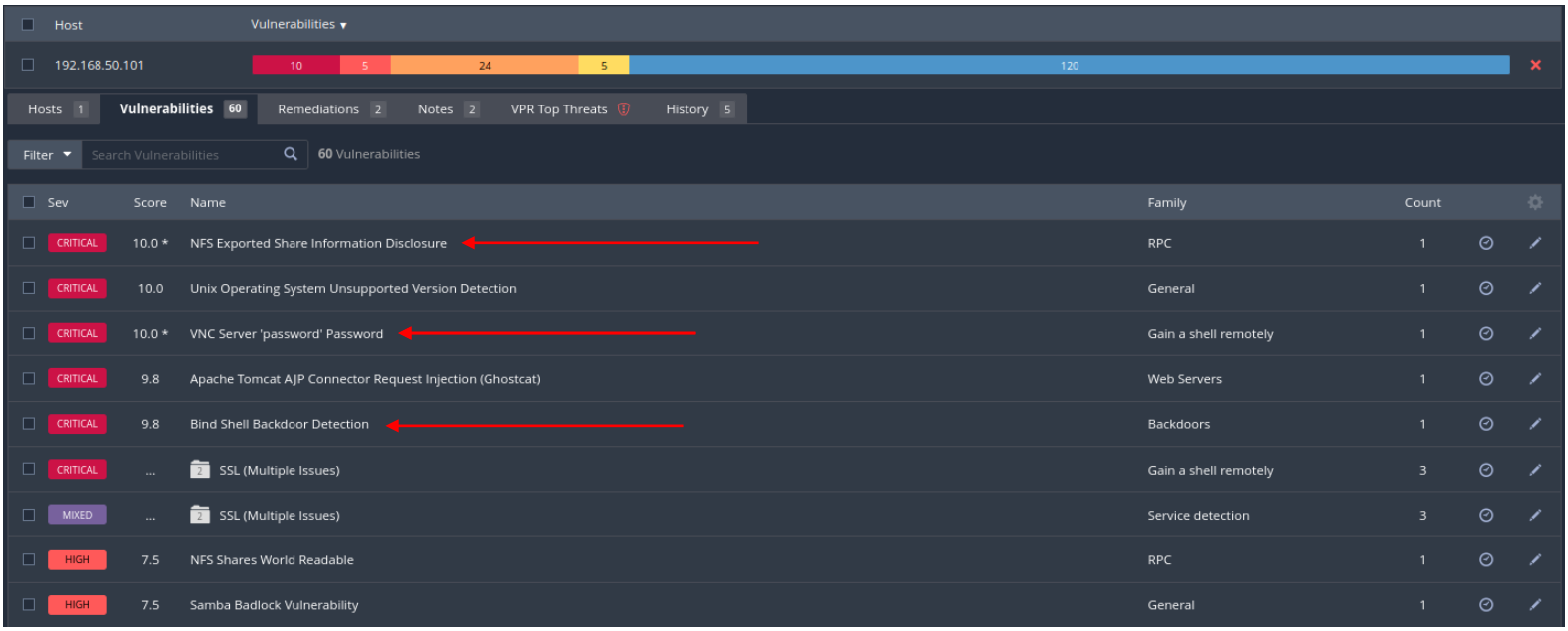
# Report

Objective: Remediation of Critical Vulnerabilities

VM: Kali, Metasploitable

Tools: Nessus, Nmap, Msfconsole, Netcat

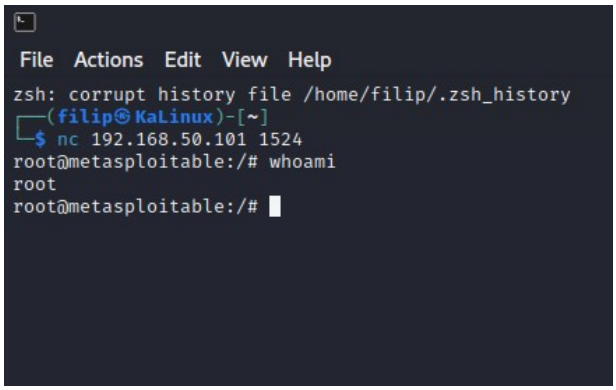


Vulnerability n. 1


Port 1524, has the xinetd super server daemon running on it.

