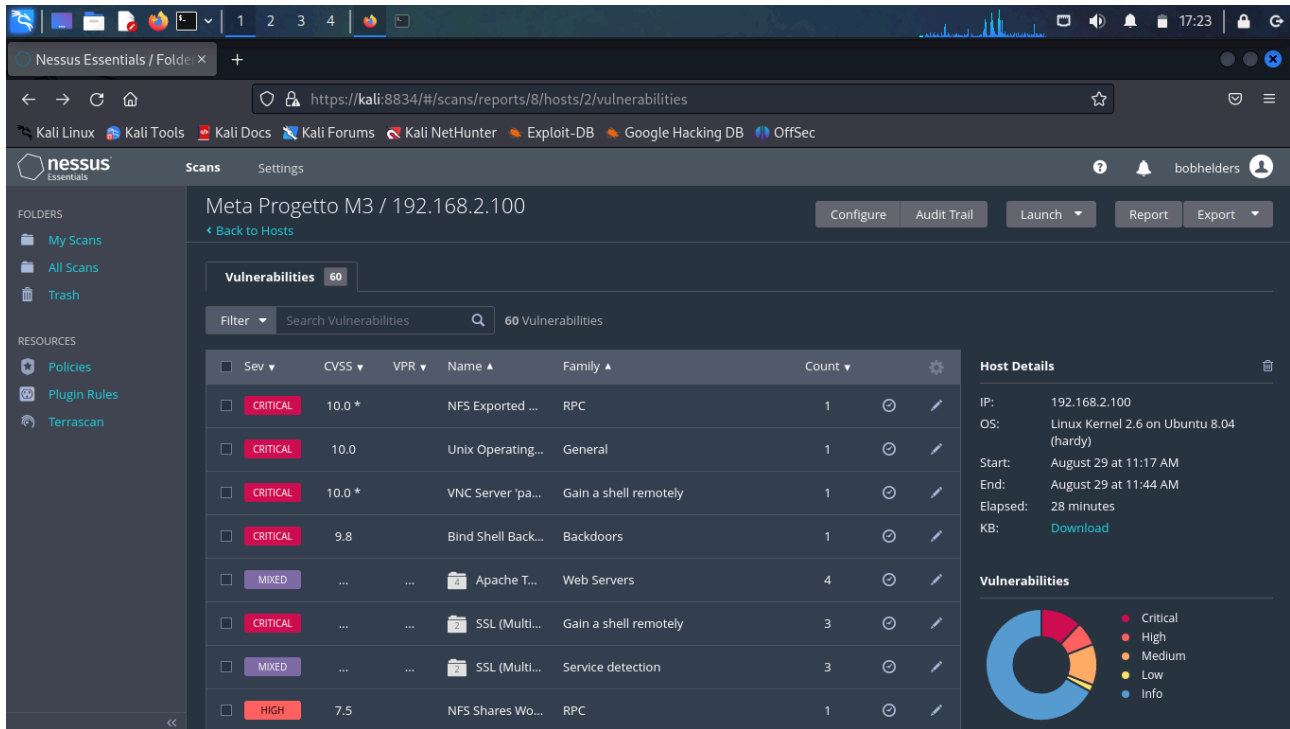


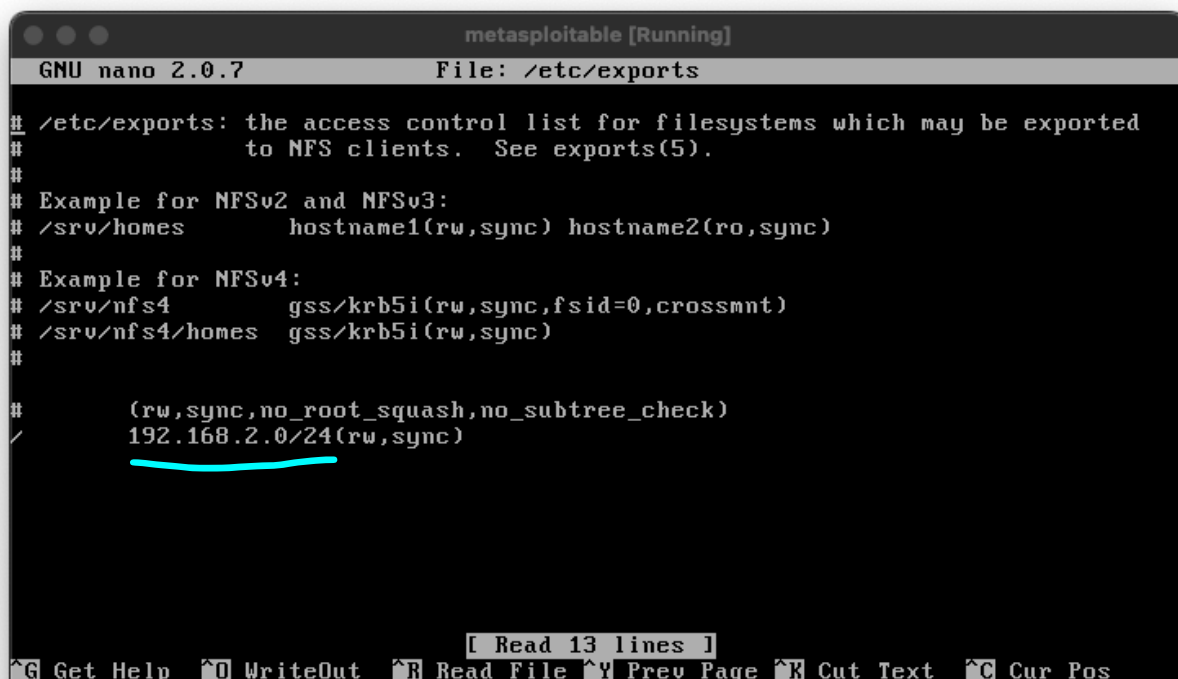
# Remediation e scansione finale



Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *		NFS Exported ...	RPC	1
CRITICAL	10.0		Unix Operating...	General	1
CRITICAL	10.0 *		VNC Server 'pa...	Gain a shell remotely	1
CRITICAL	9.8		Bind Shell Back...	Backdoors	1
MIXED	...	...	Apache T...	Web Servers	4
CRITICAL	...	...	SSL (Multi...	Gain a shell remotely	3
MIXED	...	...	SSL (Multi...	Service detection	3
HIGH	7.5		NFS Shares Wo...	RPC	1

Nell'immagine qui sopra possiamo vedere la prima scansione effettuata con Nessus.

