Claudio De cicco
25/11/2022

Remediation

1- 61708 VNC Server 'password' Password

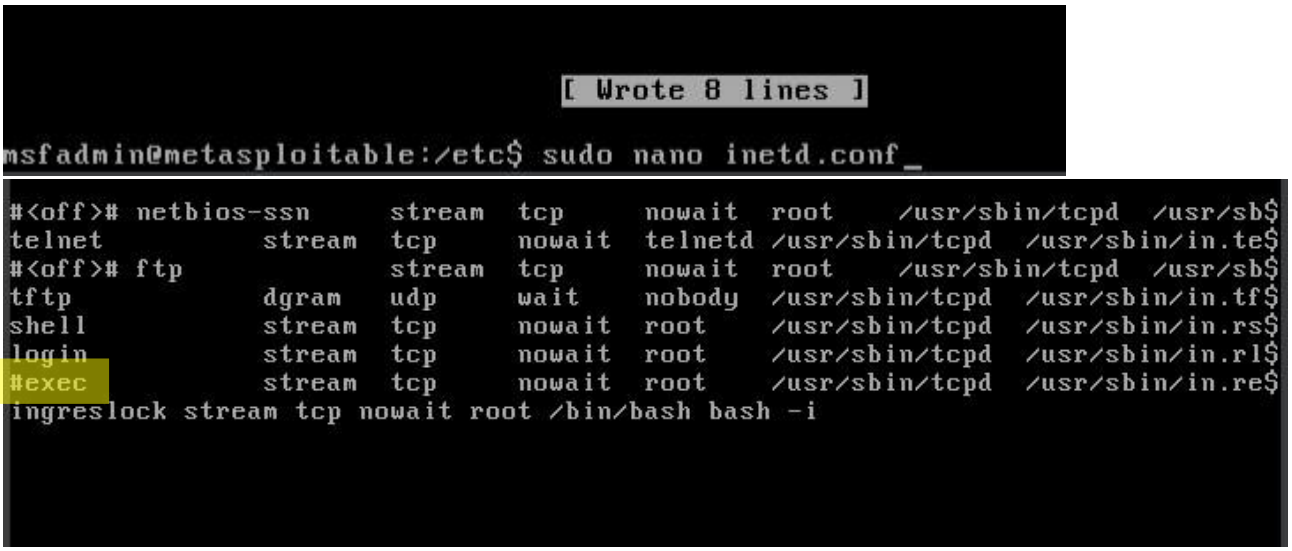
Seguendo la soluzione suggerita da Nessus sono andato a modificare la password del servizio VNC. Per farlo sono andato a lanciare il comando **vcnpasswd.**

```
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
Sorry, try again.
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Passwords do not match. Please try again.

Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
root@metasploitable:/home/msfadmin#
```

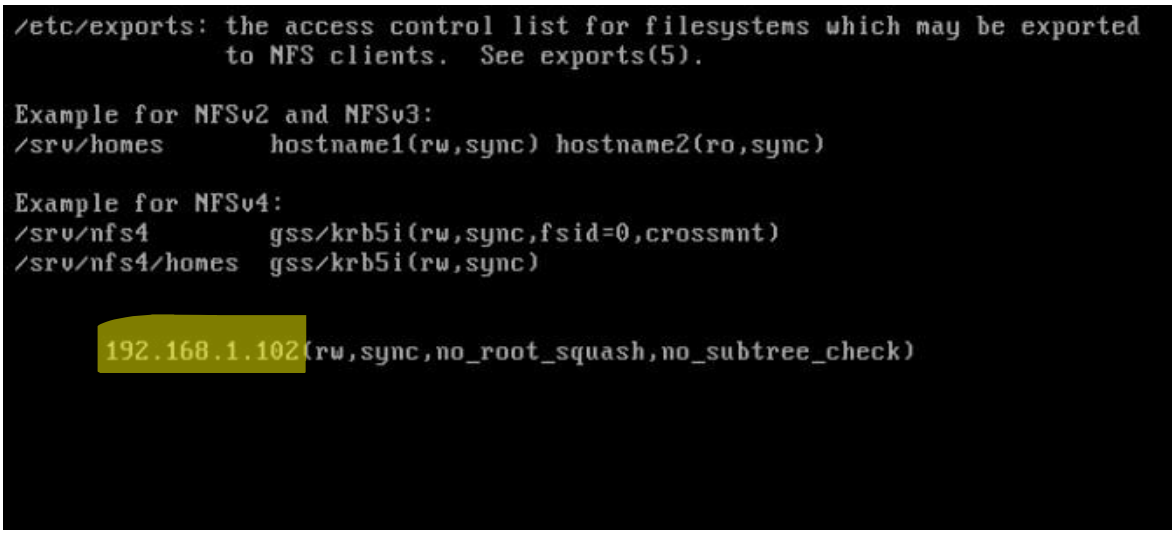
2- 10203 rexecd Service Detection

Il report Nessus ci indica di andare a rendere Commento una linea presente in inetd.conf, nello specifico la linea "exec".



3- 11356 NFS Exported Share Information Disclosure

In questo caso Nessus ci consigliava di configuare l'NFS in modo da consentire l'accesso solo agli autorizzati. Iizialmente ho provato a modificare dei permessi in /etc/hosts.deny e /etc/hosts.allow. Ma continuava a rilevarmi la vulnerabilità, quindi ricercando sono riuscito a risolverla andando a modificare /etc/exports inserendo nell'ultima riga l'indirizzo di meta in modo da concedere solo a se stesso l'accesso.



4- 51988 Bind Shell Backdoor Detection

Qui Nessus diceva di verificare se l'host fosse compromesso e se necessario reinstallare il sistema. In questo caso ho preferito creare una regola nel firewall di meta iptables andando a chiudere la porta per Kali (192.168.1.100) tramite il comando **iptables -I INPUT -p tcp -s 192.168.1.100 –dport 1524 -j DROP.** Avrei potuto chiudere la porta a tutti togliendo "-s 192.168.1.100".