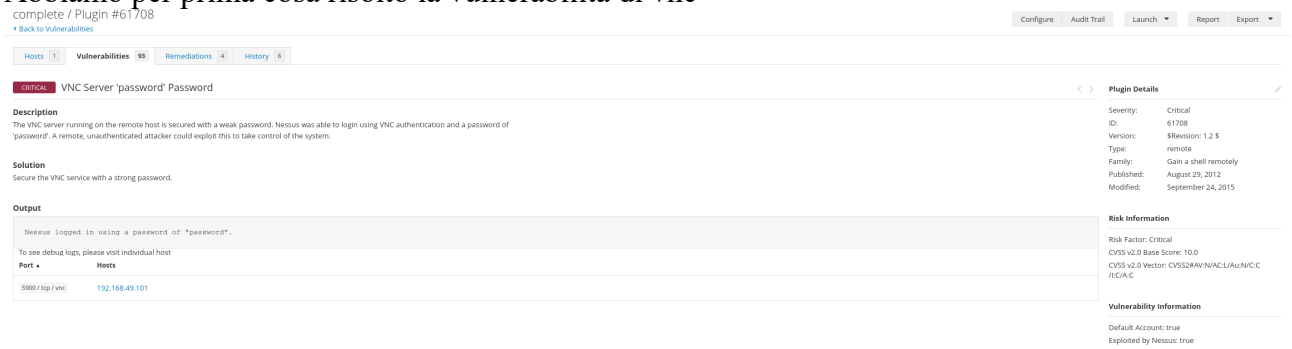
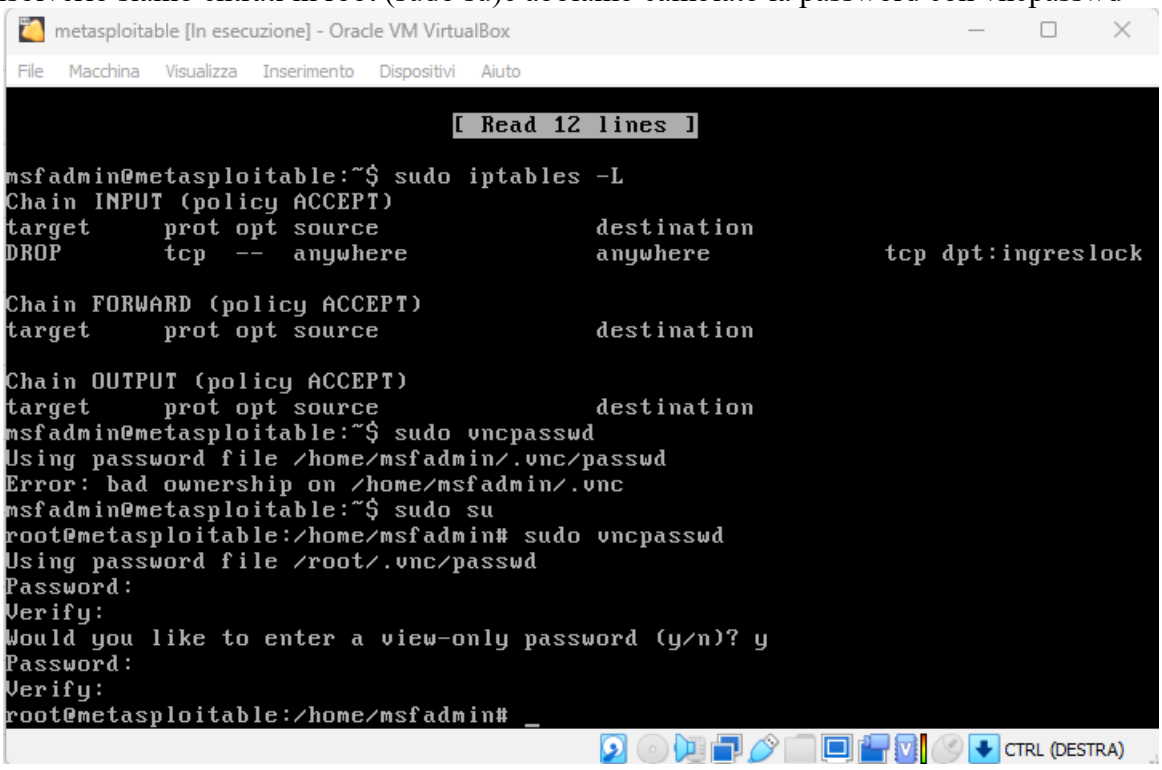
Obiettivo: correggere dalle 2 alle 4
Abbiamo cercato le vulnerabilità su metasploitable 2 da kali utilizzando nessus.
La scansione iniziale riportava:

