
ATTACK
DEFENSE
by PentesterAcademy

Name	Compromised Developer Machine I
URL	https://www.attackdefense.com/challengedetails?cid=1040
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/project-code/

```
root@attackdefense:~#
root@attackdefense:~# cd projects/root/project-code/
root@attackdefense:~/projects/root/project-code# ls -l
total 108
-rw-r--r-- 1 root root    16 May 16 16:59 README.md
drwxr-xr-x 2 root root  4096 May 16 16:59 files
-rw-r--r-- 1 root root 40563 May 16 16:59 functions.php
-rw-r--r-- 1 root root 57739 May 16 16:59 index.php
root@attackdefense:~/projects/root/project-code#
root@attackdefense:~/projects/root/project-code#
root@attackdefense:~/projects/root/project-code# cd ~
root@attackdefense:~#
```

Step 2: If we check .ssh/config file, we will find useful information about the user. The user is using id_rsa.gitlab key to authenticate to gitlab host.

Command: cat .ssh/config

```
root@attackdefense:~# cat .ssh/config
Host gitlab
    Hostname gitlab
    IdentityFile ~/.ssh/id_rsa.gitlab
    IdentitiesOnly yes
root@attackdefense:~#
```

The key is not in .ssh directory. We have to find it and move it to .ssh directory.

Commands:
find / -name id_rsa.gitlab 2>/dev/null
cp /var/opt/id_rsa.gitlab .ssh/

```
root@attackdefense:~#
root@attackdefense:~# find / -name id_rsa.gitlab 2>/dev/null
/var/opt/id_rsa.gitlab
^C
root@attackdefense:~# cp /var/opt/id_rsa.gitlab .ssh/
root@attackdefense:~#
```

Step 3: We can delete the existing directory and clone a new copy of the same project from remote server using the SSH key.

Command: git clone git@gitlab:root/project-code.git

```
root@attackdefense:~#
root@attackdefense:~# git clone git@gitlab:root/project-code.git
Cloning into 'project-code'...
The authenticity of host 'gitlab (192.5.174.3)' can't be established.
ECDSA key fingerprint is SHA256:cHQO1keq/jr/nQh58gC9cll/Y/NAd+eE9esaZyjVaMg.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'gitlab,192.5.174.3' (ECDSA) to the list of known hosts.
remote: Enumerating objects: 11, done.
remote: Counting objects: 100% (11/11), done.
remote: Compressing objects: 100% (8/8), done.
remote: Total 11 (delta 0), reused 0 (delta 0)
Receiving objects: 100% (11/11), 33.21 KiB | 11.07 MiB/s, done.
root@attackdefense:~#
```

Step 4: We can find flag.txt file in the newly cloned directory which contains the flag.

Commands:
ls -l project-code
cat project-code/flag.txt

Flag: f9a1e58bde48c2b79c712dc4208a3630

References:

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