

## 11356 - NFS Exported Share Information Disclosure

Per risolvere questa criticità sono andato a modificare il file `hosts.deny` ed il file `hosts.allow` nella cartella `/etc` che controllano i TCP Wrappers, un insieme di funzioni utili per gestire gli accessi al vostro sistema dall'esterno. In questo caso ho modificato le regole cancellando nel file `allow` il `ALL:ALL` che permetteva a tutti gli host di accedere e mettendo `ALL:ALL` in `deny` per proibire a qualunque host di connettersi. Ovviamente in ottica aziendale i file aziendali verranno modificati per permettere a chi ha il permesso di accedere.

```
msfadmin@metasploitable: /etc$ sudo nano hosts.deny _
```

```
GNU nano 2.0.7 File: hosts.deny
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
# See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:      ALL: some.host.name, .some.domain
#              ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper, as well as for
# rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
# for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID
ALL:ALL
[ Read 20 lines ]
```

```
GNU nano 2.0.7 File: /etc/hosts.allow
# /etc/hosts.allow: list of hosts that are allowed to access the system.
# See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:      ALL: LOCAL @some_netgroup
#              ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper, as well as for
# rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
# for further information.
#
```

## 61708 - VNC Server 'password' Password

Seguendo le indicazioni risolutive scritte nel report di Nessus sono andato a cambiare la password del servizio VNC che era molto debole. Per prima cosa ho fatto sudo su per avere i privilegi di root:

```
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# _
```

Dopodichè ho lanciato il comando vncpasswd per potere cambiare la password e sono andato ad inserire la nuova password più sicura:

```
root@metasploitable:/home/msfadmin# vncpasswd
[[IDUsing password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin#
```

## 51988 - Bind Shell Backdoor Detection

Per ovviare al problema della backdoor sono andato a modificare le firewall policies di meta tramite il comando iptables:

```
msfadmin@metasploitable:/$ sudo iptables -I INPUT -p tcp -s 192.168.50.100 --dport 1524 -j DROP
msfadmin@metasploitable:/$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target      prot opt source                destination           tcp dpt:ingreslock
DROP        tcp  --  192.168.50.100         anywhere              tcp dpt:ingreslock
```

In questo modo la macchina Metasploitable non accetta comunicazioni in entrata provenienti dall'IP 192.168.50.100 per il protocollo TCP sulla porta 1524.