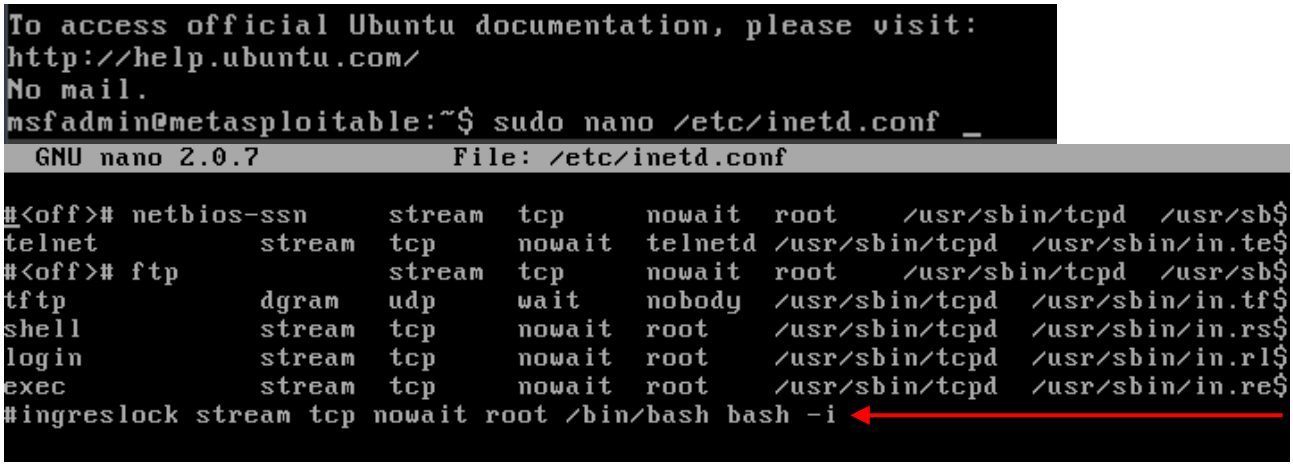

Proof of concept:

To exploit it is as simple as using Netcat command to get root access of the macchine.




Solution:

This is exploitable due to the Ingreslock backdoor on the machine. To fix it we will need to delete the last line inside:

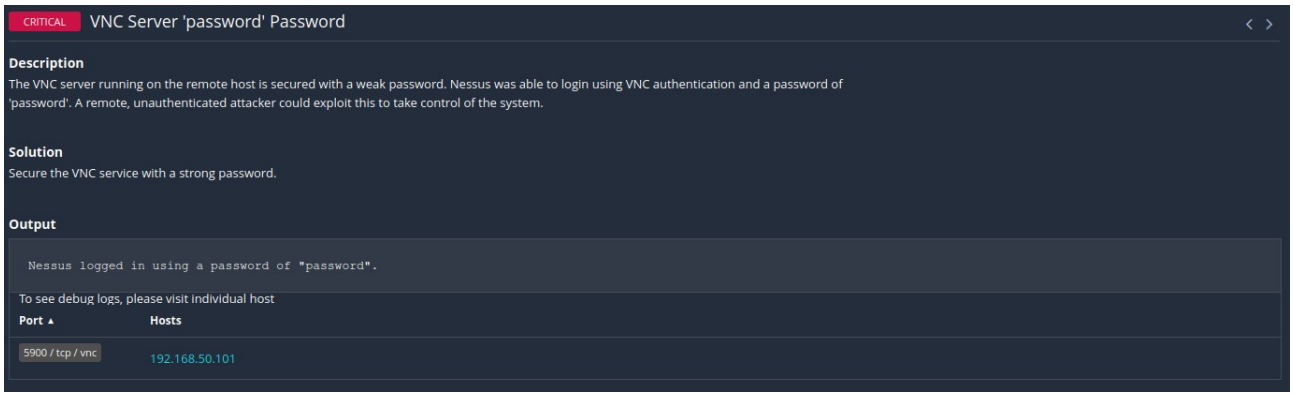



This one

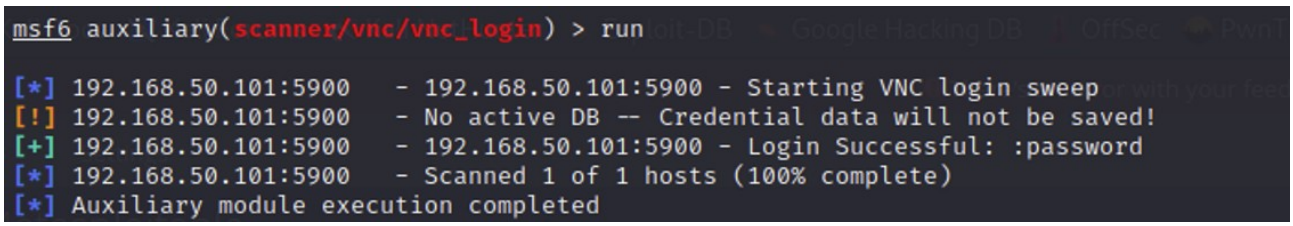
Afterwards if we try to exploit it again from Kali:

