

Alcune vulnerabilità non sono risolvibili in quanto non sono azioni compibili per il nostro laboratorio, tipo aggiornare i sistemi operativi, o la versione di Apache

CRITICAL VNC Server 'password' Password

Per sistemare questa vulnerabilità, nella macchina vittima, metasploitable in questo caso, bisogna cambiare la password VNC:

da metasploitable prendiamo i privilegi ed eleviamoci a superuser con

```
# sudo su
```

E poi lanciare

```
# vncpasswd
```

e settare la nuova password per VNC

CRITICAL NFS Exported Share Information Disclosure

Da macchina metasploitable lanciamo il comando “nano /etc/exports” e commentiamo (aggiungendo #) l’ultima riga. Così facendo andremo ad impedire di creare sessioni remote ad ogni host.

Riavviamo il servizio con il comando “/etc/init.d/nfs-common restart”

CRITICAL Bind Shell Backdoor Detection

Come si legge dal documento di analisi, questa segnalazione è dovuta alla presenza della porta 1524 aperta e “passwordless”. Configuriamo una regola firewall per impedire che ciò capiti ancora

(va creata per ogni interfaccia)

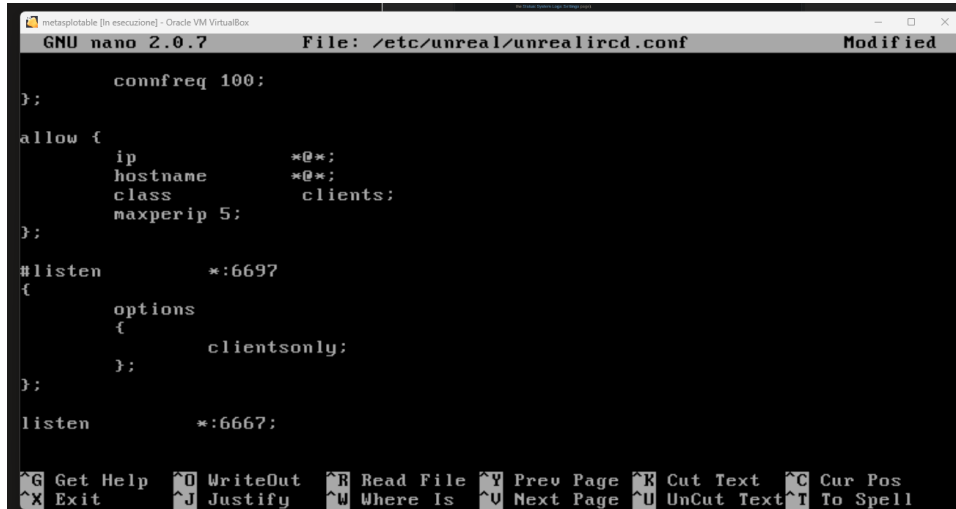
Queste vulnerabilità, per essere chiuse, chiedono di commentare la riga “login” e “rsh” in /etc/inetd.conf o disabilitare il servizio inet.

```
#<off># netbios-ssn      stream  tcp      nowait   root    /usr/sbin/tcpd  /usr/sb$
telnet      stream  tcp      nowait   root    /usr/sbin/tcpd  /usr/sbin/in.telnetd
#<off># ftp              stream  tcp      nowait   root    /usr/sbin/tcpd  /usr/sb$
ftpt        dgram   udp      wait     nobody  /usr/sbin/tcpd  /usr/sbin/in.ftptd
shell       stream  tcp      nowait   root    /usr/sbin/tcpd  /usr/sbin/in.rshd
rlogin      stream  tcp      nowait   root    /usr/sbin/tcpd  /usr/sbin/in.rlogind
exec        stream  tcp      nowait   root    /usr/sbin/tcpd  /usr/sbin/in.rexecd
ingreslock stream  tcp      nowait   root    /bin/bash bash -i
```

UNREAL RCDBACKDOOR DETECTION

Non trovata nella mia scansione, ma rilevata in altre macchine con la stessa configurazione.

Bisogna commentare la riga che tiene aperta la connessione per la porta 6697



```
GNU nano 2.0.7 File: /etc/unreal/unrealircd.conf Modified
};
    connfreq 100;

allow {
    ip          *@*;
    hostname    *@*;
    class       clients;
    maxperip 5;
};

#listen        *:6697
{
    options
    {
        clientonly;
    };
};

listen         *:6667;
```