HACKTHEBOX

Hack The Box - Writeup

Machine: Bolt

Author: c1sc0

Date: October 3, 2021

c1sc0 Guru

Rank: 416 398 ★ 22

hackthebox.eu

Contents

1 Overview

Name	IP	Difficulty
Bolt	10.10.11.114	Medium

2 Recon

Nmap scan shows three open ports which are:

Port	Service
22	SSH
80	HTTP
443	HTTPS

Table 2.1: Nmap results

2.1 Website port 80

This site will let you download a docker image “image.tar” which you can load via docker load -i image.tar. Once imported you can launch that image with interactive shell.

You can find the source of a python flask app in this container. If you run the app with flask and expose it to your attacker box you will be presented with a login page of “AdminLTE Flask”.

There are exploits for this software (also used by PiHole) but right now this looks like it cannot be used to do something

Login can be retrieved from the docker image and is admin:deabolt.

The comment section will tell us a few things about security concerns with the image and that there has to be a mail system somewhere.

2.2 other vhosts

Wfuzz will tell us there is also “mail” and “demo” as a vhost. Demo does not give us anything this moment and mail is a roundcube instance.

3 Foothold

4 Privilege Escalation

Thanks for reading...

c1sc0