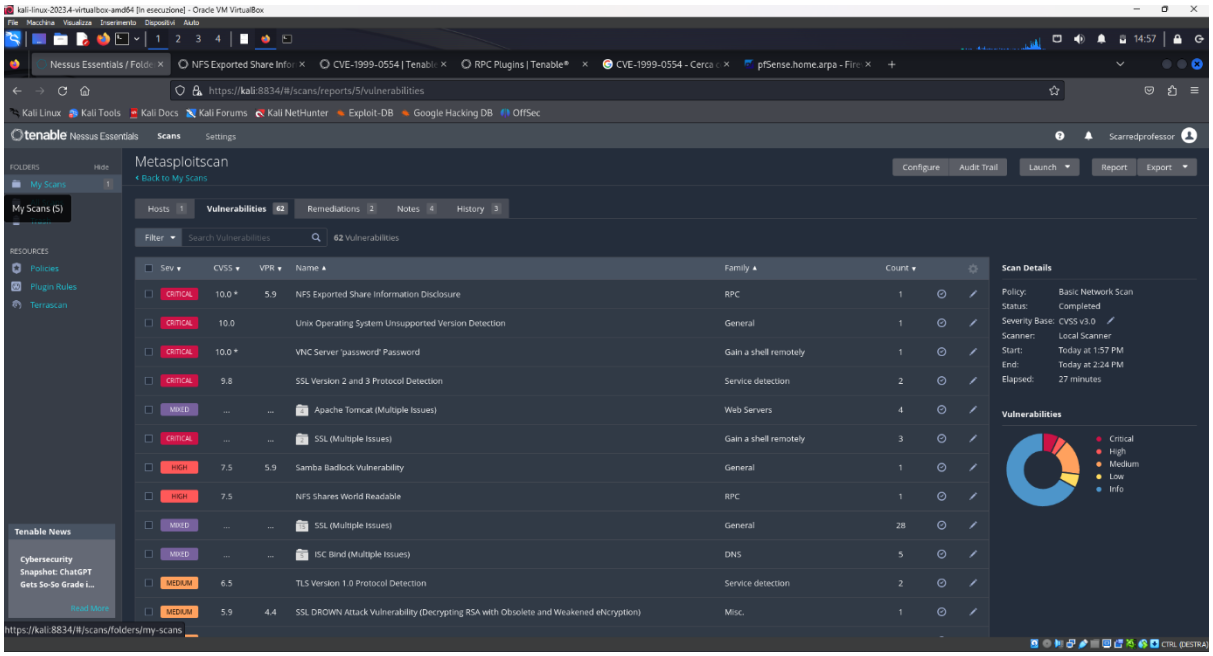
In questo caso ho determinato grazie a Nessus che la porta interessata dalla Backdoor era la 1524, quindi sono andato successivamente ad impostare una regola nel firewall che andasse a bloccare e non a rigettare il tentativo di connessione alla porta. Successivamente per conferma ho lanciato il comando nmap sulla porta 1524 per vedere che la porta

risultasse filtrata. Per vedere se il problema è stato risolto è bastato rifare la scansione su Nessus e confrontare il primo risultato della scansione con il secondo risultato con la regola del firewall applicata.






kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -p 1524 192.168.49.101
Starting Nmap 7.94SVN (https://nmap.org) at 2024-02-23 14:25 CET
Nmap scan report for 192.168.49.101
Host is up (0.0030s latency).
PORT STATE SERVICE
1524/tcp filtered ingreslock
Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds
(kali㉿kali)-[~]
$


Metasploitscan
Hosts 1
Vulnerabilities 62
Remediations 2
Notes 4
History 3
62 Vulnerabilities
Scan Details
Vulnerabilities
Critical
High
Medium
Low
Info