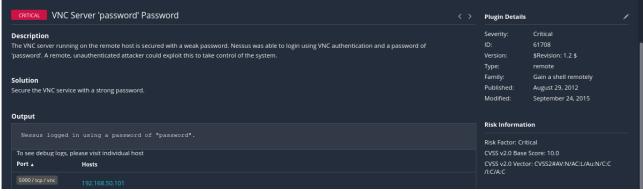
Procediamo con la configurazione della nostra macchina virtuale Metasploitable:IP192.168.50.101 1)Prima vulnerabilità :



Apriamo la macchina vituale e seguiamo i seguenti passaggi:

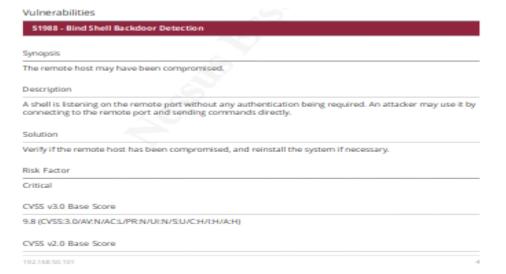
- a)digitiamo :- sudo su→ vncpasswod\_(impostiamo la password)
- b)dopo di che:

c)andiamo sul file exports sempre con sudo su:

Inseriamo al posto dell'asterisco l'IP della nostra macchina (192.168.50.101)

```
GNU nano 2.0.7
                               File: /etc/exports
 /etc/exports: the access control list for filesystems which may be exported
                 to NFS clients. See exports(5).
 Example for NFSv2 and NFSv3:
 /srv/homes
                    hostname1(rw,sync) hostname2(ro,sync)
#
 Example for NFSv4:
 /sru/nfs4
                    gss/krb5i(rw,sync,fsid=0,crossmnt)
 /srv/nfs4/homes gss/krb5i(rw,sync)
        192.168.50.101(rw,sync,no_root_squash,no_subtree_check)
                                 [ Read 12 lines ]
                            R Read File Y Prev Page R Cut Text C Cur Pos Where Is V Next Page U UnCut Text T To Spell
  Get Help
              🔭 WriteOut
  Exit
              ^J Justify
```

51988 shell



## Backdoor detection.

Eseguiamo questo comando con il quale specifichiamo che dall'IP di Kali qualsiasi tep venga Droppato sulla porta interessata.(1524)

```
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
root@metasploitable:/home/msfadmin# sudo iptables -I INPUT -p tcp -s 192.168.50.
100 --dport 1524 -j DROP_

Output DESTRA)
```

3)<u>11356 -</u> Exported NFS Share

Bind

11356-N	IFS Exported Share Information Disclosure
Synopsis	
it is possibl	e to access NFS shares on the remote host.
Description	
	e of the NFS shares exported by the remote server could be mounted by the scanning host. An sy be able to leverage this to read (and possibly write) files on remote host.
Solution	
Configure I	IFS on the remote host so that only authorized hosts can mount its remote shares.
Risk Factor	
Critical	
CVSS v2.0 i	Base Score
10.0 (CVSS)	MAY-N/AC-L/Au-N/C-C/I-C/A-C)
References	
CVE	CVE-1999-0170
CVE	CVE-1999-0211
CVE	CVE-1999-0554
Exploitable	With
Metasploit	(true)
Plugin Info	rmation
Published:	2003/03/12, Modified: 2018/09/17
Plugin Out	put
udp/2049/r	po-nfs

**Information Disclosure** 

Lo abbiamo 1	risolto nel punto 1	l inserendo l'ip	di Meta.	