OffSec Nibbles room write up:

OffSec is the proud owner of Kali Linux and the OSCP program, as well as other Offensive Security education programs. At the time of this writing, I am actively working on obtaining my OSCP certification. This is a great Linux box to study on for the OSCP.

Enumeration:

Target IP 192.168.51.47 (Note subject for change, this is the IP address I got while doing this lab.

Port 21 is open, FTP can be accessed.

Port 22 is open, SSH.

Port 80, HTTP server

And port 5437 is open, PostgreSQL

Test that first and found PostgreSQL user name:

postgres

Password:

postgres

Remedy right away, default passwords.

Ports are closed 139 and 445:

No smb or rpc.

```
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
139/tcp  closed netbios-ssn
445/tcp  closed microsoft-ds
5437/tcp open   pmip6-data
```

Foothold will be ported to 5437 to gain access to the box. The version is 17.4-1:

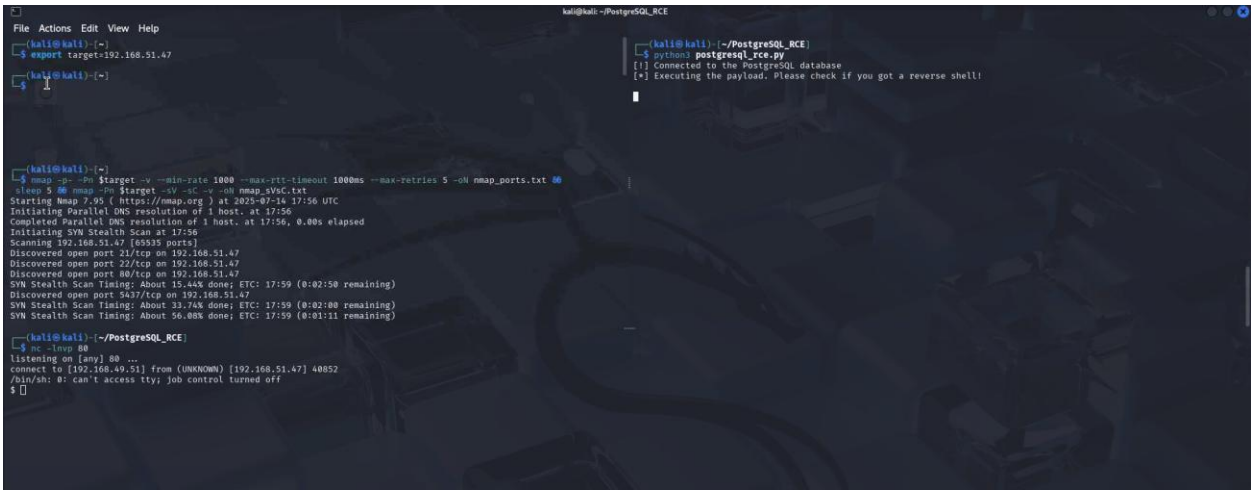
```
┌──(kali㉿kali)-[~]
└─$ psql -h $target -p 5437 -U postgres
Password for user postgres:
psql (17.4 (Debian 17.4-1), server 11.7 (Debian 11.7-0+deb10u1))
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, compression: off, ALPN: none)
Type "help" for help.

postgres=# exit
```

Since the default creds are the same, we can RCE into the machine:

https://github.com/squid22/PostgreSQL_RCE - This is probably the better one to use to access the pc. Since port 80 is open we can use that to connect to the pc.

