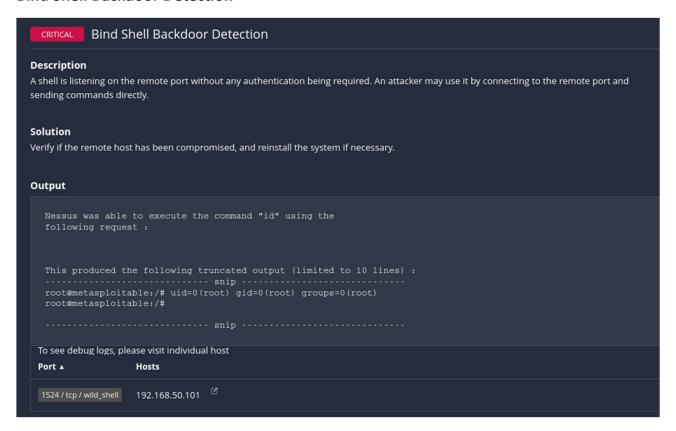
Scansioniamo il sistema Metasploitable con Nessus.



Risolviamo le vulnerabilità più gravi.

Bind Shell Backdoor Detection



Troviamo il processo relativo alla **porta**.

```
uapo U :::53 :::*

root@metasploitable:/home/msfadmin# netstat -tuln | grep ":1524"

tcp 0 0 0.0.0:1524 0.0.0.0:* LISTEN

root@metasploitable:/home/msfadmin# sudo lsof -i :1524

COMMAND PID USER FD TYPE DEVICE SIZE NODE NAME

xinetd 4455 root 12u IPv4 12317 TCP *:ingreslock (LISTEN)

root@metasploitable:/home/msfadmin# _
```

Potremmo fermare il processo o disabilitare il servizio associato, ma comunque potrebbe ripartire al riavvio; è necessario quindi **eliminare** completamente la backdoor dal sistema.

```
GNU nano 2.0.7
                             File: /etc/inetd.conf
#<off># netbios-ssn
                         stream
                                 tcp
                                          nowait
                                                  root
                                                           /usr/sbin/tcpd
                                                                            /usr/sb$
telnet
                stream
                                 nowait
                                          telnetd /usr/sbin/tcpd /usr/sbin/in.tes
                         tcp
#<off># ftp
                         stream
                                          nowait
                                                  root
                                                           /usr/sbin/tcpd
                                 tcp
                                                                            /usr/sb5
tftp
                dgram
                         udp
                                 wait
                                          nobody
                                                  /usr/sbin/tcpd
                                                                   /usr/sbin/in.tf
shell
                stream
                         tcp
                                 nowait
                                          root
                                                  /usr/sbin/tcpd
                                                                   /usr/sbin/in.rs
login
                                 nowait
                                          root
                                                  /usr/sbin/tcpd
                                                                   /usr/sbin/in.rl$
                stream
                         tcp
                                 nowait
                                                  /usr/sbin/tcpd
                                                                   /usr/sbin/in.re$
exec
                stream
                         tcp
                                          root
ingreslock stream tcp nowait root /bin/bash bash -i
                                 [ Read 8 lines ]
  Get Help
                WriteOut
                              Read File
                                            Prev Page
                                                         Cut Text
                                                                       Cur Pos
                                            Next Page
                Justify
                              Where Is
                                                         UnCut Text
```

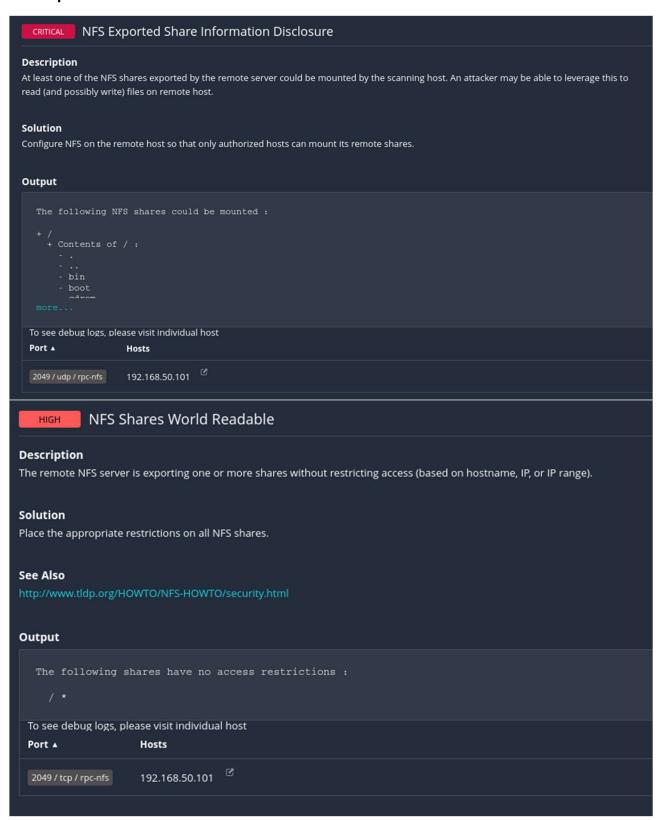
Lo facciamo andando nel file di configurazione di **inetd** e cancellando l'ultima riga, responsabile dell'apertura della backdoor tramite la quale si potevano inviare comandi direttamente nella shell di metasploitable da remoto senza autenticazione.

