ANONYMOUS\_SMB

Docker setup

1. First check docker installed by checking the docker version

docker –version

2. Pull the docker image from docker-hub

docker pull shaccuri/anonymous\_smb

3. Run the docker image using the following command

docker run –name -it -d -p 445:445 anonymous\_smb

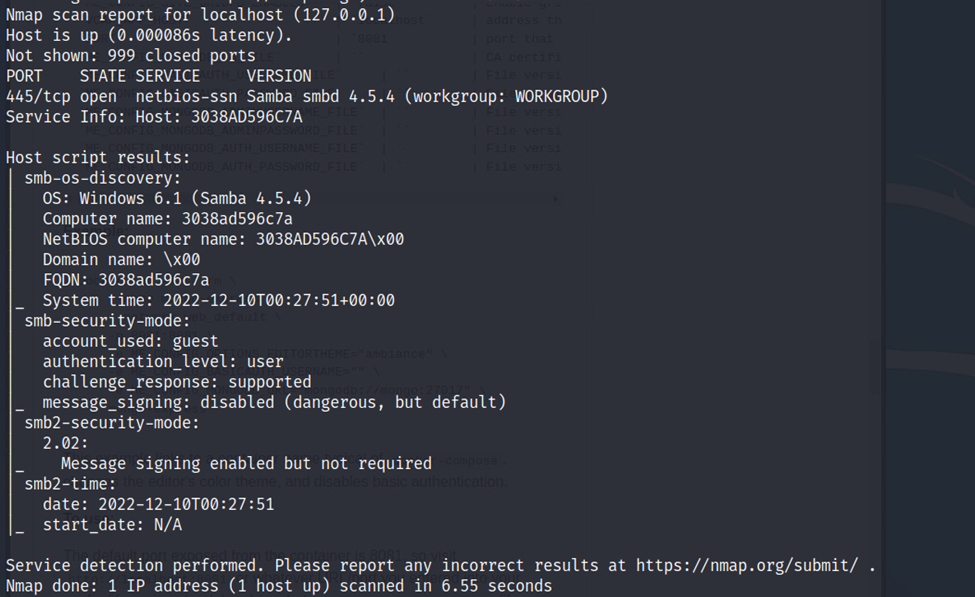
4. Get the IP address to perform vulnerability testing

Ip a

Penetration testing Guide

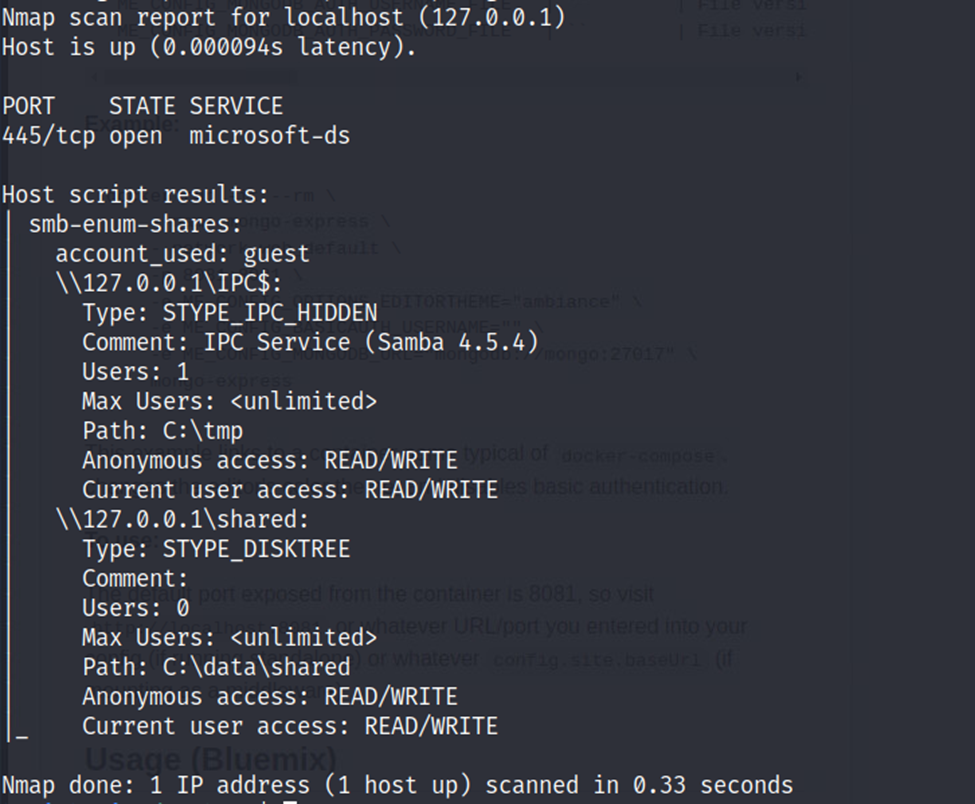
1. We have the IP address of the server, let’s perform the Nmap scan.

nmap -sC -sV ip\_address



2. We were able to identify port 445 is open and SMB is running there. We also found the version of smb. We will perform an enumeration to find out more about the shares.

Nmap -p 445 –script smb-enum-shares ip\_address



3. We can identify that there is one share that has anonymous login named shared. We will now attempt to log in as an anonymous user: password.

smbclient //server/share

4. We are successfully able to access the anonymous share. It has read-write permission so we will check that.

mkdir hello