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		Bind Shell Backdoor Detection	Backdoors	1
MIXED	...	...	Apache Tomcat (Multiple Issues)	Web Servers	4
MIXED	...	...	Phpmyadmin (Multiple Issues)	CGI abuses	4
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
MIXED	...	...	PHP (Multiple Issues)	CGI abuses	3
HIGH	8.3		CGI Generic SQL Injection (blind)	CGI abuses	1
HIGH	7.5	5.9	Samba Badlock Vulnerability	General	1
HIGH	7.5 *		CGI Generic Command Execution	CGI abuses	1
HIGH	7.5 *		CGI Generic Remote File Inclusion	CGI abuses	1
HIGH	7.5		NFS Shares World Readable	RPC	1
MIXED	...	...	ISC Bind (Multiple Issues)	DNS	5
MIXED	...	...	Twiki (Multiple Issues)	CGI abuses	2

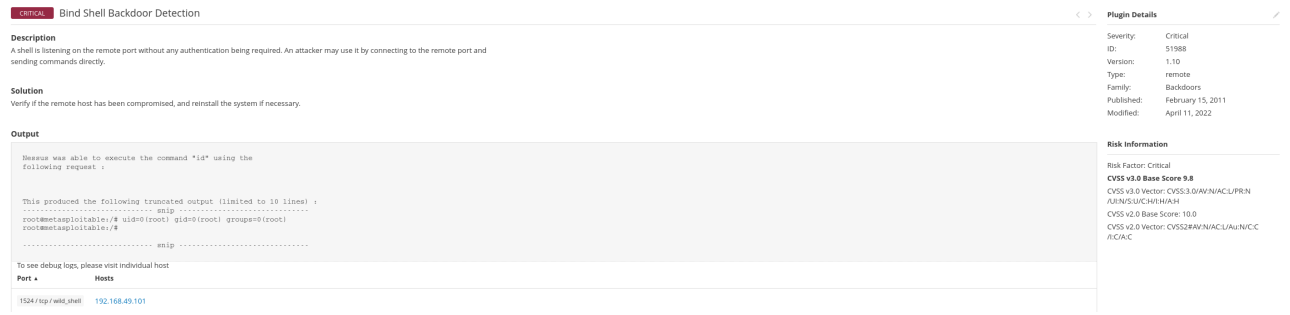
abbiamo individuato delle vulnerabilità da poter risolvere senza dare problemi all'operativa del sistema preso in esame.
Abbiamo per prima cosa risolto la vulnerabilità di vnc



