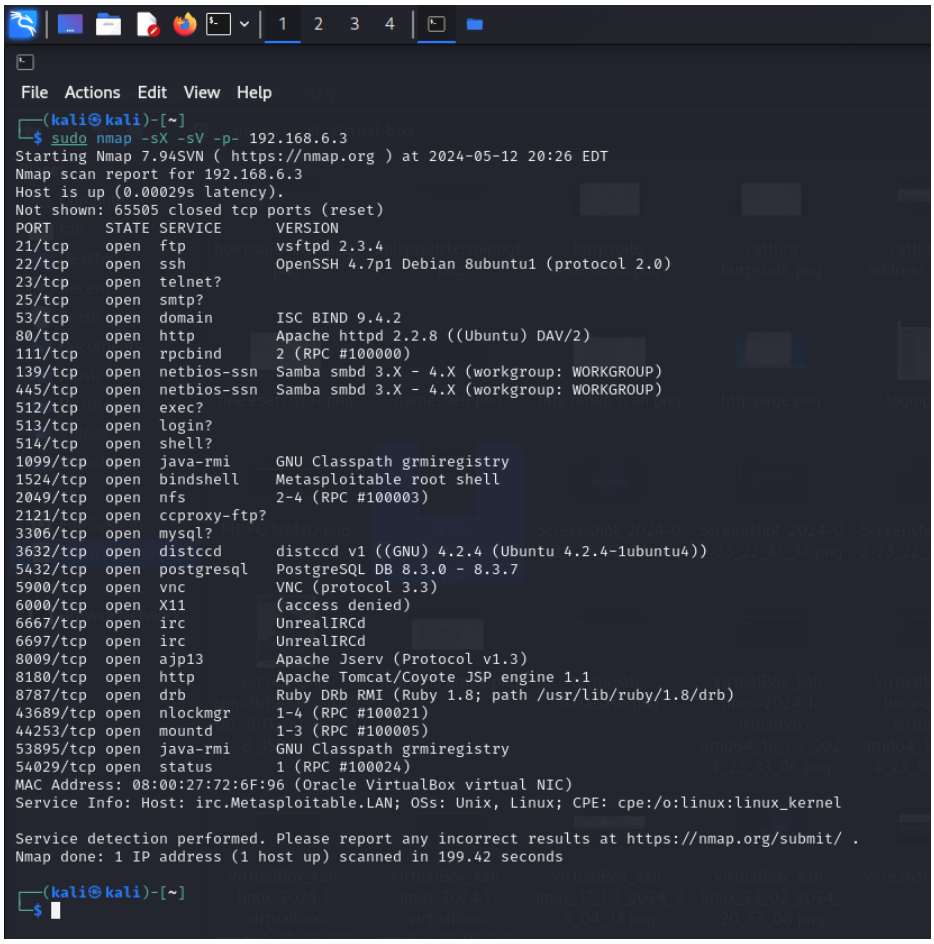
PROGETTO MODULO 3

○ Remediation Metaspoitable

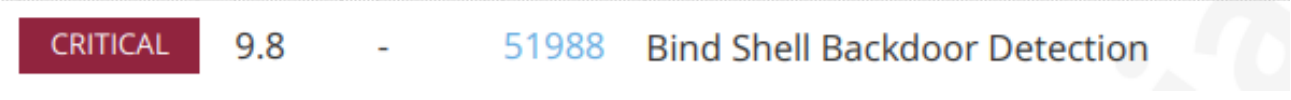
Prima di iniziare a risolvere le vulnerabilità riscontrate nella scansione effettuata con nessuss, effettuiamo una scansione manuale da terminale utilizzando Nmap.

