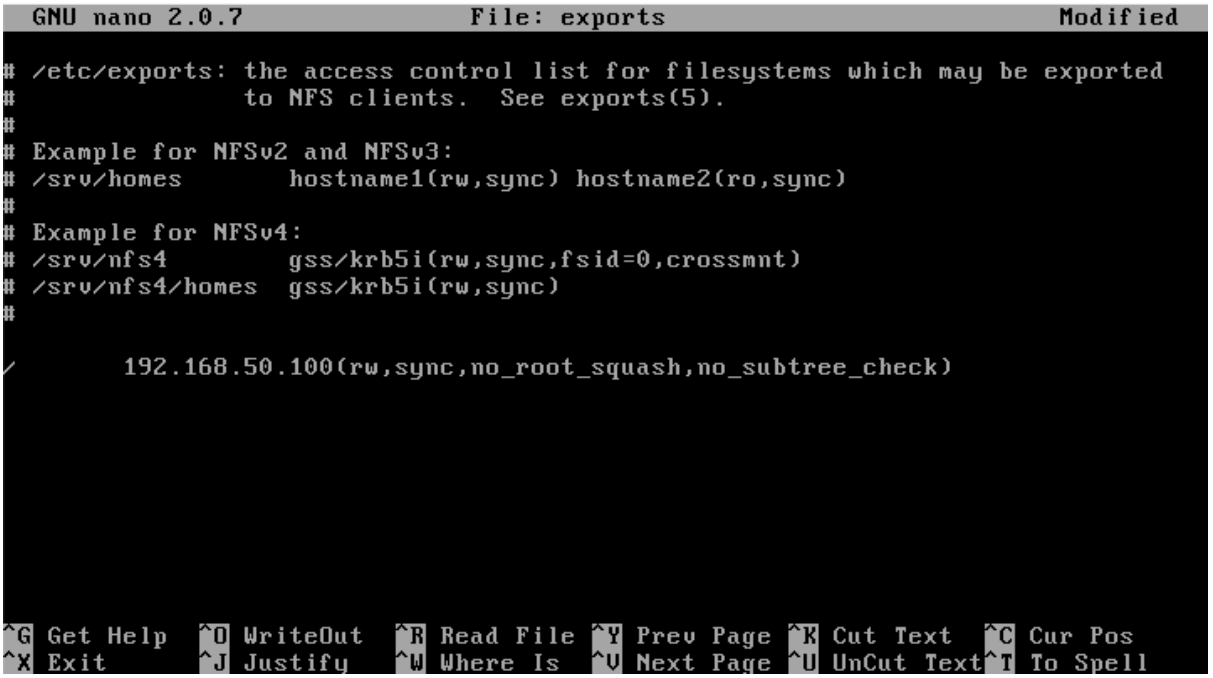
L'esercizio di oggi consisteva nel fare uno scan con Nessus a Metasploitable e risolvere alcune vulnerabilità a nostra scelta.
La prima cosa da fare è fare scan con Nessus a Metasploitable e dopo 20 minuti dovrebbe uscire una tabella (come questa ↓) dove viene indicata la vulnerabilità e la sua severità.

Vulnerabilities Total: 109

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.1	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
HIGH	7.5*	5.9	10205	rlogin Service Detection
HIGH	7.5*	5.9	10245	rsh Service Detection
MEDIUM	6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted

Di seguito le vulnerabilità che sono state scelte da risolvere per prima:
La prime due vulnerabilità è quella dell' NFS che consiste nel limitare NFS.

Questa vulnerabilità è stata risolta dopo aver configurato il file NFS come si vede qua https://www.html.it/pag/66986/configurare-nfs/ su Metasploitable sostituendo l'indirizzo IP al posto dell'asterisco, in modo che solo da Kali Linux sia possibile vedere e modificare il file (come questa ↓).



La terza vulnerabilità è la Backdoor:

CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection

Per risolvere questo problema era necessario andare su pfsense da kali linux e impostare una nuova condizione di firewall per far sì che la porta in ascolto rifiuti qualsiasi connessione verso di lei.

☐ ✖	0/0 B	IPv4 TCP	*	*	192.168.49.101	1524	*	none

In questa due foto sono le prove che la porta era aperta poi è intervenuto il firewall per bloccarla dall'ascolto.