VNC Server 'password' Password



La soluzione qui è molto semplice; basta modificare la password del servizio **vnc** con il comando da terminale **vncpasswd**, impostando una password sicura.

NFS Exported Share Information Disclosure e NFS Shares World Readable

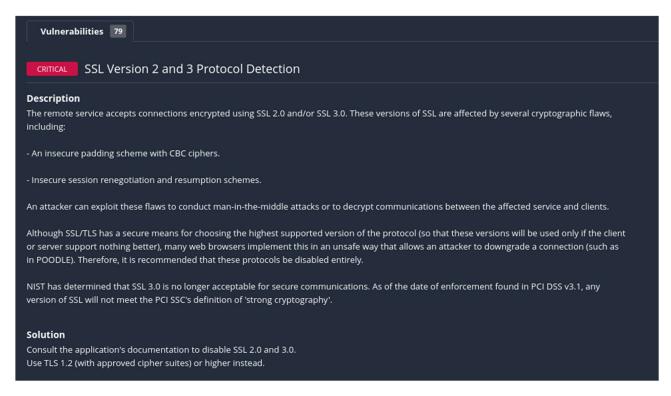


Analizziamo il file di configurazione di **nfs**.

```
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:
                 gss/krb5i(rw,sync,fsid=0,crossmnt)
/srv/nfs4
/srv/nfs4/homes
                gss/krb5i(rw,sync)
                             [ Read 10 lines ]
           10 WriteOut
                        ^R
                           Read File
                                      Y Prev Page
                                                   ^K
                                                     Cut Text
                                                                C Cur Pos
Get Help
              Justify
 Exit
                        ^₩
                           Where Is
                                        Next Page
                                                   îU UnCut TextîT
                                                                   To Spell
```

Eliminiamo la riga che permetteva l'accesso a **qualunque client da remoto** in scrittura e lettura con permessi di root; inoltre i cambiamenti effettuati sui file condivisi venivano scritti sincronamente sul disco fisico (sopra l'immagine del file di configurazione correttamente modificato). L'accesso andrà consentito soltanto a hosts specifici, sulle cartelle necessarie (non la root) e con i permessi minimi necessari.

SSL Version 2 and 3 Protocol Detection



Questo problema è presente sia sulla porta 25 dove è attivo il servizio smtp **postfix** e sulla porta 5432 dove è attivo il servizio **postgresql**.

```
GNU nano 2.0.7
                   File: /etc/apache2/mods-available/ssl.conf
                                                                   Modified
   List the ciphers that the client is permitted to negotiate.
   See the mod_ssl documentation for a complete list.
#SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
   enable only secure ciphers:
#SSLCipherSuite HIGH:MEDIUM:!ADH
# enable only secure protocols: SSLv3 and TLSv1, but not SSLv2
SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1_
G Get Help
            🔟 WriteOut
                         🔐 Read File 🔐 Prev Page 🔐 Cut Text
  Exit
              Justify
                         N Where Is
                                     Next Page UnCut Text To Spell
```

```
GNU nano 2.0.7
                    File: /etc/postgresq1/8.3/main/postgresq1.conf
max connections = 100
                                         # (change requires restart)
# Note: Increasing max_connections costs ~400 bytes of shared memory per
# connection slot, plus lock space (see max_locks_per_transaction).
                                                                       You might
# also need to raise shared_buffers to support more connections.
#superuser_reserved_connections = 3
                                         # (change requires restart)
unix_socket_directory = '/var/run/postgresql'
#unix_socket_group = '' # (c)
                                                          # (change requires rest$
                                         # (change requires restart)
#unix_socket_permissions = 0777
                                         # begin with 0 to use octal notation
                                         # (change requires restart)
#bonjour_name = ''
                                         # defaults to the computer name
                                         # (change requires restart)
# - Security and Authentication -
#authentication_timeout = 1min
                                         # 1s-600s
#ssl = true
                                         # (change requires restart)
#ssl_ciphers = 'ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH'
                                                        # allowed SSL ciphers
                                         # (change requires restart)
#password_encryption = on
#db_user_namespace = off
                               [ "tls" not found ]
                           R Read File
                                           Prev Page K Cut Text
  Get Help
             10 WriteOut
                                                                   C Cur Pos
  Exit
                Justify
                              Where Is
                                           Next Page TU UnCut Text T
```

Modificando i file di configurazione in modo tale da obbligare all'utilizzo del **tls** (aggiungendo la direttiva **SSLProtocol** su apache2 e commentando la riga che abilita l'**ssl** (ssl = true) costringendo pertanto ad utilizzare il tls, per postgresql) e rilanciando la scansione vediamo che il problema per postgresql è risolto, mentre per postfix, trattandosi di una versione molto vecchia che probabilmente non accetta direttive sulle versioni ssl, il consiglio è di **aggiornare** ad una versione più recente.

Effettuiamo nuovamente la scansione con Nessus.



Abbiamo risolto una buona parte dei problemi più gravi; si noti infine come per risolvere i rimanenti basterebbe semplicemente **aggiornare** i rispettivi software a versioni più recenti.