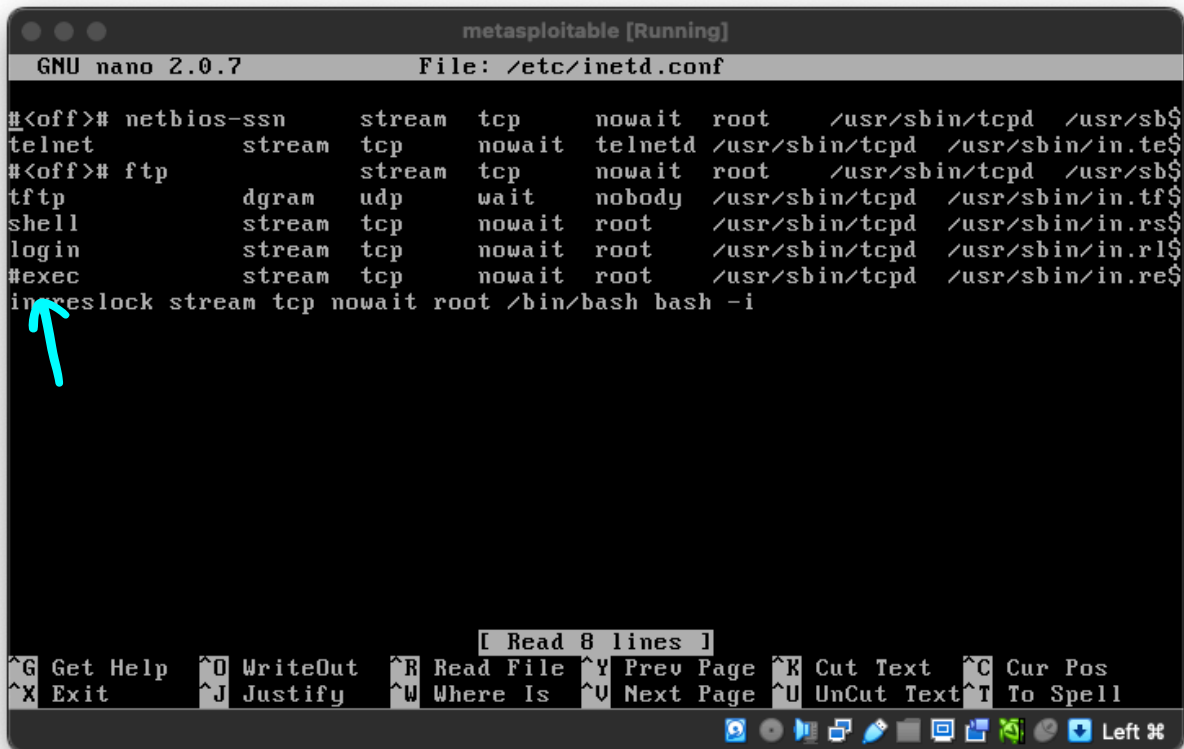
La prima vulnerabilità che sono andato a risolvere è “**NFS Exported Share Information Disclosure**”, che può essere sfruttata da un'attaccante per poter leggere e scrivere file grazie al file system condiviso. Ho semplicemente mitigato la vulnerabilità modificando i permessi di lettura e scrittura soltanto agli host appartenenti alla rete della macchina Metasploitable.



```
metasploitable [Running]
GNU nano 2.0.7 File: /etc/exports

# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
# (rw,sync,no_root_squash,no_subtree_check)
# 192.168.2.0/24(rw,sync)
```