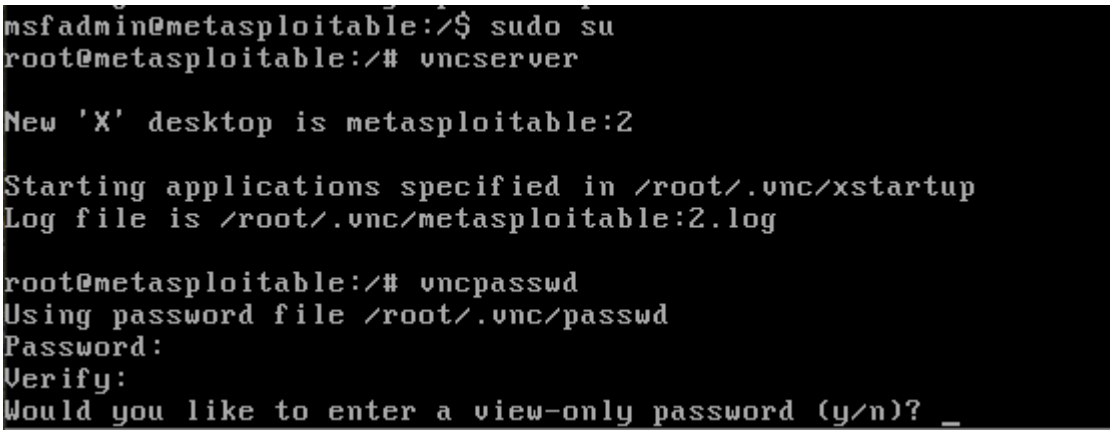
```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.49.101 1524
Trying 192.168.49.101 ...
Connected to 192.168.49.101.
Escape character is '^]'.
root@metasploitable:/# whoami
root
root@metasploitable:/# root@metasploitable:/# exit
exit
Connection closed by foreign host.
```

```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.49.101 1524
Trying 192.168.49.101 ...
```

La quarta Vulnerabilità:

CRITICAL	10.0*	-	61708	VNC Server 'password' Password

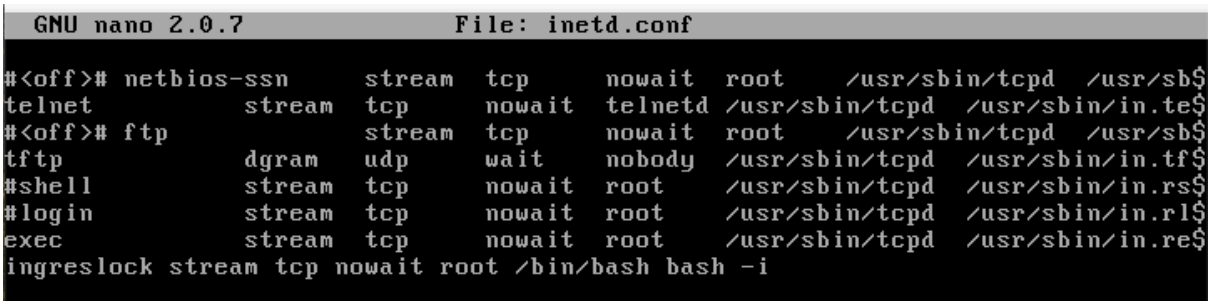
Per risolvere questo problema è necessario cambiare la password che in questo caso era da fare su Metasploitable che abbiao trovato su questo sito
https://linuxconfig.org/how-to-change-vnc-password-on-linux



Le ultime due vulnerabilita :

HIGH	7.5*	5.9	10205	rlogin Service Detection
HIGH	7.5*	5.9	10245	rsh Service Detection

In questo caso le ultime due vulnerabilità sono i service detection dove è stato necessario aprire il file inetd.conf su metasploitable e cambiare la riga del shell e la riga del login e mettere davanti a loro un # per farle diventare dei commenti così che la scansione non li legge e li ignora.



Dopo aver applicato le remediation proposte si noterà che il numero di vulnerabilità diminuisce il che sottolinea che le remediation erano corrette.

Vulnerabilities Total: 95

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.1	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
MEDIUM	6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	42263	Unencrypted Telnet Server
MEDIUM	5.9	4.4	136808	ISC BIND Denial of Service
MEDIUM	5.9	3.6	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	4.4	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)