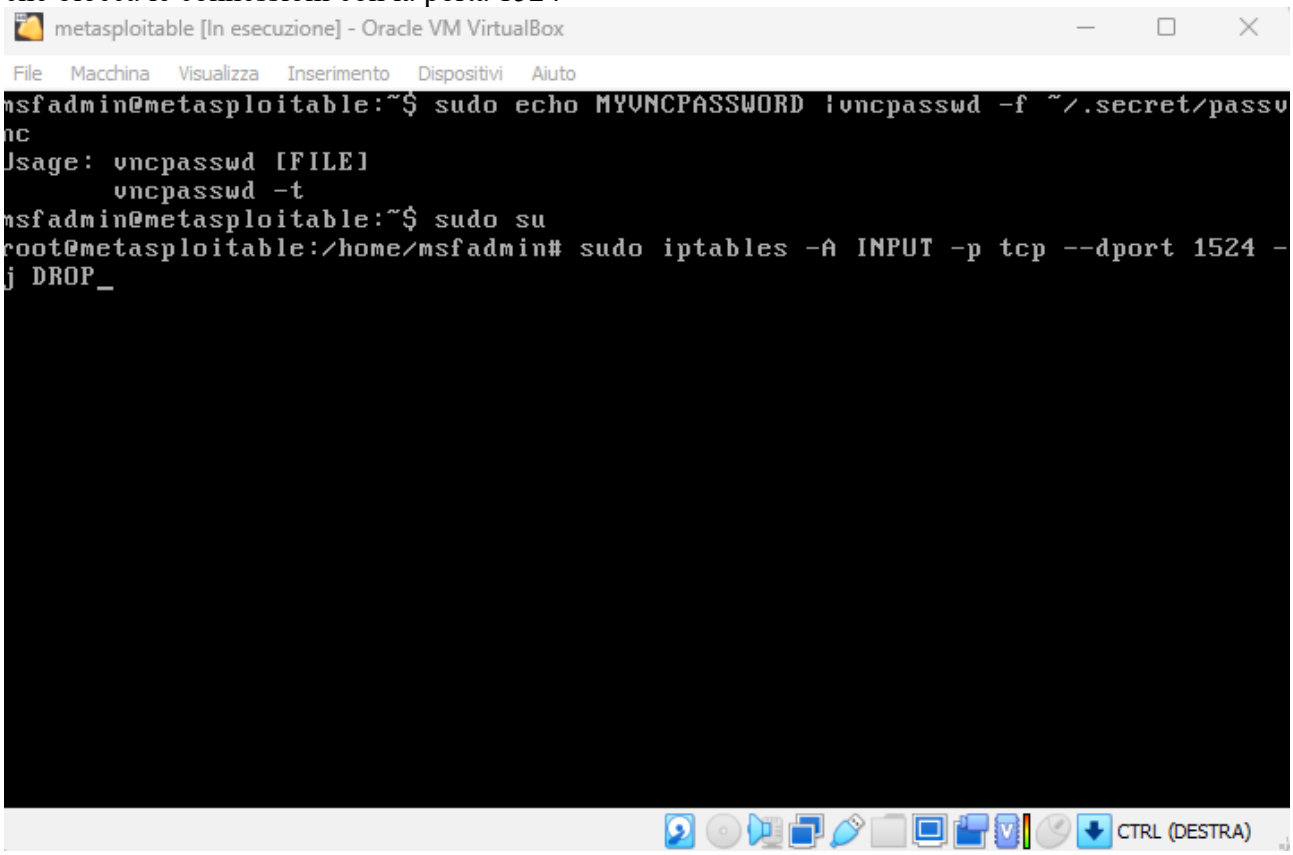
per risolverlo siamo entrati in root (sudo su)e abbiamo cambiato la password con vncpasswd