Vulnerability n. 2

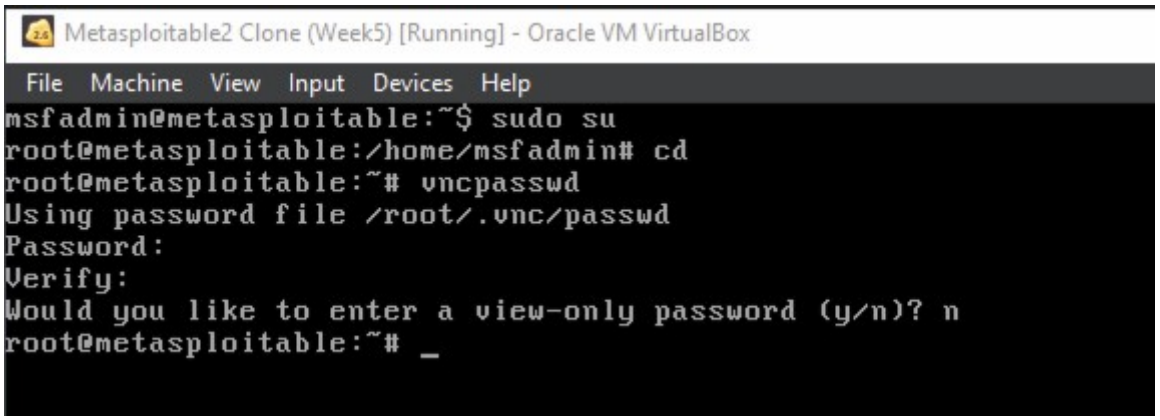

This is a simple misconfiguration, where the default password wasn't changed.



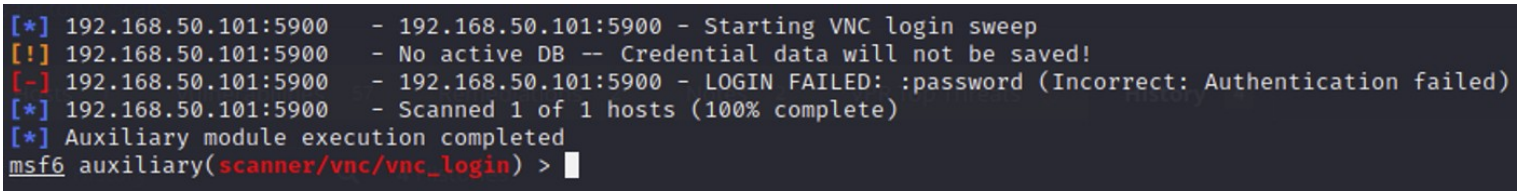

Proof of Concept:
This can be checked with msfconsole using Kali:



