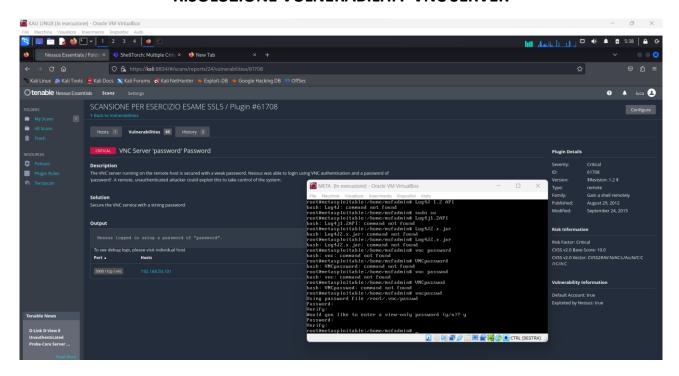
### **CONSEGNA ESERCIZIO S5L5**

### RISOLUZIONE VULNERABILITA' VNC SERVER



Per risolvere la seguente criticità siamo andati a variare la **password del server VNC** mettendone una più sicura in modo da non permettere ad un attaccante di entrare con facilità.

## RISOLUZIONE VULNERABILITA' "RLOGIN SERVICE DETECTION" E "RSH SERVICE DETECTION"

HIGH	7.5 *	5.9	rlogin Service Det	Service detection	1	0	1
HIGH	7.5 *	5.9	rsh Service Detec	Service detection	1	0	1

```
#<off># netbios-ssn
                        stream
                                tcp
                                         nowait
                                                 root
                                                         /usr/sbin/tcpd
                                                                         /usr/sb$
telnet
                                nowait
                                         telnetd /usr/sbin/tcpd /usr/sbin/in.te$
                stream
                        tcp
#<off># ftp
                        stream
                                tcp
                                         nowait
                                                root
                                                         /usr/sbin/tcpd
                        udp
                                wait
                                                /usr/sbin/tcpd /usr/sbin/in.tf$
tftp
                dgram
                                         nobody
                                                /usr/sbin/tcpd /usr/sbin/in.rs$
#shell
                                nowait
                stream
                        tcp
                                        root
                                                /usr/sbin/tcpd /usr/sbin/in.rl$
                        tcp
#login
                                nowait
                                        root
                stream
Hexec
                stream
                        tcp
                                nowait
                                        root
                                                /usr/sbin/tcpd /usr/sbin/in.re$
ingreslock stream tcp nowait root /bin/bash bash -i
```

Per risolvere la seguente criticità abbiamo reso commenti la linea di **login** e **exec**, rendendole quindi #login e #exec.

Successivamente abbiamo fatto il restart del servizio xinetd.

#### RISOLUZIONE DELLA VULNERABILITA' BIND SHELL BACKDOOR DETECTION



Questa criticità è stata risolta andando a chiudere la porta **tcp:1524** attraverso la riga di comando sovrastante.

```
host is up (0.00033s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp
                             ssh
                             telnet
3/tcp
             open
3/tcp
                             domain
                            rpcbind
netbios-ssn
11/tcp
 39/tcp
             open
45/tcp
12/tcp
                             microsoft-ds
             open
                             exec
ol2/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
524/tcp filtered ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ft
                             rmiregistry
                             ccproxy-ftp
3306/tcp open
5432/tcp open
                            mysql
postgresql
900/tcp open
                            vnc
X11
5000/tcp open
5667/tcp open
3009/tcp open
3180/tcp open
                             unknown
MAC Address: 08:00:27:CA:2B:54 (Oracle VirtualBox virtual NIC)
  ap done: 1 IP address (1 host up) scanned in 1.40 seconds
```

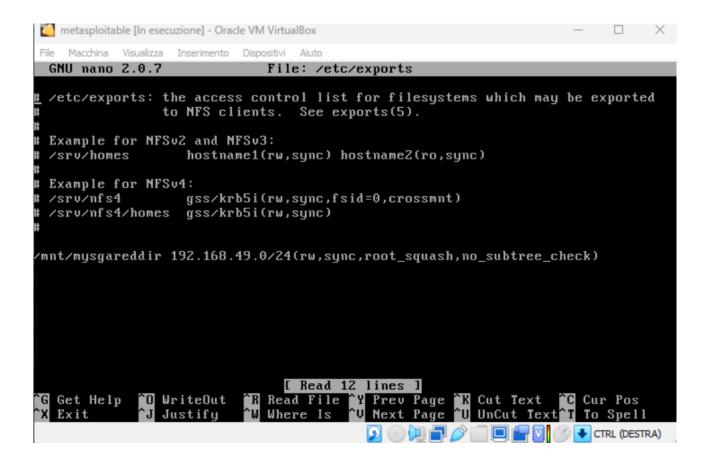
Come possiamo dall'immagine di sopra e stato eseguito un comando <<nmap>> per controllare che la porta tcp:1524 risultasse effettivamente filtered dal firewall.



Successivamente è stato eseguito un controllo ulteriore attraverso **NESSUS** per controllare che la **vulnerabilità** fosse scomparsa.

# RISOLUZIONE DELLA CRITICITA': NFS EXPORTED SHARE INFORMATION DISCLOSURE

NFS Exported Share Information Disclosure
<b>Description</b> At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.
Solution Configure NFS on the remote host so that only authorized hosts can mount its remote shares.  Output
The following NFS shares could be mounted:  + / + Contents of /: 7E,UTW.}R - bin - boot - more
To see debug logs, please visit individual host  Port ▲ Hosts
2049 / udp / rpc-nfs 192.168.49.101 <sup>©</sup>



Questa criticità è stata risolta limitando gli accessi ai soli utenti sotto lo stesso <b>Network</b> così da impedire a utenti esterni l'accesso.