

# AZIONI DI RIMEDIO ALLE VULNERABILITÀ CRITICHE SCELTE

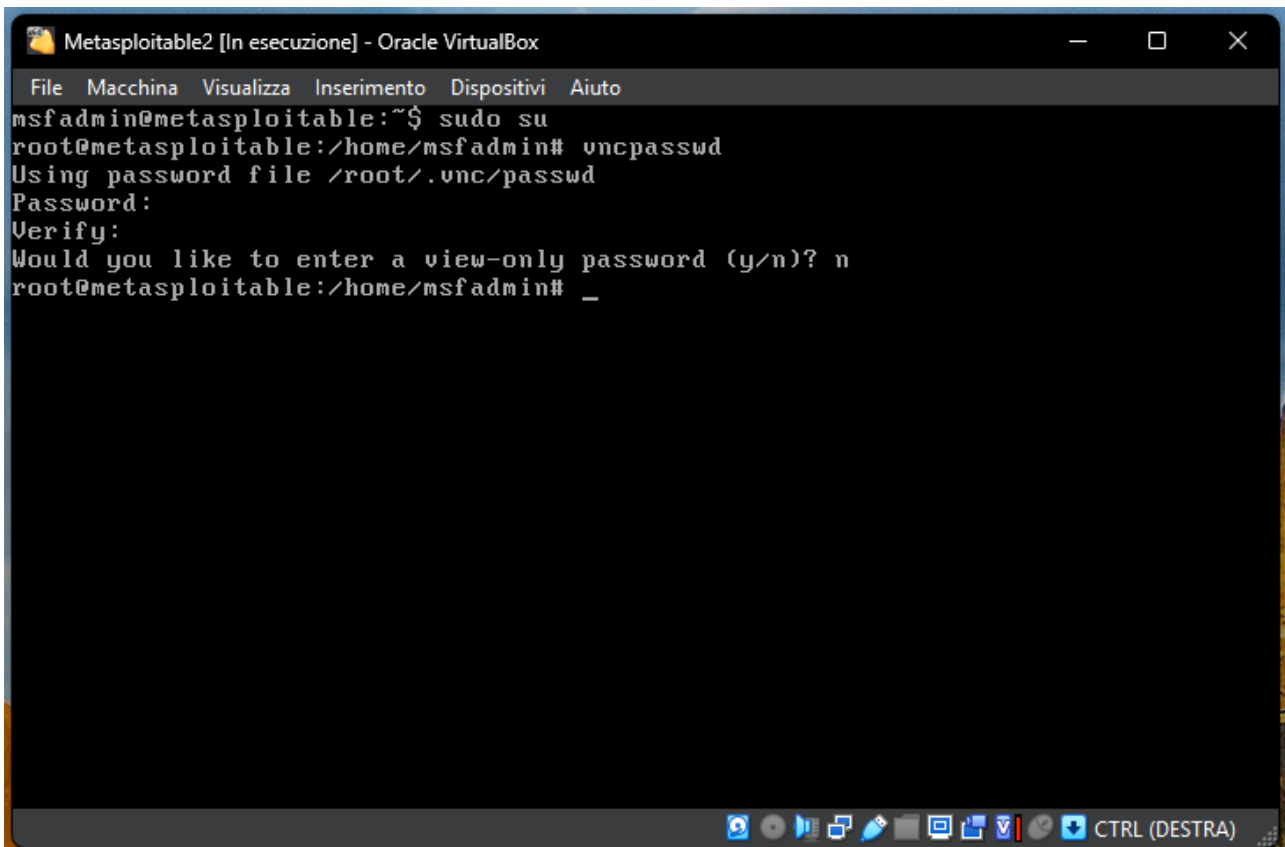
- **Prima vulnerabilità:**

CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password
----------	-------	---	---	-------	--------------------------------

- **Azione di rimedio:**

- Mi sono elevato ad utente di root per essere certo che le modifiche vengano apportate.
- Tramite il comando: “`vncpasswd`” ho cambiato la password preesistente (password) con una più sicura.

Screenshot:



```
Metasploitable2 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin# _
```

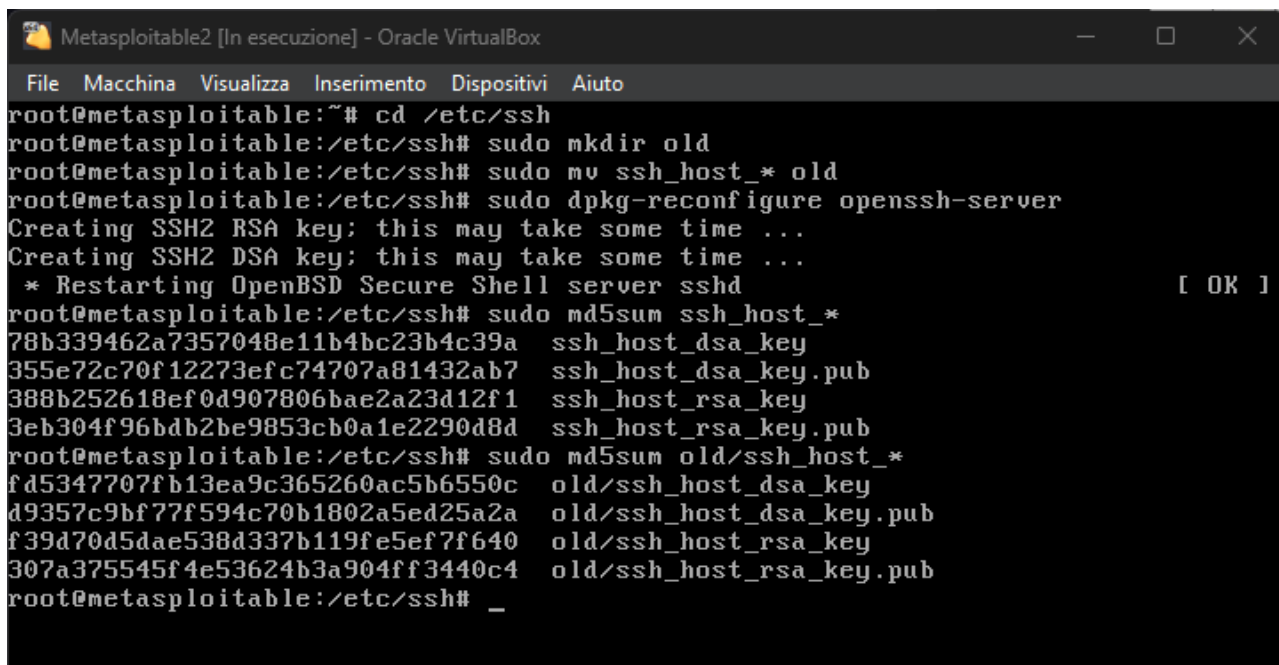
- **Seconda vulnerabilità:**

CRITICAL	10.0*	5.1	0.0165	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
----------	-------	-----	--------	-------	--

- **Azione di rimedio:**

- Per tentare di risolvere questa vulnerabilità con codice **32314**, che indica un problema nella generazione delle chiavi SSH ho provato a rigenerare le chiavi SSH.
- Quindi mi sono spostato nella cartella `ssh` tramite il comando: `cd /etc/ssh`.
- Ho creato una directory `old` tramite il comando: `mkdir old`.
- Dunque, ho spostato tutto quello che era presente nella cartella `ssh` nella cartella `old`, tra qui le chiavi, con il comando: `mv ssh_host_* old`.
- Infine, ho riconfigurato il server SSH per rigenerare le chiavi mancanti tramite il comando: `dpkg-reconfigure openssh-server`.

Screenshot:



```
Metasploitable2 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
root@metasploitable:~# cd /etc/ssh
root@metasploitable:/etc/ssh# sudo mkdir old
root@metasploitable:/etc/ssh# sudo mv ssh_host_* old
root@metasploitable:/etc/ssh# sudo dpkg-reconfigure openssh-server
Creating SSH2 RSA key; this may take some time ...
Creating SSH2 DSA key; this may take some time ...
* Restarting OpenBSD Secure Shell server sshd [ OK ]
root@metasploitable:/etc/ssh# sudo md5sum ssh_host_*
78b339462a7357048e11b4bc23b4c39a  ssh_host_dsa_key
355e72c70f12273efc74707a81432ab7  ssh_host_dsa_key.pub
388b252618ef0d907806bae2a23d12f1  ssh_host_rsa_key
3eb304f96bdb2be9853cb0a1e2290d8d  ssh_host_rsa_key.pub
root@metasploitable:/etc/ssh# sudo md5sum old/ssh_host_*
fd5347707fb13ea9c365260ac5b6550c  old/ssh_host_dsa_key
d9357c9bf77f594c70b1802a5ed25a2a  old/ssh_host_dsa_key.pub
f39d70d5dae538d337b119fe5ef7f640  old/ssh_host_rsa_key
307a375545f4e53624b3a904ff3440c4  old/ssh_host_rsa_key.pub
root@metasploitable:/etc/ssh# _
```

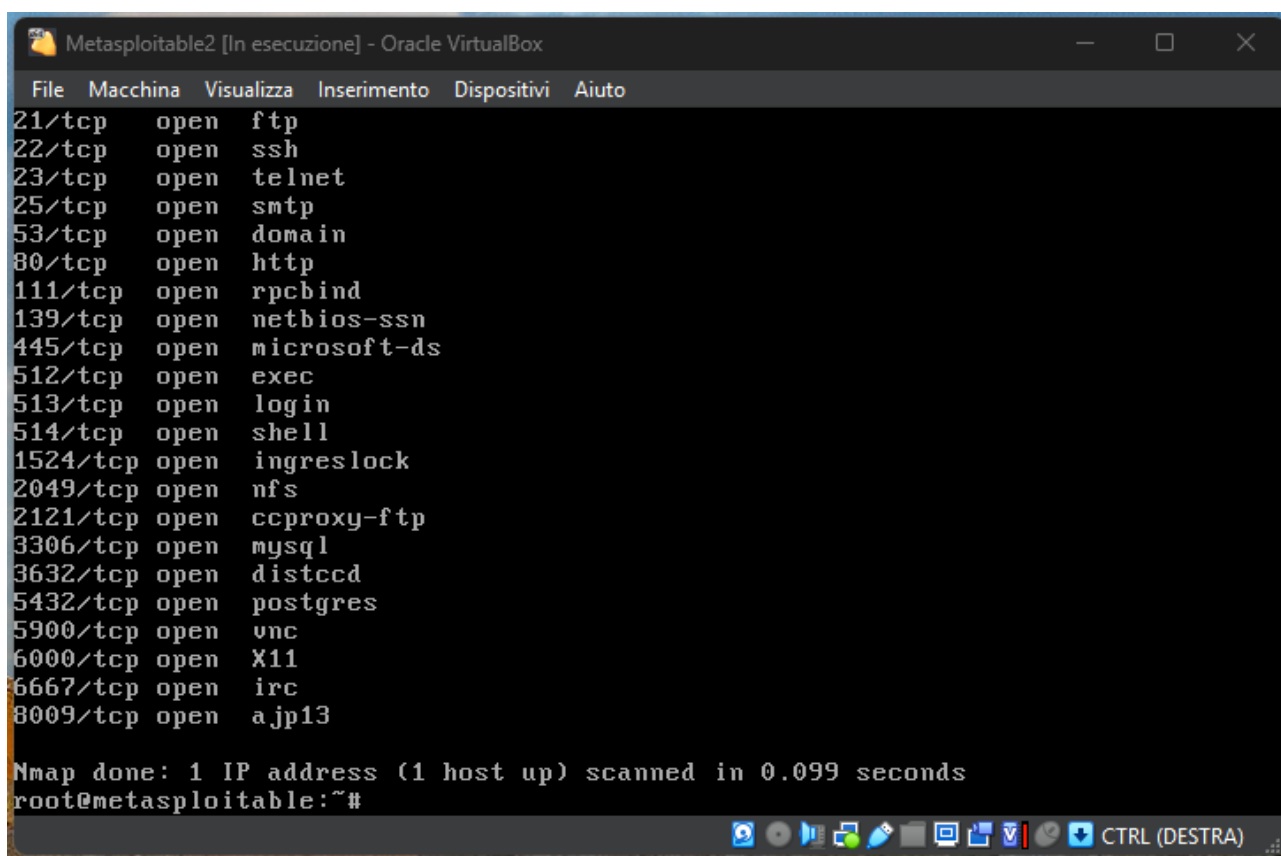
- Terza vulnerabilità:

CRITICAL	10.0*	7.4	0.6132	46882	UnrealIRCd Backdoor Detection
----------	-------	-----	--------	-------	-------------------------------

- Azione di rimedio:

