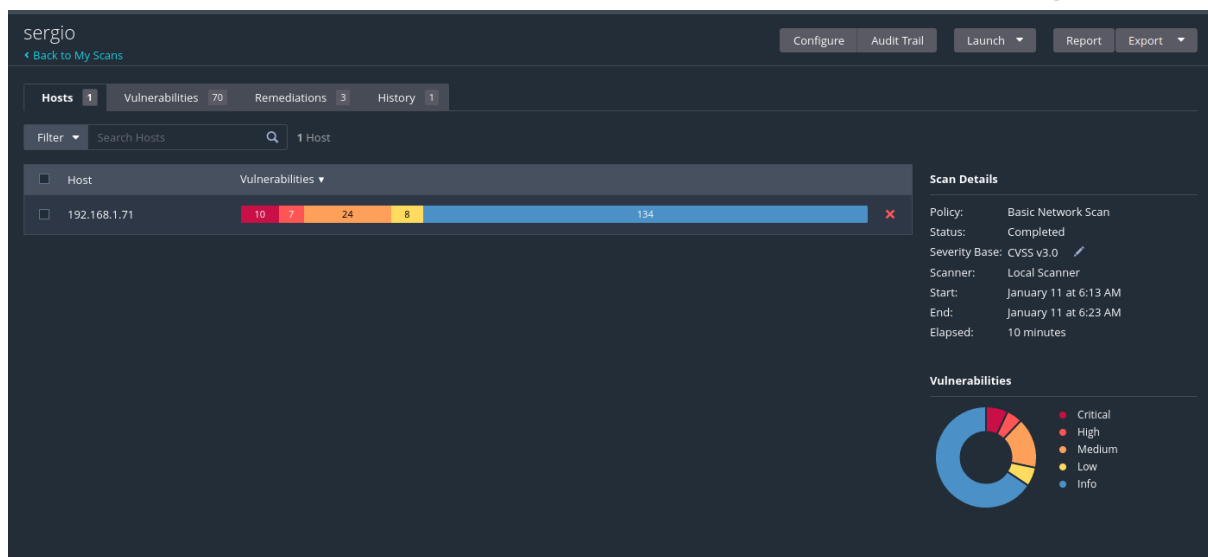


PROGETTO SETTIMANA 5

Nel progetto di oggi ci viene chiesto di effettuare una scansione sulla macchina metasploitable con il programma Nessus per verificare le vulnerabilità per poi andare a risolvere. Eseguita la scansione possiamo notare che la macchina metasploitable ha diverse vulnerabilità (anche troppe), ne abbiamo 10 **critiche** 7 **high** 24 **medie** 8 **basse** e 134 **info**. Come si può notare nell'immagine.



Come vulnerabilita ho scelto “ VNC Server ‘password’ Password, dalla descrizione di Nessus capiamo che la password del VNC è molto debole poiché la password attuale è “password”, quindi ho eseguito il comando `vncpasswd` per andare ad inserire una password più sicura, ho scelto una alfanumerica.

```
meta [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
Login with msfadmin/msfadmin to get started

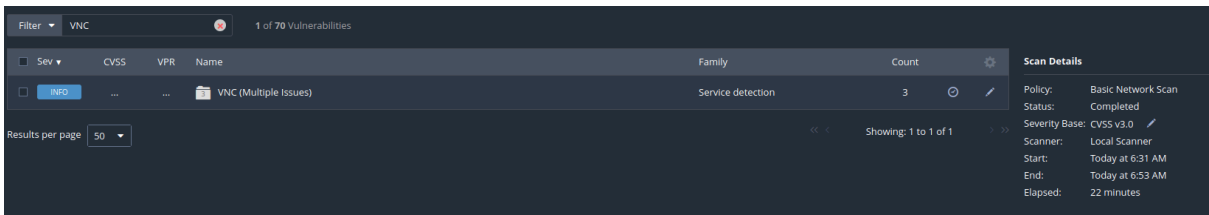
metasploitable login: msfadmin
Password:
Last login: Fri Jan 12 04:03:52 EST 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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.

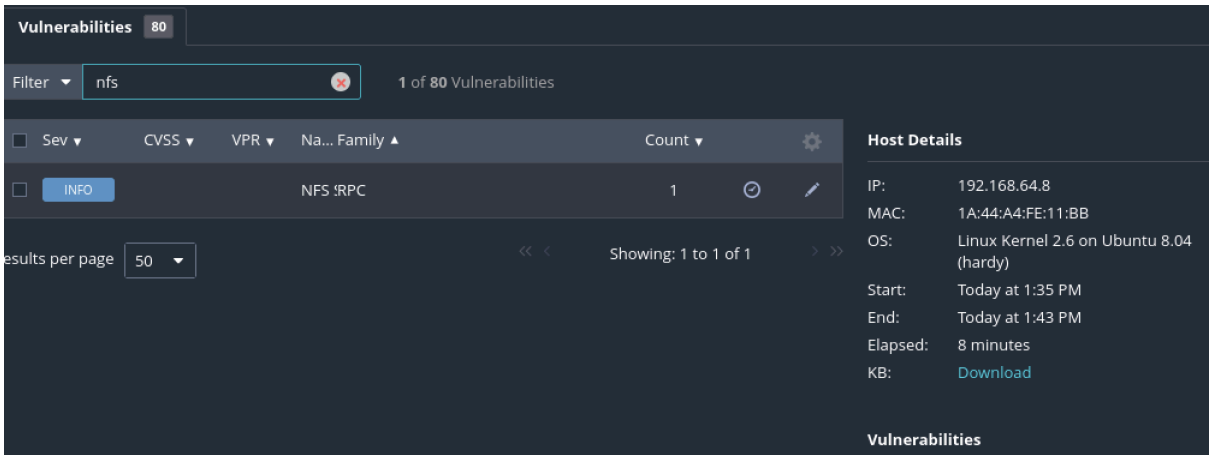
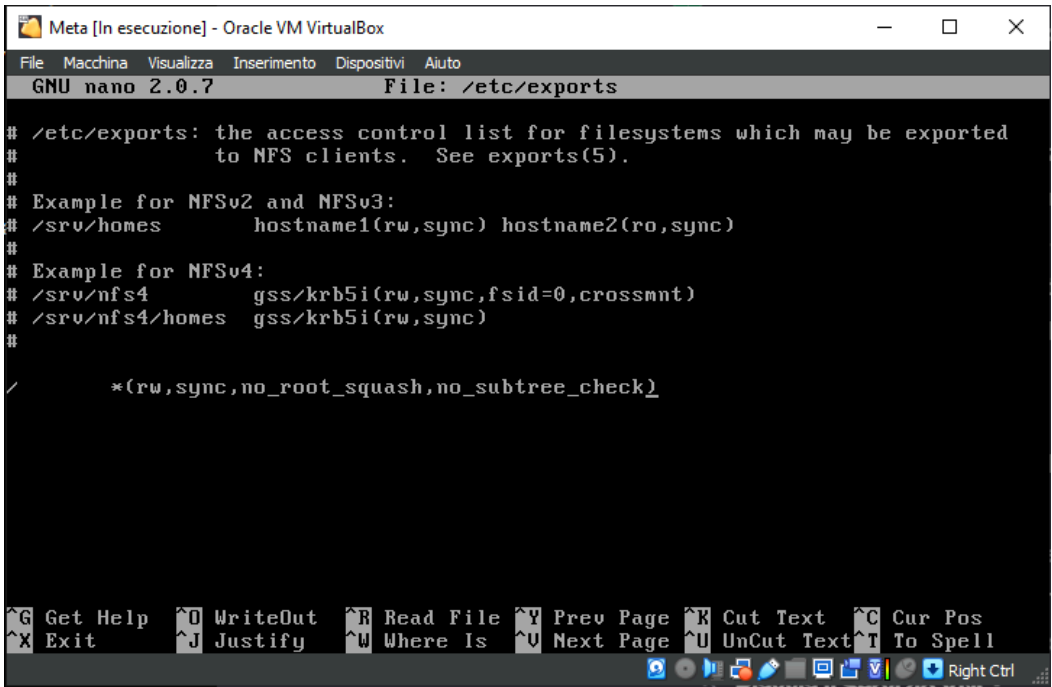
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

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:~$
```

