REMEDIATION OF VULNERABILITIES

Elenco vulnerabilità risolte

Elenco passaggi effettuati per risolvere le vulnerabilità

1) NFS Exported Share Information Disclosure

Nell'immagine sottostante possiamo vedere, all'ultima riga del file, la configurazione errata del servizio NFS nel quale viene data la possibilità a qualsiasi indirizzo IP (rappresentato dall'asterisco) di accedere ai dati dalla cartella root (indicata dalla barra).

```
  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:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes  gss/krb5i(rw,sync)
#

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

Al fine di risolvere tale vulnerabilità è stato deciso di restringere l'accesso alla sola directory *media*, quindi non più quella *root,* ai soli host presenti sulla stessa rete della macchina scansionata ipotizzando il caso nel quale tale macchina operi come scambio di media tra i vari client della rete. È stata anche eliminata l'opzione *no_root_squash* in quanto è un'opzione estremamente pericolosa che consente agli utenti root remoti lo stesso privilegio dell'utente root della macchina host.

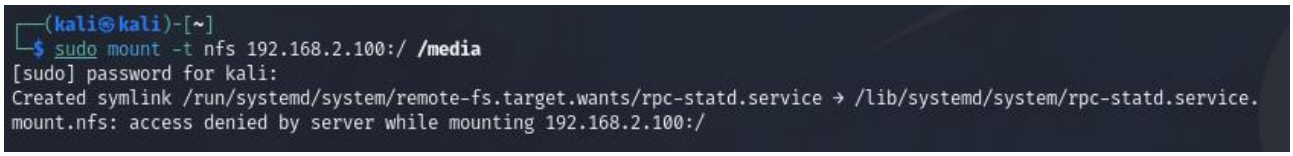
```
  GNU nano 2.0.7            File: /etc/exports

# /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:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes  gss/krb5i(rw,sync)
#

/media  192.168.2.0/24(rw,sync,no_subtree_check)
```

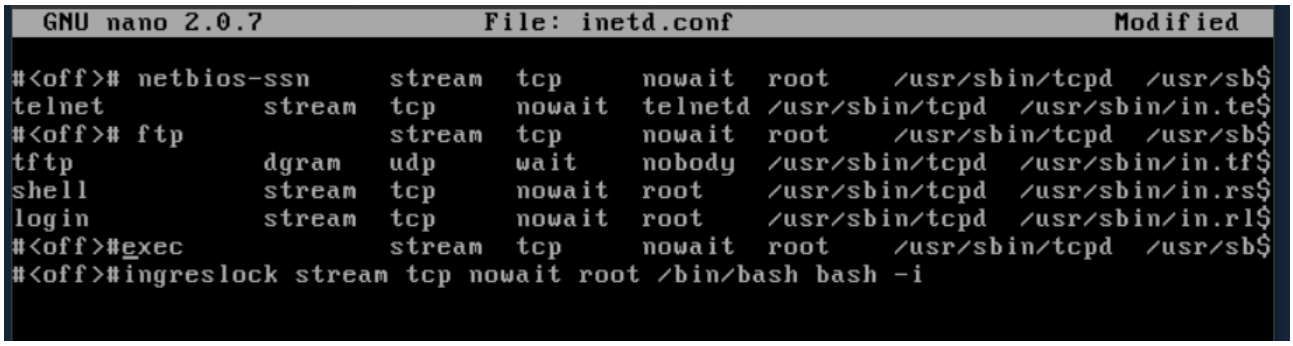
Con il comando *sudo exportfs -arv* sono state applicate le modifiche apportate al file di configurazione.

Infine, come si può notare dall'immagine seguente, le modifiche apportate impediscono il *mount* della cartella *media* in quanto la macchina kali si trova su un'altra rete.

