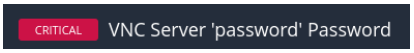
RIMEDI ALLE VULNERABILITA' CRITICHE DI

METASPLOTABLE

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5	5.9	Samba Badlock Vulnerability	General	1
HIGH	7.5		NFS Shares World Readable	RPC	1

1) ***Critical:* VNC Server "password" password.**



Per rimediare a questa vulnerabilità, data per l'inefficacia della password, ho impostato una password alternando numeri e caratteri con il comando:

vncpasswd

la password richede massimo

8 caratteri: M3t4spl-

```
Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Fri Jun 28 03:53:48 EDT 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
msfadmin@metasploitable:~$
```

vncserver -kill :1

2) ***Critical:** Blind Shell Backdoor Detection.*

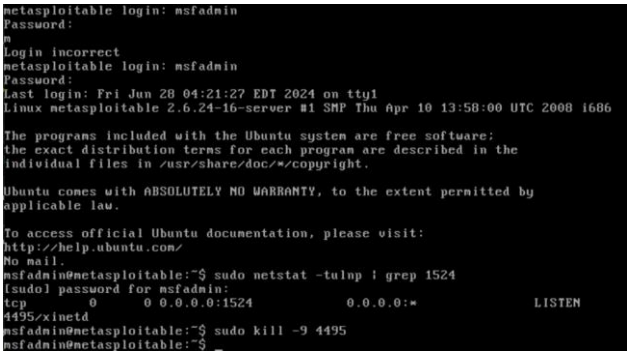
Per rimuovere la backdoor, toccherà capire quale porta è in ascolto alla 1524 tcp/vnc,

Per fare ciò eseguiamo il comando:

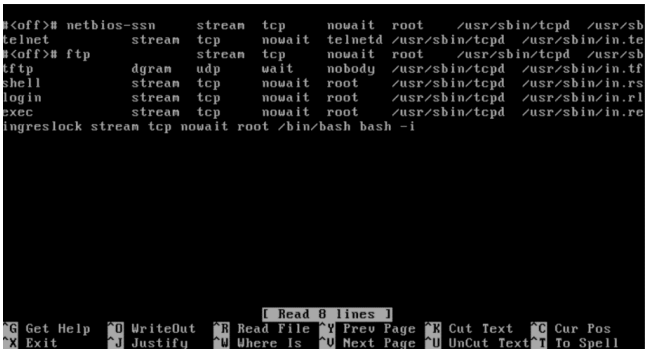
sudo netstat -tulnp | grep 1524

troverà la porta in ascolto 4495 che andremo a chiudere con il comando:

sudo kill -9 4495



sudo nano /etc/inetd.conf



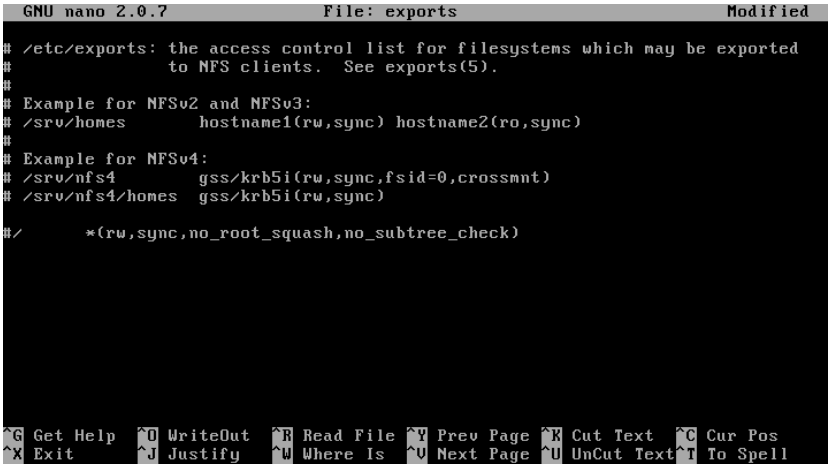
Ed eliminare la riga: Shell stream e salvare.

3) ***Critical:** NFS exported s.i disclosure*

Entrare sulla cartella /etc e modificare il file

/ *(rw, sync, no_root_squash,no_subtree_check)

aggiungendo un commento #



#/ *(rw, sync, no_root_squash,no_subtree_check) e salvare.