- nmap -sX -sV 192.168.6.3

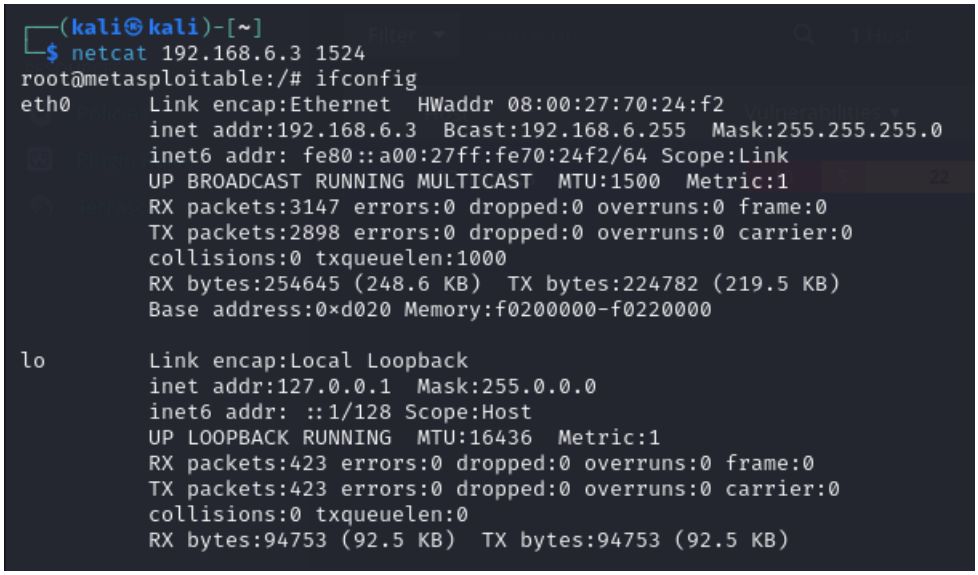
1. in questo tipo di scansione utilizziamo **-sX** per inviare pacchetti TCP con i flag FIN, PSH e URG , ma senza il flag SYN. Viene utilizzata per analizzare la topologia di rete e individuare eventuali host vulnerabili, inoltre non tenta di stabilire una connessione TCP completa.
2. Lo switch **-sV** invece tenta di determinare le versioni dei servizi in esecuzione su porte aperte.



1. La prima vulnerabilità che andiamo a risolvere riguarda BIND SHELL BACKDOOR DETECTION

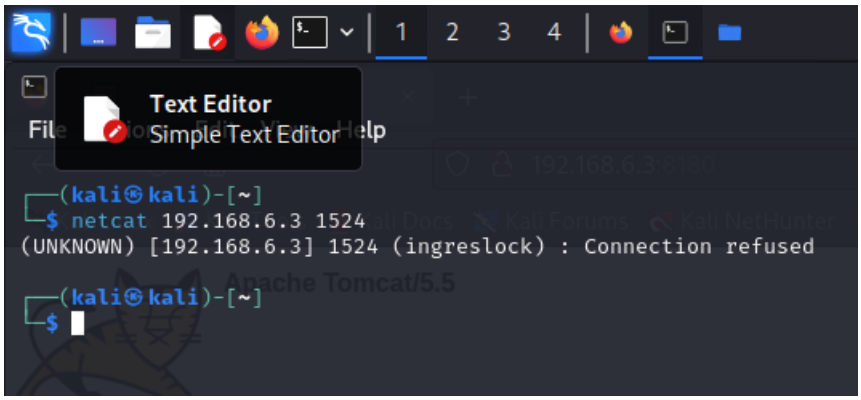


Questa vulnerabilità ci permette di poterci collegare alla porta 1524 con il comando nc 192.168.6.3 1524 della macchina metaspoitable facendoci ottenere l'accesso ad una connessione root senza che ci venga richiesta l'autenticazione.



Per risolvere questa vulnerabilità andiamo a modificare in metaspoitable il file /etc/inetd.conf utilizzando l'editor di testo nano commentando la riga che sta per ultima : **#ingreslock stream tcp nowait root /bin/bash bash -i**