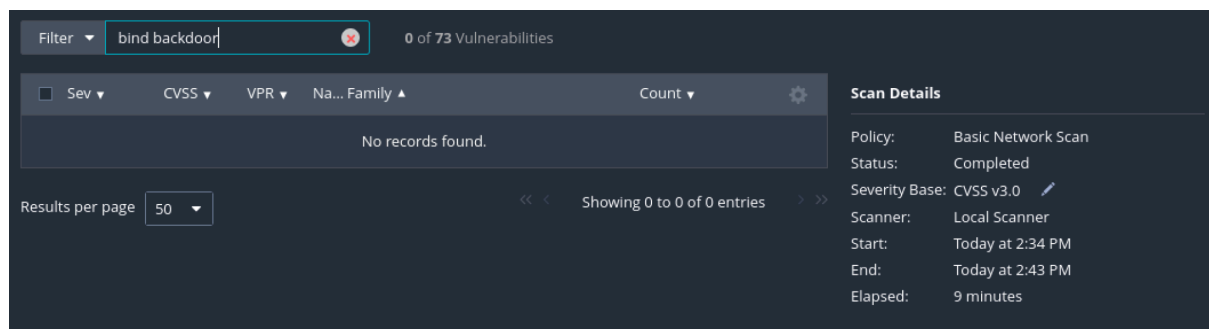
Come vediamo nella foto non si trova più nelle vulnerabilità.



Come seconda vulnerabilità da sistemare ho scelto “NFS Exported Share Information Disclosure” poiché le informazioni sono facilmente intercettabili da host non autorizzati che potrebbero leggere o scrivere sul nostro server da remoto. Per sistemare questa vulnerabilità sono entrato nella directory (/etc/exports) ed ho eliminato i permessi (ovvero l’ultima stringa).



Come terza vulnerabilità ho scelto “Bind Shell Backdoor Detection” ovvero che esiste una shell in ascolto su una porta remota che non ha bisogno di autenticazione, un criminale informatico potrebbe usarla per inviare comandi da remoto. Per risolverla ho utilizzato sia nmap che meta , nessus ci dice che la porta aperta è la numero 1524, quindi ho eliminato il processo da meta per riuscire ad eliminarlo ho individuato il processo tramite il comando `lsof -i :1524` , dopodichè l’ho eliminato con il comando `kill`, verificando la sua chiusura anche con nmap.



Infine abbiamo lo scan finale dove possiamo vedere che non ci sono più le tre vulnerabilità.

<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System U...	General	1	🕒	✎
<input type="checkbox"/>	CRITICAL	9.8		SSL Version 2 and 3 Prot...	Service detection	2	🕒	✎
<input type="checkbox"/>	CRITICAL	9.8	9.0	Apache Tomcat AJP Con...	Web Servers	1	🕒	✎
<input type="checkbox"/>	CRITICAL	📁 2 SSL (Multiple Issues)	Gain a shell remotely	3	🕒	✎
<input type="checkbox"/>	HIGH	7.5	6.7	Samba Badlock Vulnerab...	General	1	🕒	✎
<input type="checkbox"/>	MIXED	📁 15 SSL (Multiple Issues)	General	28	🕒	✎
<input type="checkbox"/>	MIXED	📁 5 ISC Bind (Multiple Is...	DNS	5	🕒	✎
<input type="checkbox"/>	MEDIUM	6.5		TLS Version 1.0 Protocol ...	Service detection	2	🕒	✎
<input type="checkbox"/>	MEDIUM	5.9	3.6	SSL Anonymous Cipher S...	Service detection	1	🕒	✎