La vulnerabilità “**rexecd Service Detection**” che si trova sulla slide della consegna non è stata trovata dalla scansione iniziale. Nonostante ciò ho controllato lo stesso il file di configurazione del servizio inetd e ho commentato la linea “exec” per evitare l’esecuzione di comandi da remoto, in quanto non c’è alcuna autenticazione.



```
metasploitable [Running]
GNU nano 2.0.7 File: /etc/inetd.conf

#<off># netbios-ssn    stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/
telnet                stream  tcp    nowait  telnetd  /usr/sbin/tcpd  /usr/sbin/in.telnetd
#<off># ftp            stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/
tftp                  dgram  udp    wait    nobody   /usr/sbin/tcpd  /usr/sbin/in.tftpd
shell                 stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rsh
login                 stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlogin
#exec                  stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rexecd
in.xlock stream tcp nowait root /bin/bash bash -i

[ Read 8 lines ]
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text    ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page  ^U UnCut Text  ^T To Spell
```

La terza vulnerabilità “**VNC Server password ‘password’**” è stata semplicemente cambiando la password del server (per motivi puramente didattici e di spiegazione è stata scelta la password ciao123, ovviamente una password non sicura). Questa poteva essere cambiata sia manualmente tramite la modifica del file oppure tramite il comando vncpasswd.