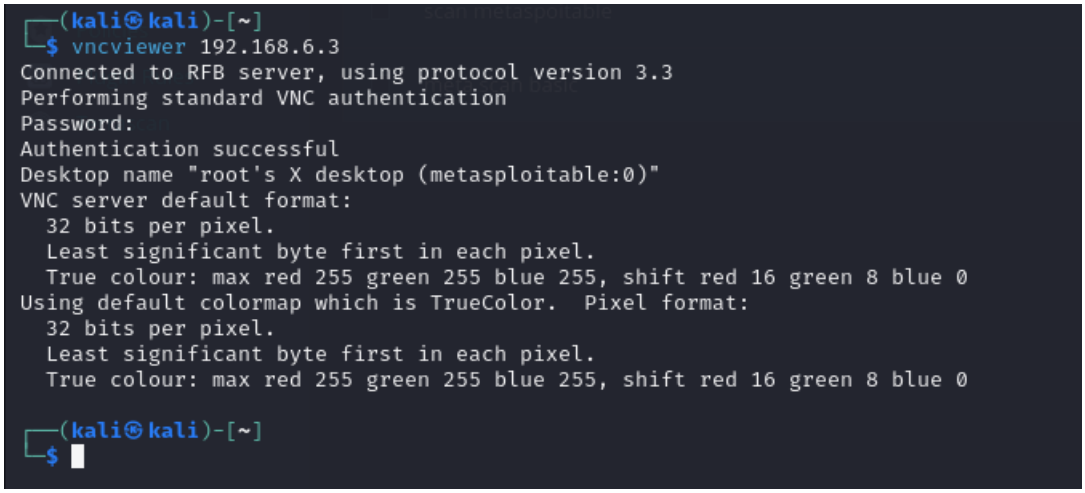
Se proviamo a collegarci alla porta 1524 dopo aver effettuato la modifica, notiamo che la connessione è chiusa.



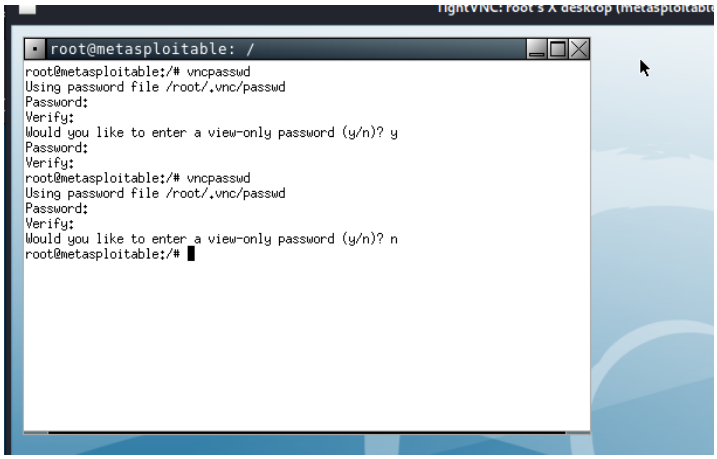
2. La seconda vulnerabilità che andremo a risolvere riguarda VNC SERVER

CRITICAL	10.0*	-	61708	VNC Server 'password' Password

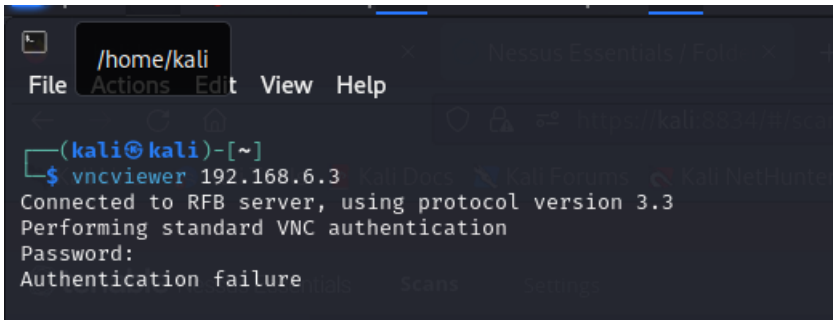
Questa vulnerabilità consente ad un attaccante di poter accedere al server VNC semplicemente utilizzando il comando vncviewer 192.168.6.3 e utilizzando come credenziali “password – password”



Per risolvere questa vulnerabilità impostiamo una nuova password più sicura direttamente dall’editor grafico di vnc su metaspoitable utilizzando i privileggi root .



