**Enumeration**

Nmap scan results

Text

Description automatically generated

Open Ports

Port 22 SSH

Port 8080 Apache tomcat 9.0.38

Dirsearch results

Text

Description automatically generated

**Foothold**

Graphical user interface, application, chat or text message, website

Description automatically generated

Yaml has known vulnerabilities.

I used a payload from github

<https://github.com/artsploit/yaml-payload>

create a shell in /yaml-payload. I saved mine as hack.sh

Text

Description automatically generated with medium confidence

Edit AwesomeScriptEngineFactory.java in /src/artsploit. Add your ip address and the reverse shell name and where it will get saved to on the machine. The tmp folder

Text

Description automatically generated

Change back to yaml payload folder and run

javac src/artsploit/AwesomeScriptEngineFactory.java

jar -cvf yaml-payload.jar -C src/ .

Start a python3 http server using. Python3 -m http.server 80 && start nc -nvlp I used port 2121

Put the following payload in the yaml parser

Text

Description automatically generated

Should get shell on nc listener

Text

Description automatically generated

Looking around in tomcat we find a users file.

/opt/tomcat/conf/tomcat-users.xml

And we find <user username="admin" password="whythereisalimit" roles="manager-gui,admin-gui"/>

admin:whythereisalimit

Now we can ssh into the machine.

Get user.txt

**Privilege Escalate**

Sudo -l shows. (ALL) NOPASSWD: /usr/bin/go run /opt/wasm-functions/index.go

Cat out index.go

Text

Description automatically generated

And we can see that the file is not using absolute paths for deploy.sh or main.wasm.

Move index.go to /tmp

The files will be unable to be deployed we will need to change it over to a wat file edit the const to 1.

Then change it back to a wasm file, before uploading back to the remote host.

Once this is done we can create our own deploy.sh. Adding in our ssh rsa token.

Then rerun sudo /usr/bin/go run /opt/wasm-functions/index.go

Should say ready to deploy

ssh -i authorized\_keys root@10.10.10.227

Root is now mine!

Text

Description automatically generated

<https://app.hackthebox.eu/profile/280458>

Goodluck!!