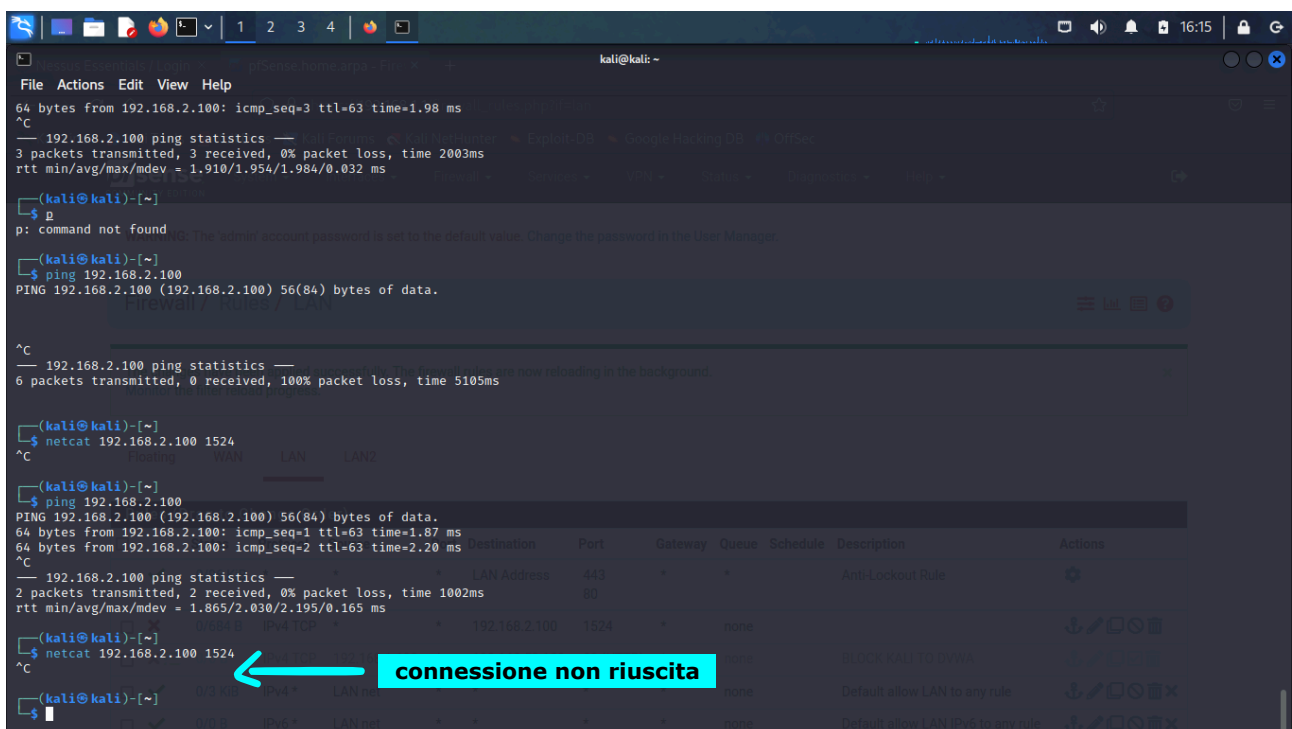
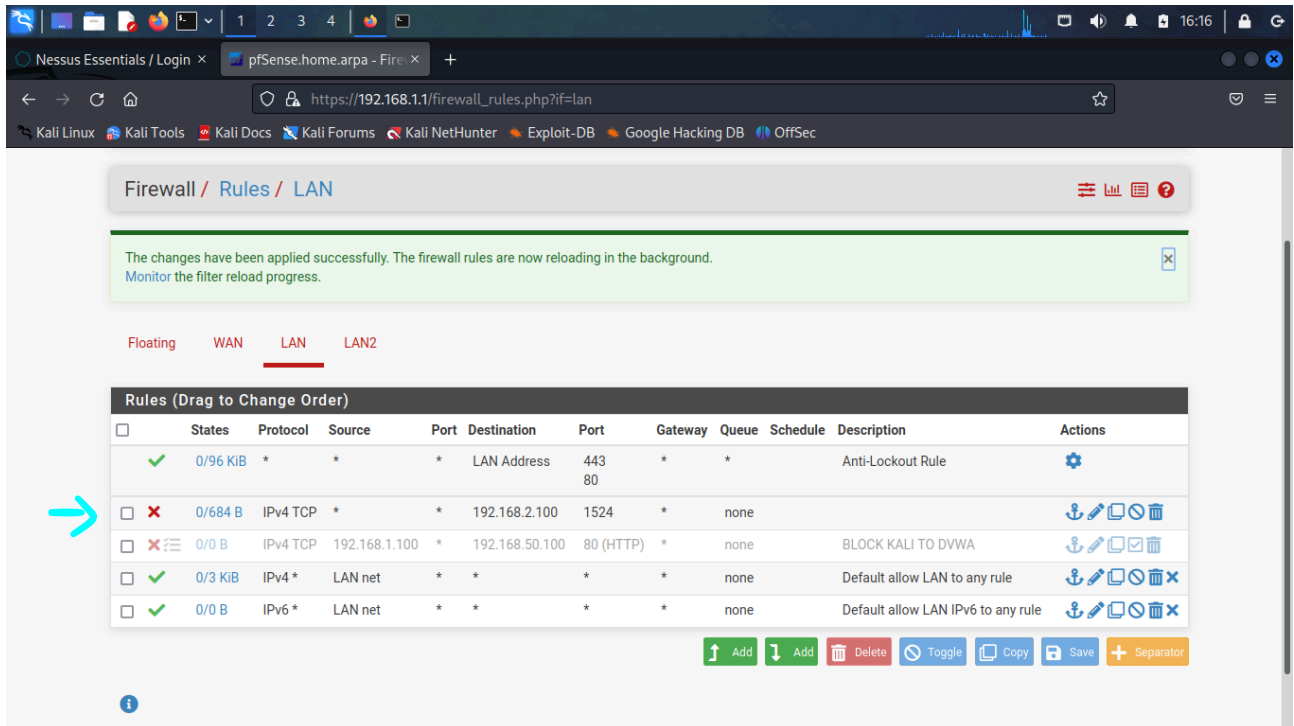


```
metasploitable [Running]
GNU nano 2.0.7 File: passwd

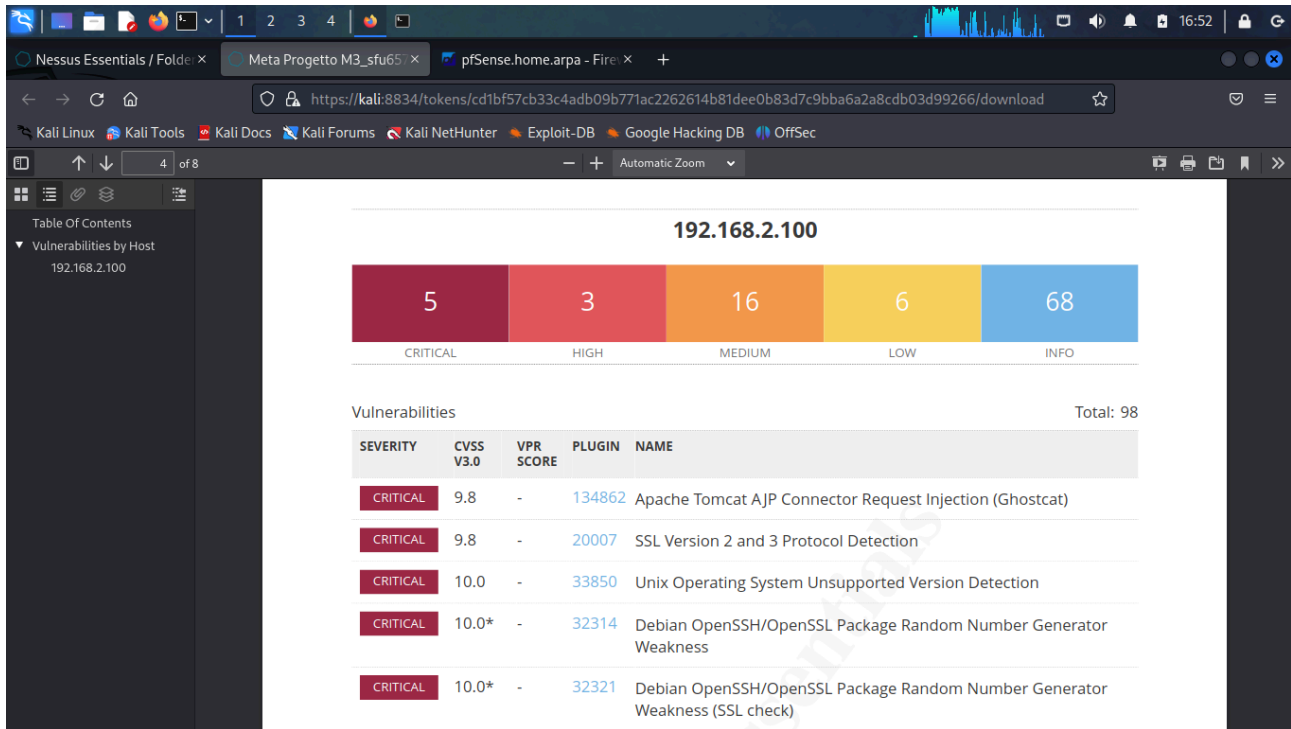
ciao123

[ Read 1 line ]
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text    ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page  ^U UnCut Text  ^T To Spell
```

Sono riuscito a mitigare poi la “**Bind Shell Backdoor Detection**” semplicemente attraverso una regola di firewall, impedendo alla macchina metasploitable di ricevere pacchetti TCP sulla porta 1524, in cui è attivo il demone collegato alla backdoor.



Una volta capito che la porta 1524 era associata alla shell in ascolto ho usato il comando “sudo fuser 1524/tcp” per ricevere in output il PID del processo associato al demone. Ho usato poi di conseguenza “ps aux | grep ‘PID’” per trovare il servizio xinetd. Sono sicuro che da qui in qualche modo si possa mitigare la vulnerabilità in maniera più efficace rispetto ad una regola di firewall. Sicuramente continuerò con la ricerca e approfondirò la questione.



Infine dopo aver fatto lo scan di nuovo con Nessus possiamo vedere che le vulnerabilità mitigate non sono più presenti.