Vulnerable\_MongoDB

Docker setup

1. Pull the docker image from docker-hub

docker pull shaccuri/vulnerablemongo

2. Add network or use host network in the following command

docker network create mongonet

3. Run the docker image using the following command

docker run -d -p 27017:27017 -name mongodb -net mongonet shaccuri/vulnerablemongo

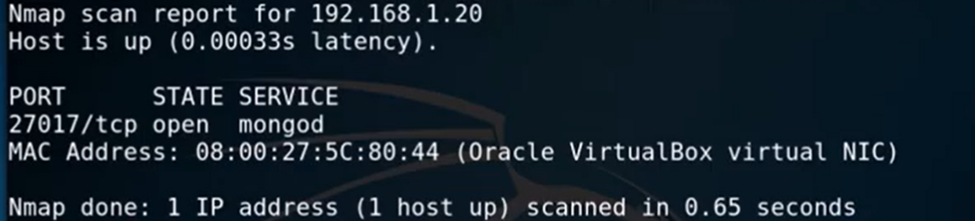
4. Get the IP address to perform vulnerability testing

Ip a

Penetration testing Guide

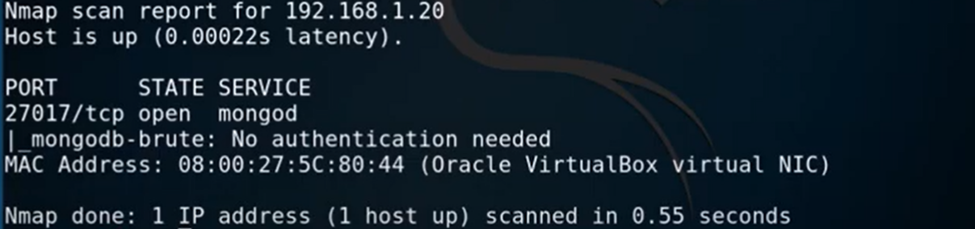
1. We have the IP address of the server, let’s perform the Nmap scan.

nmap -sC -sV ip\_address



2. Identified the mongodb service now run mongodb script

Nmap -p 27017 ip\_address - - script mongodb-brute



3. Since there is no authentication required. You can log in to the database using mongo client.