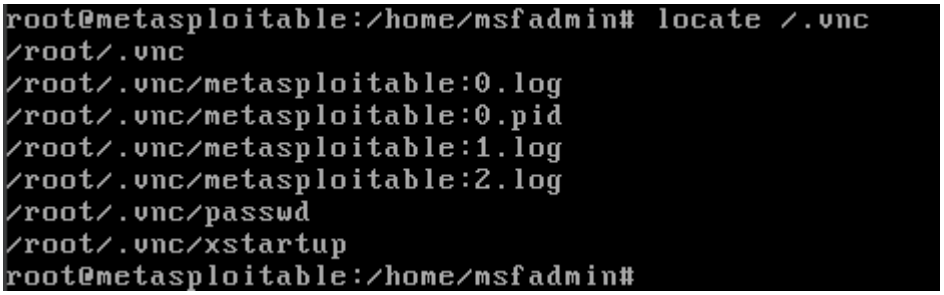
LISTA VULNERABILITA

Indice generale

VNC Server 'password' Password - CRITICAL

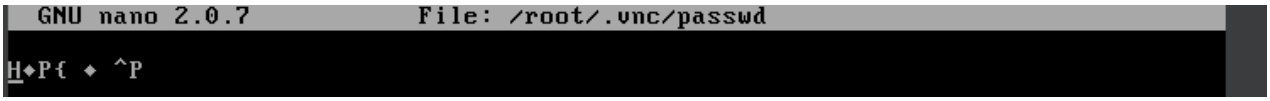
Per fixare questa vulnerabilità , stando al report di NESSUS , bastava rinforzare la password di VNC (Virtual Network Computing) , un software che permette l accesso remoto alla macchina.

Effettuando delle ricerche risultava che il file fosse all interno della cartella **/.vnc** , dovevo quindi trovare la sua posizione , per farlo ho usufruito del comando “ locate “



una volta localizzata , ho dato un occhiata al file “ passwd “ che era quello di mio interesse

Questo risulta essere il contenuto al suo interno.



la password standard risulta criptata.

Per cambiarla invece ho usufruito del comando **“ passwd “** da terminale come utente SUPER USER (sudo su) , perché non utilizzando il SUPER USER , la modifica non venica effettuata.

Il comando **passwd** ha come funzionalità quella di modificare appunto la password di VNC

Ri facendo la scansione con Nessus il problema risulta FIXATO

Bind Shell Backdoor Detection – CRITICAL

Per fixare questa vulnerabilità , stando al report di NESSUS , Verificare se l'host remoto era stato compromesso e se necessario, reinstallare il sistema.
Non è stato necessario reinstallare il sistema perché stando al report di Nessus e accertandomi del problema , risultavano aperte della backdoor nelle porte TCP1524 /6667.
Essendo in modalità SUPER USER per accertarmi del problema ho usato il seguente comando :
“ **netstat -tuln | grep 1524** “
`netstat :` mi restituisce le connessione all interno della macchina

`-t` : filtra la richiesta alle connessioni TCP.

`-u` : filtra la richiesta alle connessioni UDP.

`-l` : filtra la richiesta solo per le porte in ascolto (listening) per l eventuale Backdoor

`-n` : visualizza gli indirizzi IP e numeri di porta in formato numerico

`|` : consente di passare l'output di un comando come input a un altro comando

```
root@metasploitable:/home/msfadmin# netstat -tuln | grep 1524
tcp        0      0 0.0.0.0:1524            0.0.0.0:*               LISTEN
```

`grep 1524` : serve per filtrare tutte le righe della risposta che contengono "1524".

il comando successivo mi è servito ad indentificare il processo che stava creando il processo , ed è e : **lsof -i :1524**
lsof: Stands for "list open files" elenca i file aperti da processi in esecuzione su un sistema

-i: r filtra i risultati in base alle connessioni di rete.

```
root@metasploitable:/home/msfadmin# sudo lsof -i :1524
COMMAND  PID USER   FD   TYPE DEVICE SIZE NODE NAME
xinetd  4430 root   10u  IPv4  12016       TCP *:ingreslock (LISTEN)
```

:1524: specifica la porta di rete che mi interessa, nel mio caso la 1524.

avendo scoperto che era **xinetd** a causare il problema è bastato rimuoverlo per la risoluzione della porta **1524**

Un altra possibile soluzione era quella di utilizzare il firewall creando una regola su Pfsense che andasse a fitltrare o bloccare il traffico di dati della porta interessata , in questo caso la 1524.

46882 - UnrealIRCd Backdoor Detection

Per fixare questa vulnerabilità , ho sfruttato ciò che forniva nessus nella descrizione , ovvero : Il server IRC remoto è una versione di UnrealIRCd con una backdoor che consente a un utente malintenzionato di eseguire codice arbitrario sull'host interessato.” Per risolvere questo problema , ho sfruttato la prima parte dei passaggi usati per risolvere per la Bind Shell Backdoor detection ovvero :

“ **netstat -tuln | grep 6667** “ poi “ **lsof -i :6667 “**

```
root@metasploitable:/home/msfadmin# netstat -tuln | grep 6667
tcp        0      0 0.0.0.0:6667            0.0.0.0:*               LISTEN
root@metasploitable:/home/msfadmin# lsof -i :6667
COMMAND    PID USER   FD   TYPE DEVICE SIZE NODE NAME
unrealirc 4571 root    2u  IPv4  12222       TCP *:ircd (LISTEN)
```

Dopo aver confermato che Unreal IRC aveva una Backdoor ho effettuanto una ricerca su dove potesse essere la cartella di configurazione per controllare eventuali anomalie .

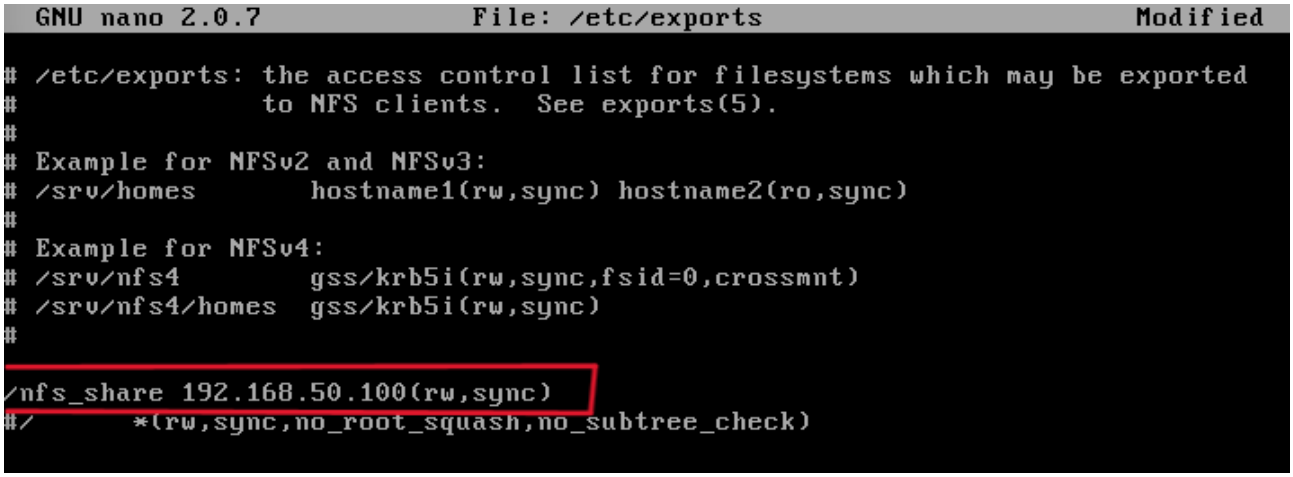
Una vlta trovata la cartella, sono appunto andato a cercare al suo interno qualche voce che potesse creare il problema , per farlo ho sfruttato la funzione di ricerca delle parole presneti nel testo con **ctrl+w** e filtrando per **Listen** trovando così due voci in ascolto sulla porta 6667 e 6697

Per risolvere ho commentato le due voci mettendoci il # di fronte

```
  GNU nano 2.0.7        File: /etc/unreal/unrealircd.conf

};

listen          *:6697
{
        options
        {
                clientsonly;
        };
};

listen          *:6667;
```

NFS Exported Share Information Disclosure –CRITICAL

Per fixare questa vulnerabilità , stando al report di NESSUS bisognava Configurare NFS sull'host remoto in modo che solo gli host autorizzati possano accedervi
Per fare ciò ho cambiato le impostazioni di condivisione della Directory di NFS
/nfs_share : è la cartella che condivido attraverso NFS
specifico l Ip che ha la possibilità di accedervi (192.168.50.100 – VB kali)
rw : corrisponde al permesso di scrittura e lettura
sync : indica che che le impostazioni di scrittura vengono effettuate dopo che sono state confermate.



Rexecd service detection

Questa vulnerabilità in origine non era presente, ma eseguendo degli accertamenti risultava presente , perr fixarla, stando ai “ consigli di NESSUS online, bisognava commentare la sezione '**exec**' in **/etc/inetd.conf** e riavviare il processo.

Samba Badlock Vulnerability - HIGH

Per fixare questa vulnerabilità , stando al report di NESSUS , bastava aggiornarlo alla versione 4.2.11 / 4.3.8 / 4.4.2 , questo problema non era risolvibile a causa della nostra versione della macchina Metasploitable (versione 2) a cui sono stati bloccati gli aggiornamenti.

Essendo non utile ai nostri scopi didattici ho optato per la sua rimozione utilizzando i seguenti comandi :

sudo apt-get remove samba , che serve appunto per rimuovere il pacchetto samba

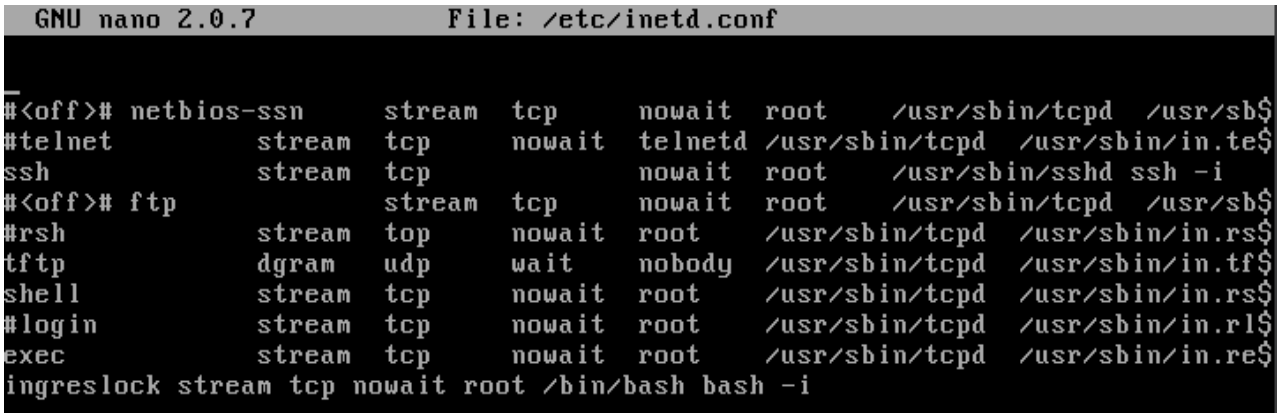
sudo apt-get purge samba , usato in aggiunta per eliminare eventuali pacchetti collegati a esso .

```
root@metasploitable:/home/msfadmin# sudo apt-get remove samba
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  samba-common
Use 'apt-get autoremove' to remove them.
The following packages will be REMOVED:
  samba
0 upgraded, 0 newly installed, 1 to remove and 138 not upgraded.
After this operation, 6590kB disk space will be freed.
Do you want to continue [Y/n]? y
(Reading database ... 37634 files and directories currently installed.)
Removing samba ...
Stopping Samba daemons: nmbd smbd.
root@metasploitable:/home/msfadmin# sudo apt-get purge samba
Reading package lists... Done
Building dependency tree
Reading state information... Done
Package samba is not installed, so not removed
The following packages were automatically installed and are no longer required:
  samba-common
Use 'apt-get autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 138 not upgraded.
root@metasploitable:/home/msfadmin# _
```

rlogin Service Detection - HIGH

Per fixare questa vulnerabilità , stando al report di NESSUS , bastava Commentare la riga 'login' in /etc/inetd.conf

essendo in modalita Superuser ho utilizzato il comando – “ nano /etc/inetd.conf “



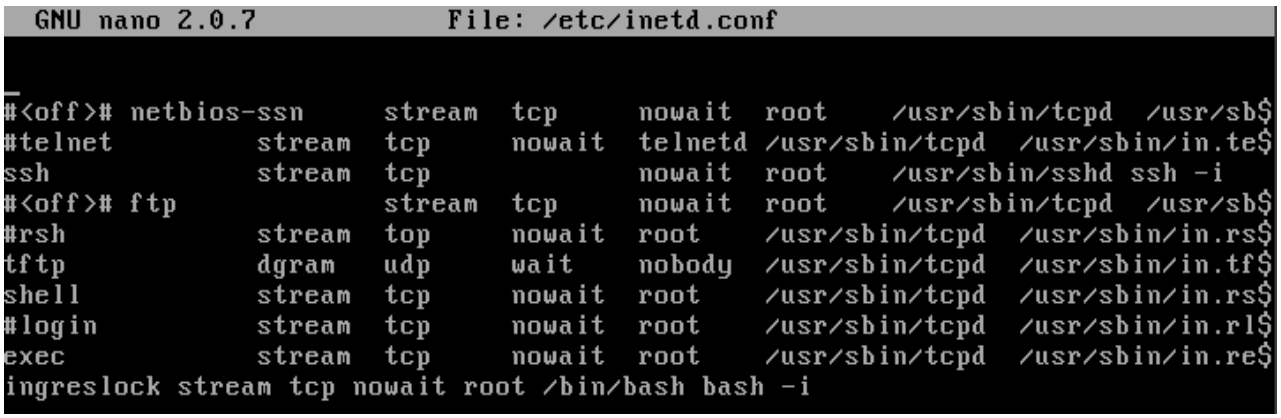
una volta entrati all interno è bastato mettere un cancelleto di fronte alla riga “ login “ come da suggerimento per risolvere il problema

rsh Service Detection - HIGH

Il principio è lo stesso di rlogin “ Service Detection – HIGH ”

Per fixare questa vulnerabilità , stando al report di NESSUS , bastava Commentare la riga 'login' in /etc/inetd.conf

essendo in modalita Superuser ho utilizzato il comando – “ nano /etc/inetd.conf “



una volta entrati all interno è bastato mettere un cancelleto di fronte alla riga “ rsh “ come da suggerimento per risolvere il problema