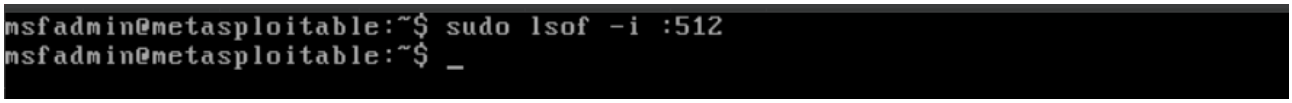


2) rexecd Service Detection

Questa vulnerabilità è stata risolta disabilitando dai file di configurazione del demone *inetd,* il servizio *exec* ovvero il servizio che è causa la vulnerabilità.

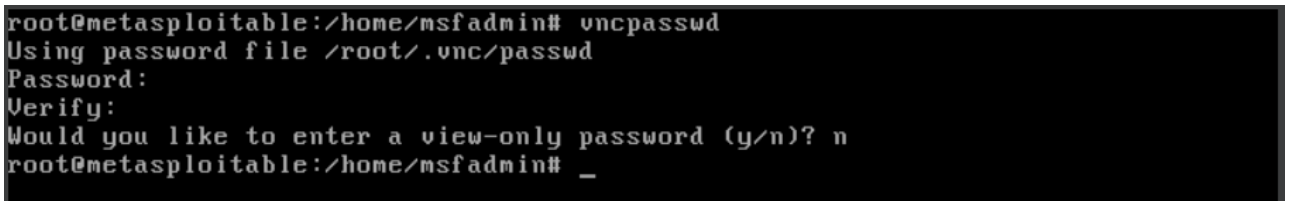


Come controprova è stata verificata la presenza del servizio *exec* sulla porta 512 in quanto quest'ultima è quella utilizzata da tale servizio.



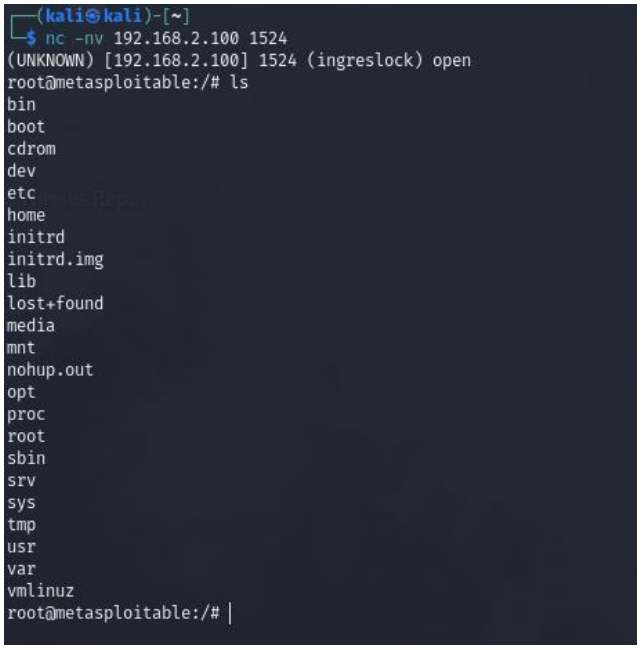
3) VNC Server 'password' Password

La terza vulnerabilità è stata risolta cambiando la password di accesso precedente ovvero "password" con una più complessa tramite il comando *vncpasswd* da utente root.

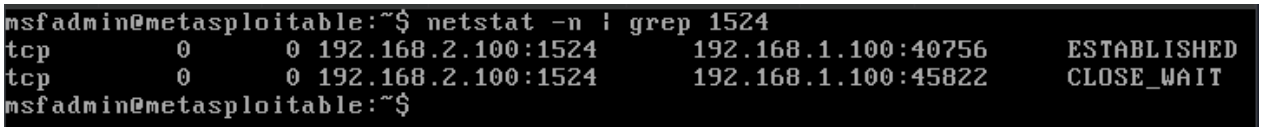


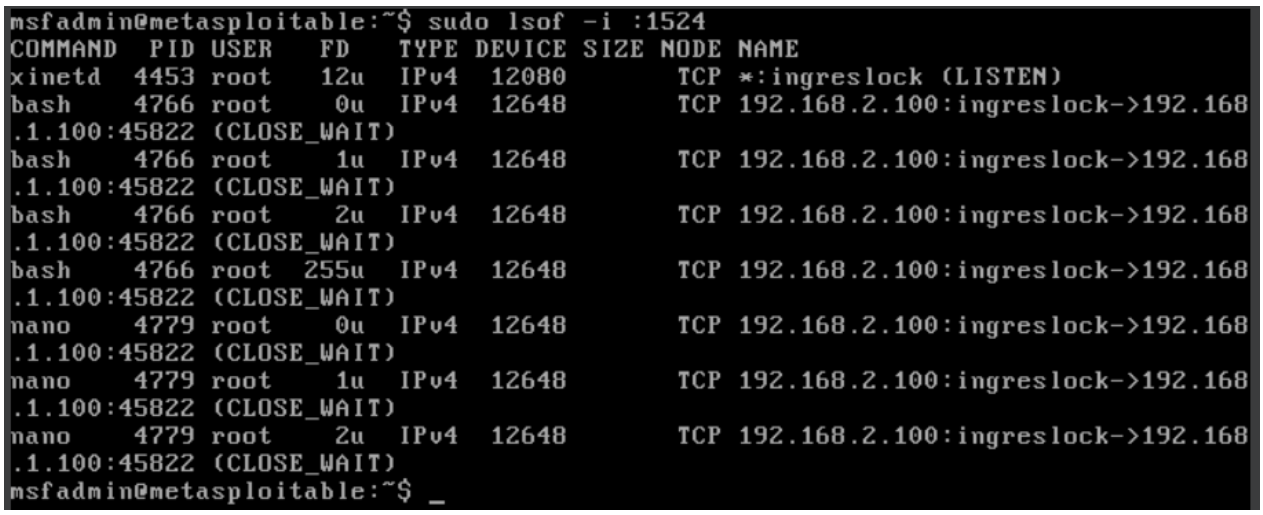
4) Bind Shell Backdoor Detection

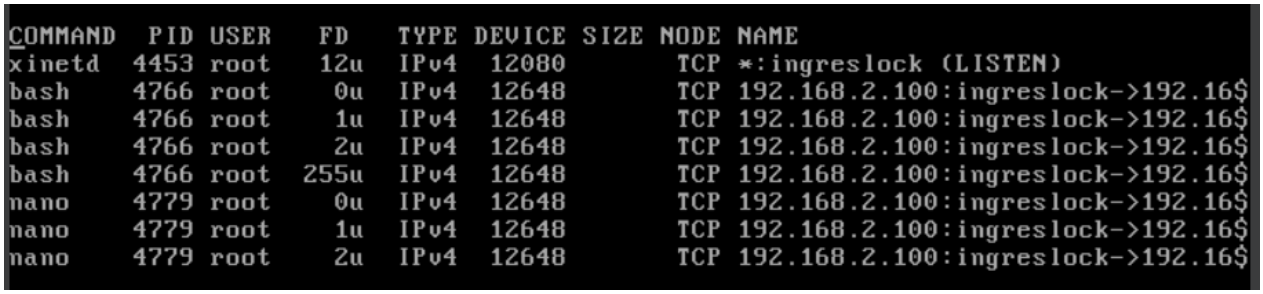
L'ultima vulnerabilità risolta permetteva l'utilizzo della shell della macchina target tramite una macchina remota come si può evincere dall'immagine successiva.