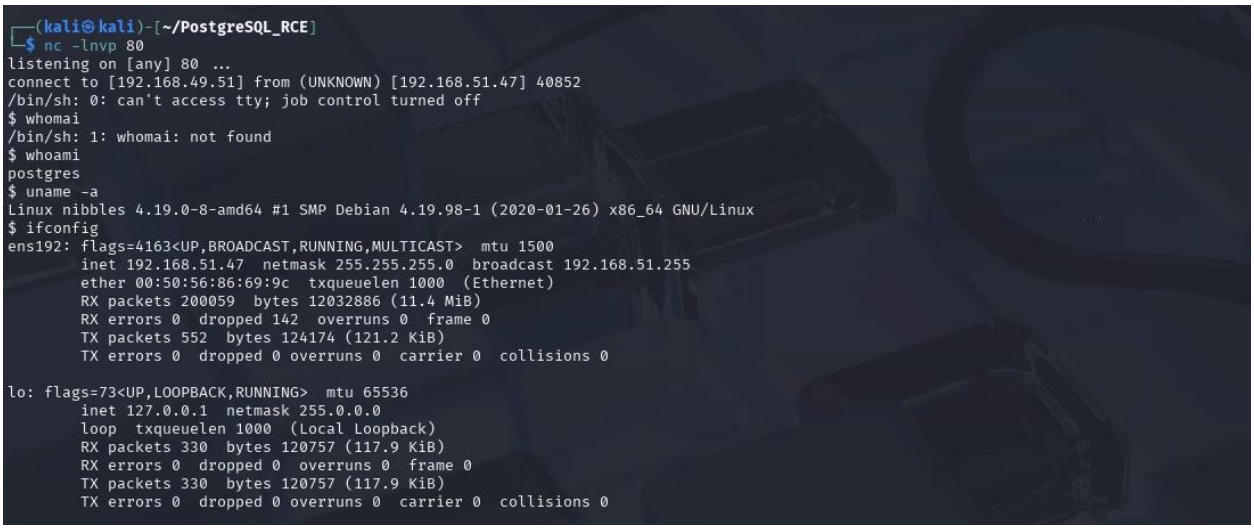
Before try the remote code here:

Evaluating the structure of the shell, and ip address:

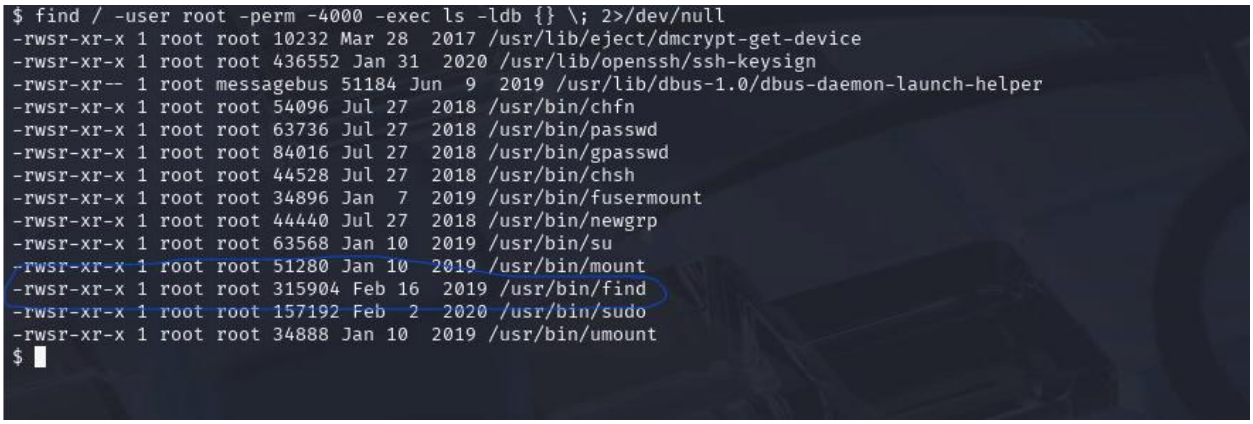


Gained shell.

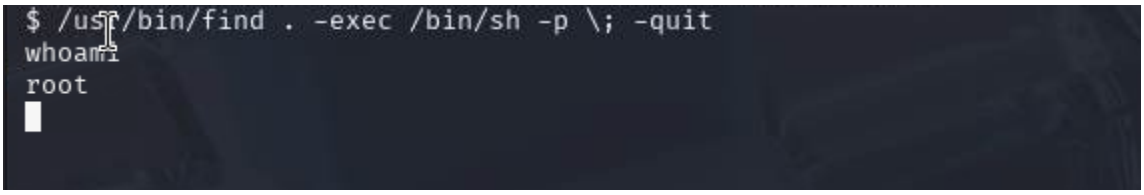
Enumerating user and access:



Privilege escalation:



Ticket for the admin/root access. No need to run linPEAS since we can find the SUID no problem:



Gained access without issues after stopping the service.

Flags: