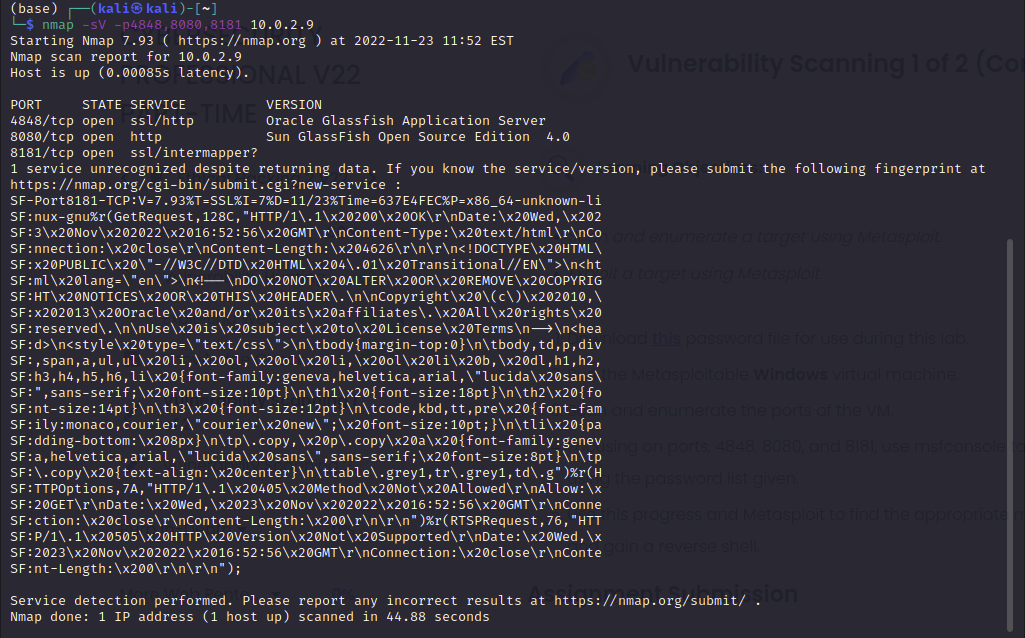
Vulnerability Scan 1

This document contains several screen shots showing the vulnerability scan of the glassfish server and the exploitation to obtain the reverse shell.

The first thing I did was run ifconfig on my host machine to determine the IP of my host machine. I then ran an nmap scan of my network to locate my target machine. My target machine is located at 10.0.2.9. From here I used various tools to see what I can find out about the target machine.



Nmap scan showing services on each port. The ports are running Glassfish. Since port 8181 came back with minimal information I ran a Rustscan to see if I could get additional information.

Text

Description automatically generated

Rustscan provided a little more information on the ports. All three ports are running Oracle GlassFish version 4.0 and Java is of particular importance for our future exploit. Port 4848 is running ssl/http. Port 8080 is running http and port 8181 is running ssl/http.

Graphical user interface, text, email

Description automatically generated

Screen shot of some information I found through searching the internet as it pertains to Glassfish vulnerabilities.

Text

Description automatically generated

Metasploit scanner to brute force the password of the Glassfish server. I used the auxiliary/scanner/http/glassfish\_login module brute force the password.

Text

Description automatically generated

Setting the password file location in Metasploit so that the webserver can be exploited.

Text

Description automatically generated

Final preparation before the brute force attack is attempted.

Text

Description automatically generated

Scanner starting to brute force the password.

Text

Description automatically generated

Successful completion of the scanner. The password for the webserver is ‘sploit’.

Graphical user interface, text, application

Description automatically generated

Logging into the webserver with the username ‘admin’ and password ‘sploit’.

Graphical user interface, text, application, email

Description automatically generated

Webserver access where I was able to look around and see what I could potentially exploit.

Text

Description automatically generated

Preparation to obtain the reverse shell. I used the exploit/multi/http/glassfish\_deployer to obtain a reverse shell of the target.

Text

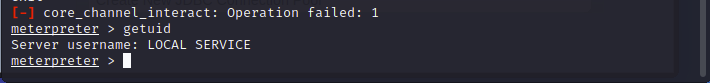
Description automatically generated

Setting the various setting as needed to exploit the target and obtain the reverse shell.

Text

Description automatically generated

Reverse shell successfully obtained.



Local service is the access level obtained.

Text

Description automatically generated

My name echoed on the target machine.