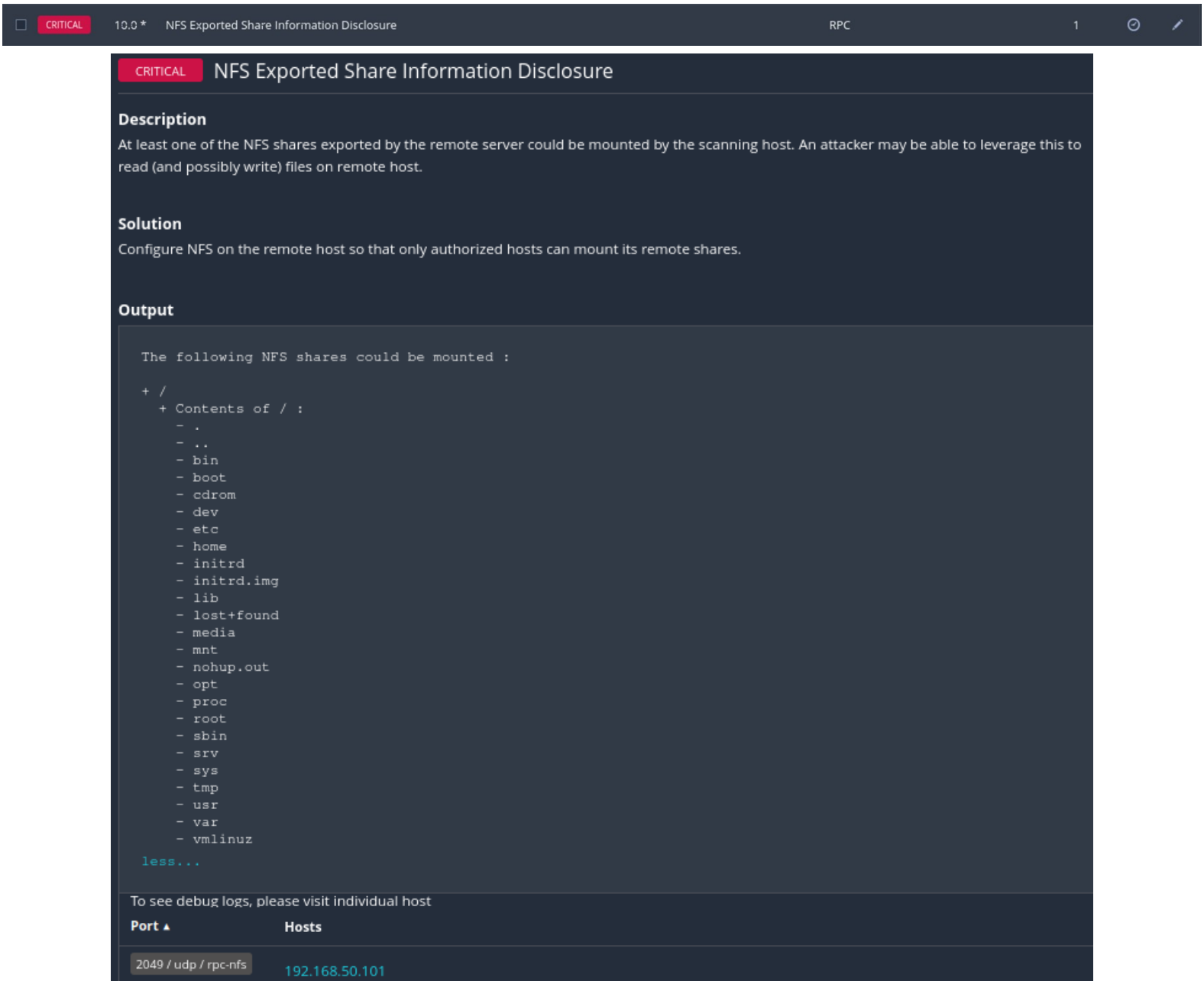

Solution:
Changing the password.




After changing the password we should get failed Authentication on next try of exploiting it.



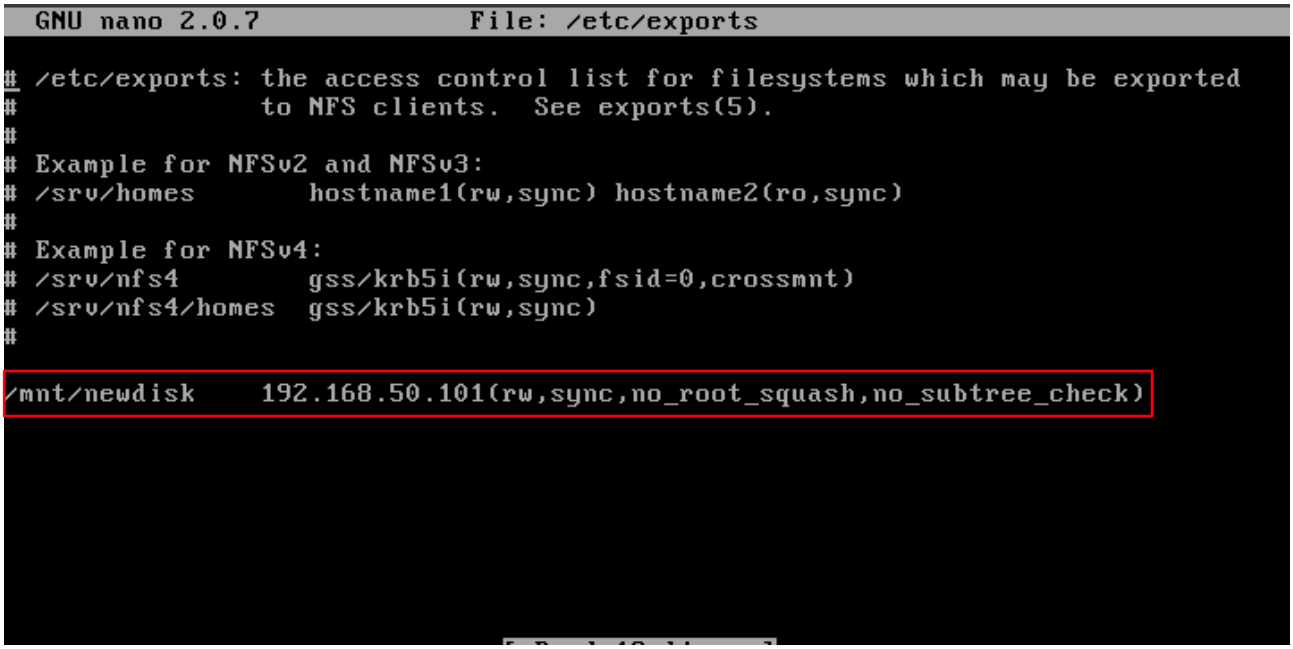
Vulnerability n. 3




POC: missing, in order to exploit and install of nfs-common is needed on Kali

Solution:
There are meny ways to harden the NFS service
one of them is:

Here once again we will modify the last line




After remediation: