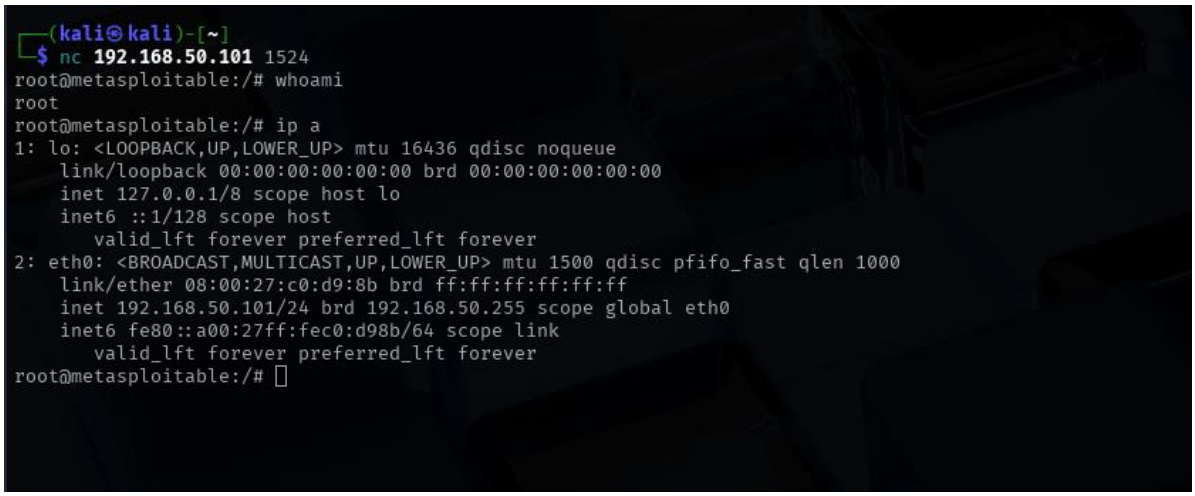
ESERCIZIO DI FINE MODULO M3- RemediatonMeta

Dall'analisi effettuata con Nessus andiamo ed intervenire sulla "**PRIMA"** vulnerabilità critica la **Bind Shell Backdoor Detection**

Avviamo Nmap da Kali e controlliamo eventuali porte aperte con il comando **nmap -Sv 192.168.50.101**

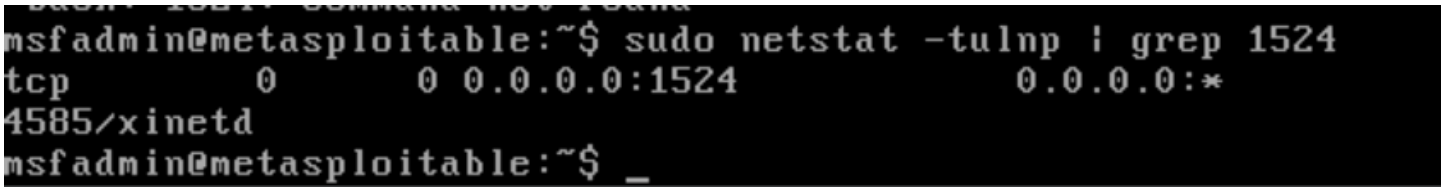
Dopo aver appurato che questa porta è aperta è questa vulnerabilità si può usare come backdoor, decidiamo di sfruttarla utilizzando il Netcat.

Con il comando **Netcat > nc 192.168.50.101 1524,** ci si connette a questa porta, ottenendo una shell. Successivamente inseriamo il comando **Whoami,** se la connessione alla **porta 1524** concede privilegi elevati, il risultato sarà **root**, il che significa pieno controllo del sistema. Adesso inseriamo un qualsiasi comando come **ip a**, ed il risultato sarà la configurazione di rete della Metasploitable, ciò significa che dal terminale di Kali stiamo eseguendo comandi sulla shell di Meta.



Adesso è arrivato il momento di intervenire con un'azione di rimedio ed eliminare questi privilegi non autorizzati.

Tramite shell di Meta eseguiamo questo comando **sudo nestat -tulnp | grep 1524** con questo comando vengono visualizzate le porte che stanno attualmente ascoltando in entrata e con **grep 1524** filtra l'output per mostrare solamente il contenuto che contiene **1524.** Questo comando è stato eseguito con i privilegi di amministratore in quanto senza non veniva visualizzato il PID ed il nome processo.



Per fermare questo processo utilizzeremo il comando **kill -p 4585** e successivamente **ufw deny 1524** per chiudere la porta.

Dopo aver eseguito tutti questi processi ri eseguo una scansione da Kali su meta per controllare che non ci sia più la porta aperta.

La **SECONDA** vulnerabilità critica trovata sempre con scansione Nessus è **VNC Server 'password' Password:** in pratica la password utilizzata è molto debole, per cui non si raggiungono gli standard di sicurezza desiderati. La soluzione di rimedio che andremo ad utilizzare è quella di aggiornare la password con una più forte. La nuova password utilizzata è: **Cat12.c**

```
msfadmin@metasploitable:~$ cd /.vnc/
-bash: cd: /.vnc/: No such file or directory
msfadmin@metasploitable:~$ ls -l
total 12
-rw-r--r-- 1 root     root       55 2025-01-26 14:47 pacchetto dati
-rw-r--r-- 1 msfadmin msfadmin   12 2025-01-26 13:41 PROVA PER COLLEGAMENTO
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
msfadmin@metasploitable:~$ cd /msfadmin/.vnc/
-bash: cd: /msfadmin/.vnc/: No such file or directory
msfadmin@metasploitable:~$ ls
pacchetto dati  PROVA PER COLLEGAMENTO  vulnerable
msfadmin@metasploitable:~$ ls -l
total 12
-rw-r--r-- 1 root     root       55 2025-01-26 14:47 pacchetto dati
-rw-r--r-- 1 msfadmin msfadmin   12 2025-01-26 13:41 PROVA PER COLLEGAMENTO
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
msfadmin@metasploitable:~$ cat msfadmin
cat: msfadmin: No such file or directory
msfadmin@metasploitable:~$ cd /home/msfadmin/.vnc/
msfadmin@metasploitable:~/.vnc$ ls
passwd
msfadmin@metasploitable:~/.vnc$ cat passwd
m♦♦♦♦♦#♦m♦♦♦♦♦#♦msfadmin@metasploitable:~/.vnc$ rm passwd
msfadmin@metasploitable:~/.vnc$ ls
msfadmin@metasploitable:~/.vnc$
```

Ora proseguiamo all'eliminizaione della **TERZA** vulnerabilità **Apache Tomcat SEoL (<=5x5.x)**

La soluzione di rimedio prevedeva l'aggiornamento di Apache Tomcat 5.5 ma non è disponibile su Metasploitable. Dopo vari tentativi e comandi e non potendo utilizzare più un azione di firewall, ho provveduto ad eliminare il servizio con il seguente comando **sudo apt-get remove tomcat5.5.**

Successivamente tramite Kali ho controllato che il servizio non era più in ascolto

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-18 08:41 EST
Nmap scan report for 192.168.50.101
Host is up (0.00036s latency).
Not shown: 979 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
MAC Address: 08:00:27:C0:D9:8B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:li

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.51 seconds

┌──(kali㉿kali)-[~]
└─$
```


Proseguo con la scansione Nessus finale per controllare se le azioni di rimedio siano andate a buon fine.