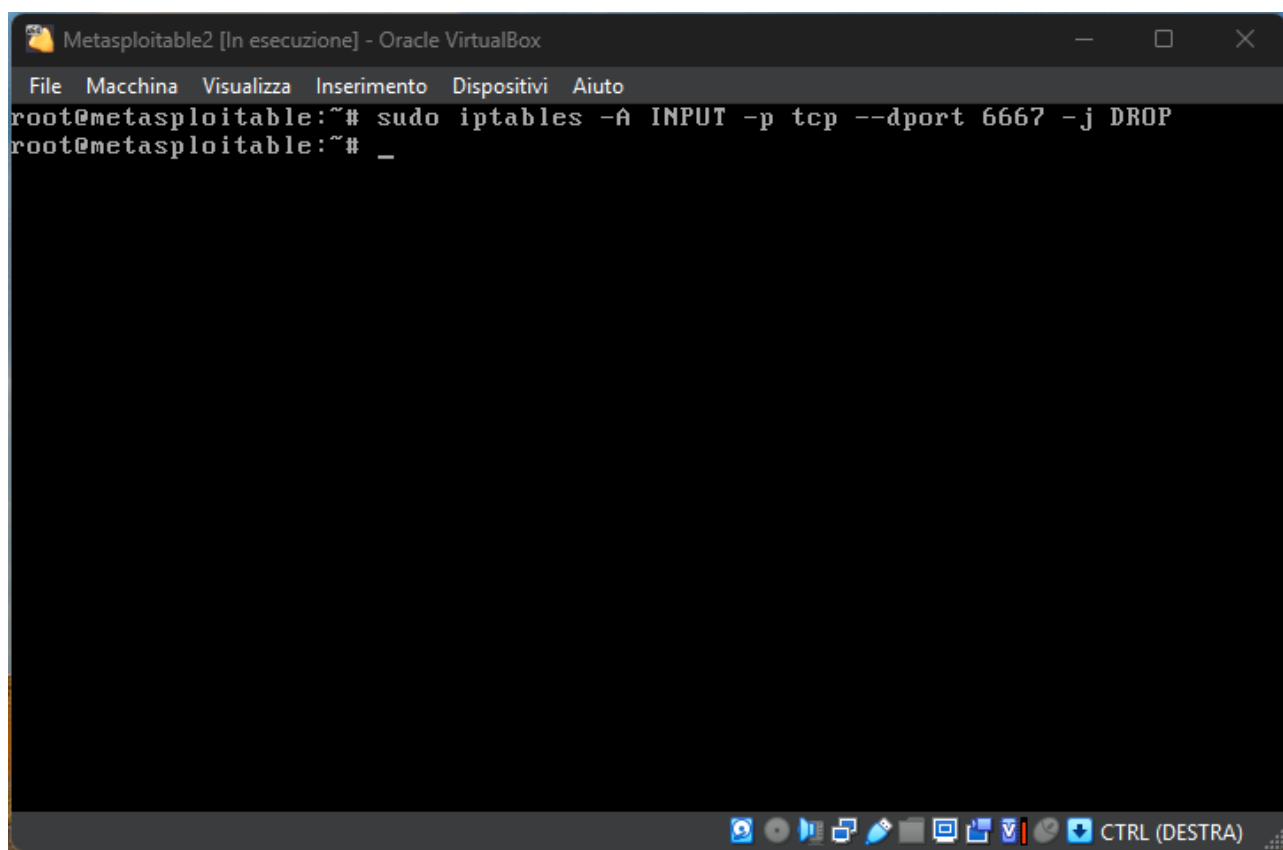
- Per risolvere questa vulnerabilità ho dovuto bloccare il traffico verso la porta 6667 con una regola firewall usando iptables.
- Quindi, ho usato il comando:  
“`iptables -A INPUT -p tcp -dport 6667 -j DROP`”.
- Dunque, ho verificato effettivamente che la porta 6667 fosse affetta dalla regola firewall impostata.

Screenshot:



```
Metasploitable2 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgres
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13

Nmap done: 1 IP address (1 host up) scanned in 0.099 seconds
root@metasploitable:~#
```



Metasploitable2 [In esecuzione] - Oracle VirtualBox

File	Macchina	Visualizza	Inserimento	Dispositivi	Aiuto
21/tcp	open		ftp		
22/tcp	open		ssh		
23/tcp	open		telnet		
25/tcp	open		smtp		
53/tcp	open		domain		
80/tcp	open		http		
111/tcp	open		rpcbind		
139/tcp	open		netbios-ssn		
445/tcp	open		microsoft-ds		
512/tcp	open		exec		
513/tcp	open		login		
514/tcp	open		shell		
1524/tcp	open		ingreslock		
2049/tcp	open		nfs		
2121/tcp	open		ccproxy-ftp		
3306/tcp	open		mysql		
3632/tcp	open		distccd		
5432/tcp	open		postgres		
5900/tcp	open		vnc		
6000/tcp	open		X11		
6667/tcp	filtered		irc		
8009/tcp	open		ajp13		

Nmap done: 1 IP address (1 host up) scanned in 1.387 seconds  
root@metasploitable:~# \_

CTRL (DESTRA)