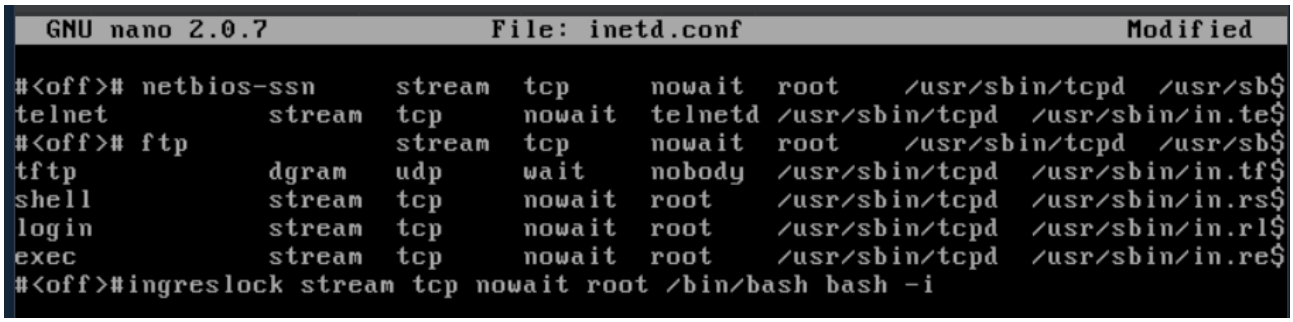
Per correggere tale vulnerabilità è stato necessario disabilitare il servizio *ingreslock* operante sulla porta 1524 tramite la quale avviene la connessione tra macchine.

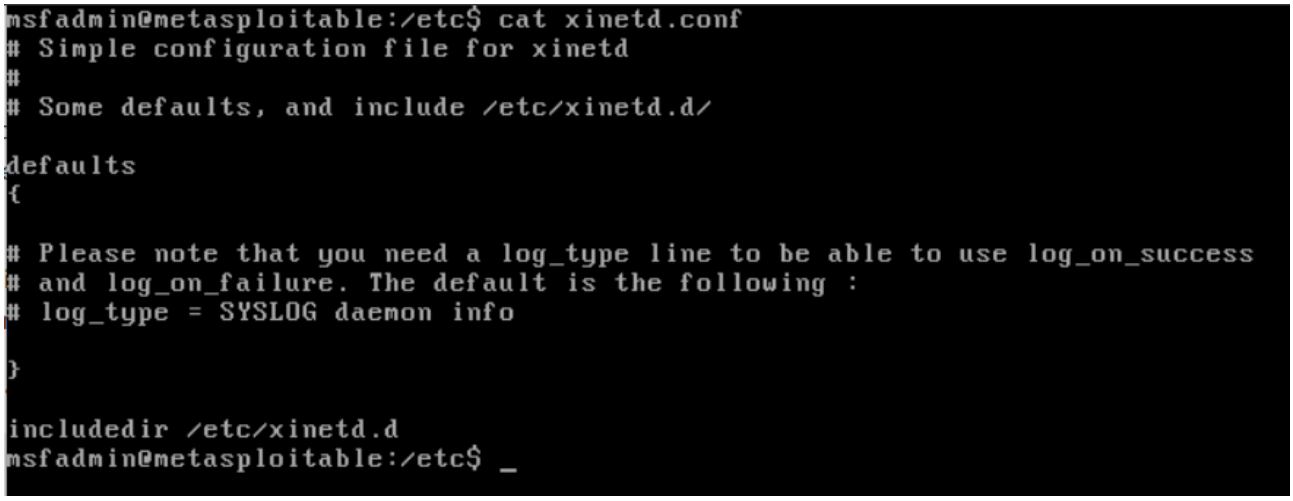






Per disabilitare il servizio *ingreslock* sono stati modificati i file di configurazione dei demoni *inetd* e *xinetd.*





Come controprova è stata verificata la presenza del servizio sulla porta 1524 in quanto quest'ultima è quella utilizzata da tale servizio.

Infine, come si può notare dall'immagine seguente, le modifiche apportate impediscono l'accesso alla shell sulla macchina target.