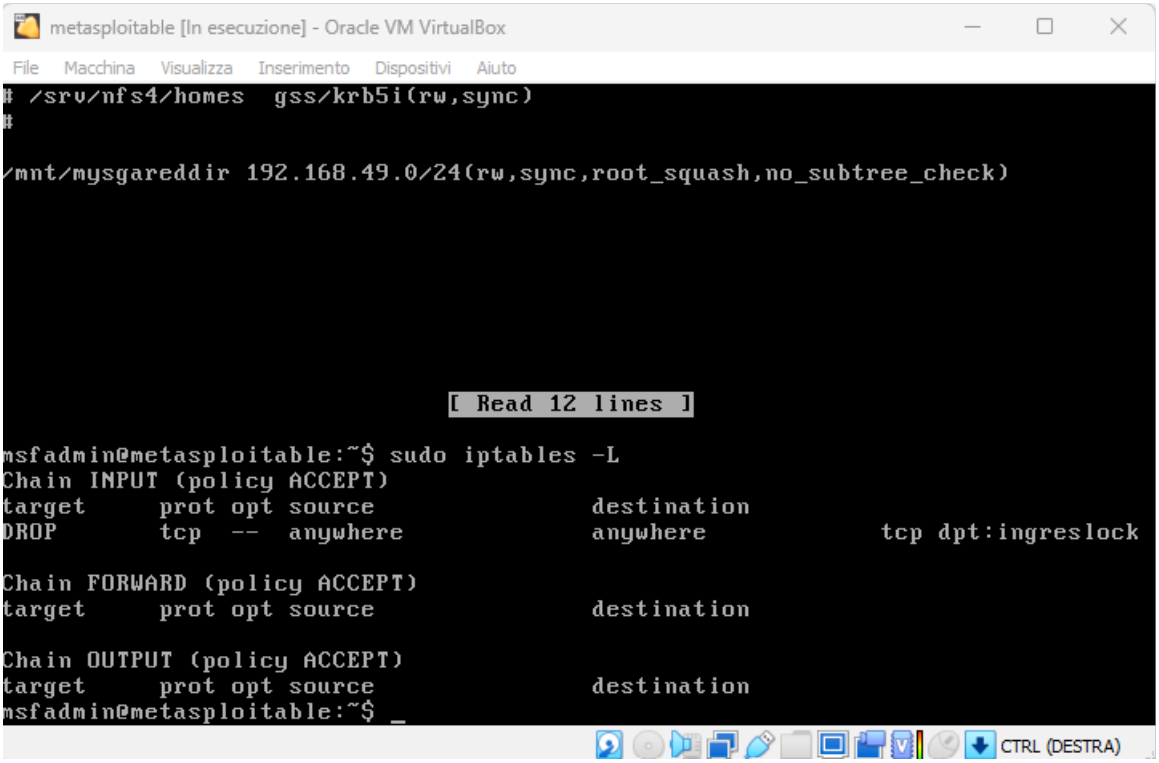
a seguire abbiamo preso in esame la vulnerabilita della backdoor aperta sulla porta 1524



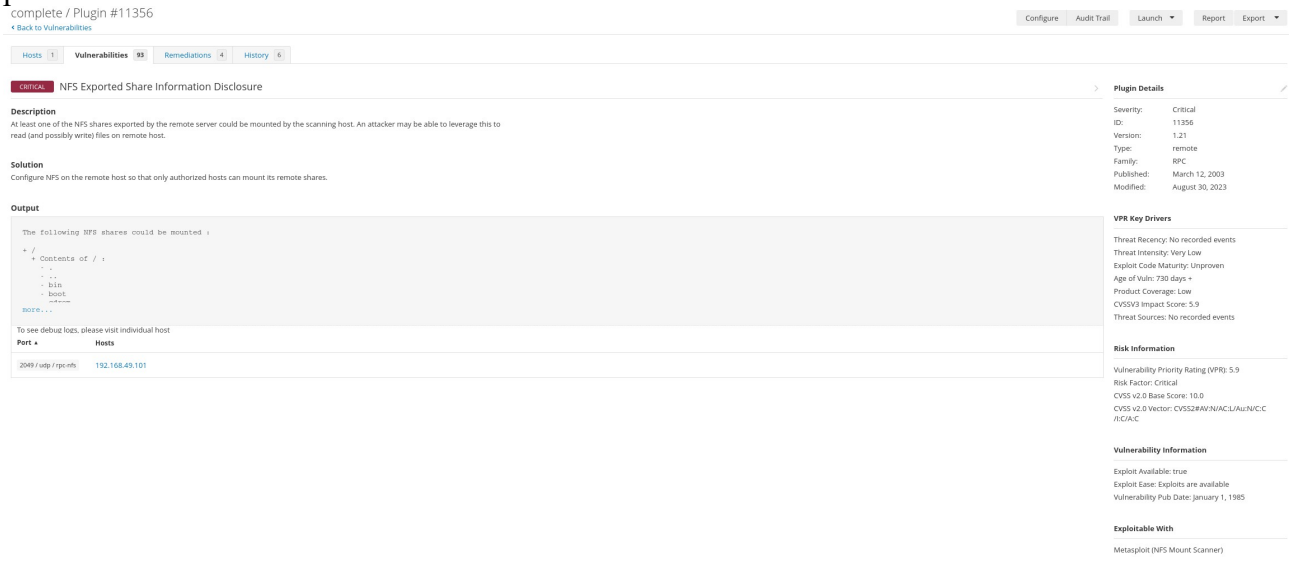
per risolvere questo problema siamo entrati in iptables dando il comando per aggiungere la regola che blocca le connessioni con la porta 1524