Se proviamo a connetterci nuovamente con lo stesso comando e con le credenziali password – password ci accorgiamo che l'autenticazione fallisce perché abbiamo impostato una password più sicura.



3. terza vulnerabilità che andremo a risolvere riguarda NFS EXPORTED SHARE INFORMATION DISCLOURE

Nfs è un protocollo di rete che consente ad un pc client di utilizzare la rete per accedere a directory condivise tramite un punto di montaggio da server remoti come se fossero disponibili in locale. In questo caso abbiamo un accesso libero ad un punto di montaggio , che permette all'attaccante di leggere e scrivere sulla nostra macchina.

- Per risolvere questo problema utilizzeremo il comando **rpcinfo 192.168.6.3** per capire su quali porte è in ascolto nfs

```
┌──(kali㉿kali)-[~]
└─$ rpcinfo 192.168.6.3
   program version netid     address                service    owner
    100000    2    tcp       0.0.0.0.0.111          portmapper unknown
    100000    2    udp       0.0.0.0.0.111          portmapper unknown
    100024    1    udp       0.0.0.0.142.175        status     unknown
    100024    1    tcp       0.0.0.0.158.73         status     unknown
    100003    2    udp       0.0.0.0.8.1            nfs        unknown
    100003    3    udp       0.0.0.0.8.1            nfs        unknown
    100003    4    udp       0.0.0.0.8.1            nfs        unknown
    100021    1    udp       0.0.0.0.144.199        nlockmgr   unknown
    100021    3    udp       0.0.0.0.144.199        nlockmgr   unknown
    100021    4    udp       0.0.0.0.144.199        nlockmgr   unknown
    100003    2    tcp       0.0.0.0.8.1            nfs        unknown
    100003    3    tcp       0.0.0.0.8.1            nfs        unknown
    100003    4    tcp       0.0.0.0.8.1            nfs        unknown
    100021    1    tcp       0.0.0.0.130.195        nlockmgr   unknown
    100021    3    tcp       0.0.0.0.130.195        nlockmgr   unknown
    100021    4    tcp       0.0.0.0.130.195        nlockmgr   unknown
    100005    1    udp       0.0.0.0.134.162        mountd     unknown
    100005    1    tcp       0.0.0.0.229.236        mountd     unknown
    100005    2    udp       0.0.0.0.134.162        mountd     unknown
    100005    2    tcp       0.0.0.0.229.236        mountd     unknown
    100005    3    udp       0.0.0.0.134.162        mountd     unknown
    100005    3    tcp       0.0.0.0.229.236        mountd     unknown

┌──(kali㉿kali)-[~]
```

Utilizzando il comando **showmount -e 192.168.6.3** otteniamo informazioni sul server nfs.

```
┌──(kali㉿kali)-[~]
└─$ showmount -e 192.168.6.3
Export list for 192.168.6.3:
/ *

┌──(kali㉿kali)-[~]
└─$
```

In questo caso le informazioni che ci viene fornita è che un eventuale attaccante potrebbe tranquillamente montare sulla propria macchina “ / “ che sta ad indicare il file system con proprietà root per la maggior parte dalle macchine linux.

Per risolvere questa vulnerabilità andiamo a modificare il file **/etc/exports ,** commentiamo l’ultima riga del file e abilitiamo l’esempio che ci mostra il file aggiungendo l’ip di metaspoitable.

```
 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       192.168.6.3(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes  gss/krb5i(rw,sync)
#

#/      *(rw,sync,no_root_squash,no_subtree_check)

                        [ Read 12 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

4. La quarta vulnerabilità che risolveremo è **APACHE TOMCAT AJP**

CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)

Per risolvere questa vulnerabilità andiamo direttamente nel terminle della macchina metaspoitable e configuriamo il file /etc/tomcat5.5/server.xml utilizzando l'editor nano con privileggi root.

Con questo metodo andiamo ad abilitare il connettore AJP in modo che venga avviatocon fattore di sicurezza.

Dentro il file /etc/tomcat5.5/server.xml andiamo ad aggiungere la stringa **secretRequired="true",** accanto alle altre sulla porta 8009, successivamente aggiungiamo un'altra stringa **secret="<string>"**