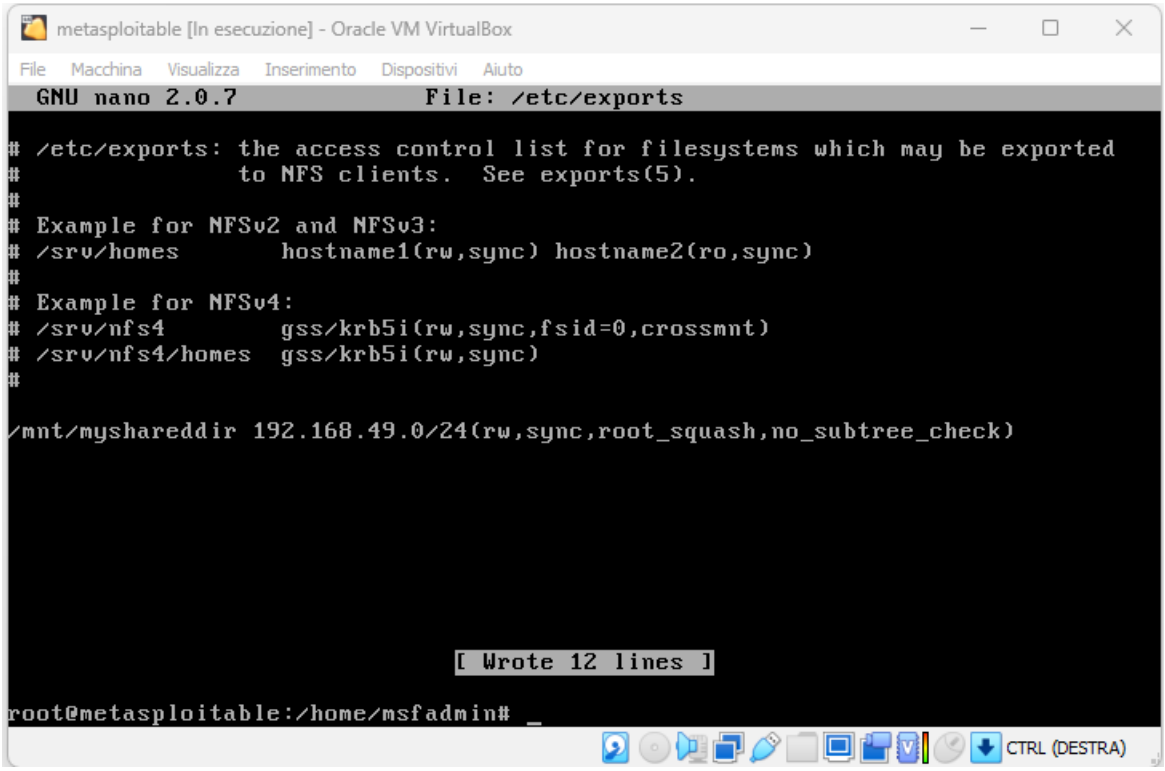
e nelle tabelle del router troviamo:



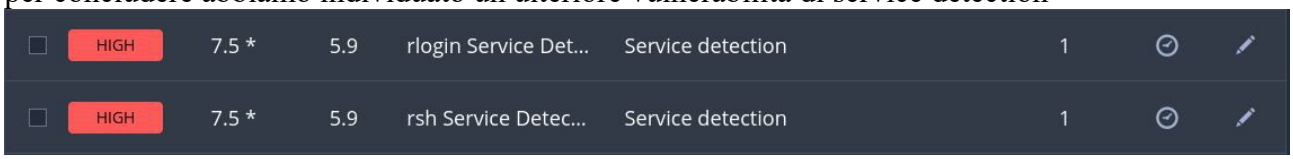
per la vulnerabilita relativa ai file nfs:



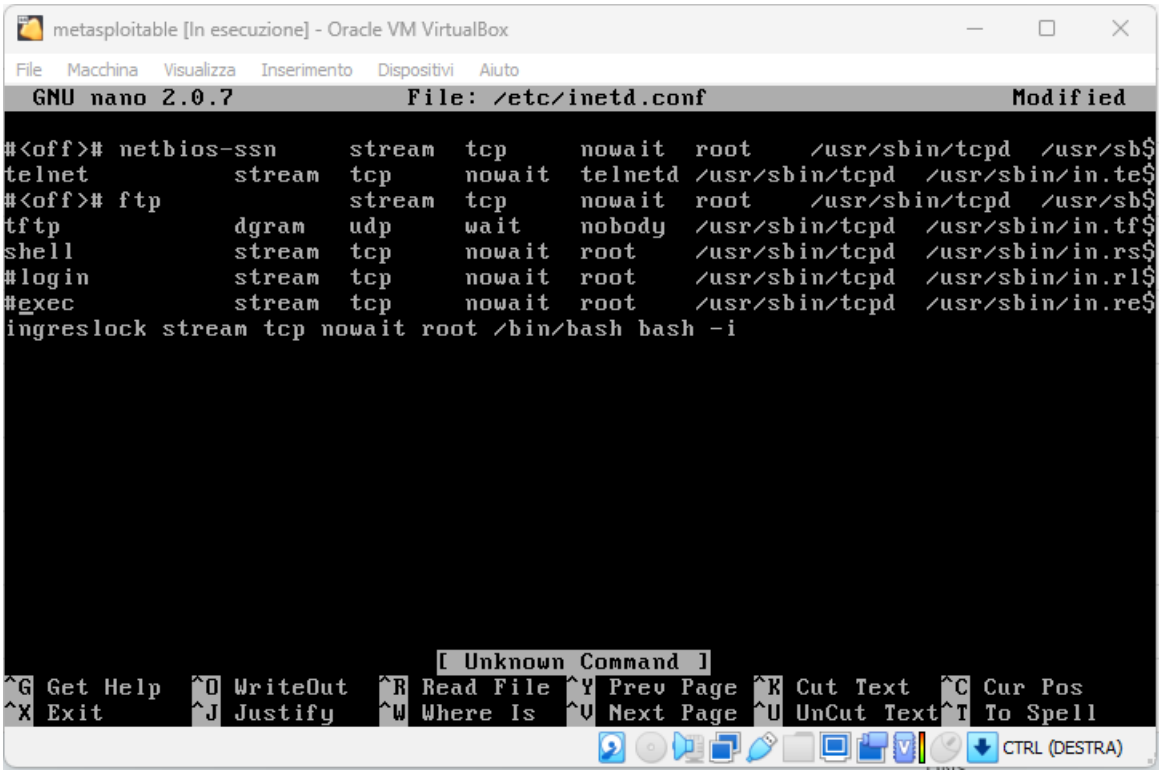
abbiamo modificato il file exports presente per limitare gli ho host che possono entrare nei file condivisi



per concludere abbiamo individuato un ulteriore vulnerabilità di service detection



per poterla risolvere siamo andati a modificare il file inetd.conf andando a commentare le righe di login ed exec:



cosi facendo abbiamo risolto alcuni tra i problemi critici e alti presenti nel sistema senza rallentare l'operatività dei sistemi.
La nuova scansione nessus riporta:

come possiamo vedere nelle vulnerabilità di livello critico e alto non sono più presenti i problemi riscontrati in precedenza