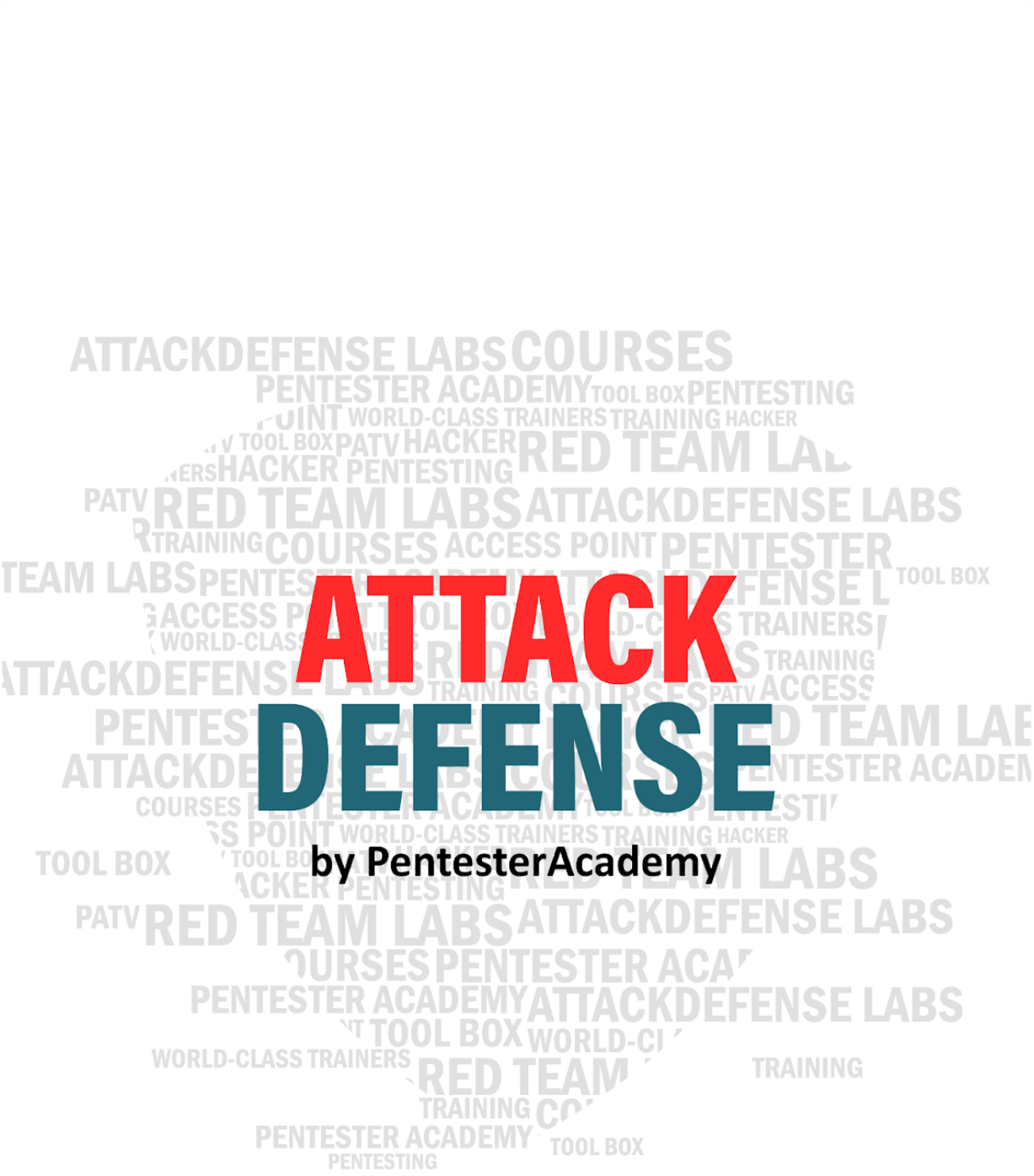
ATTACK
DEFENSE
by PentesterAcademy

Name	Talisman: Pre-Commit Code Scanning
URL	https://www.attackdefense.com/challengedetails?cid=2046
Type	DevOps Basics: Sensitive Information Scan

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. Also, note that the IP addresses and domain names might be different in your lab.

Challenge Description

Talisman is a tool to scan code changes for sensitive information (SSH keys, AWS tokens) before pushing it to a Git repository. It is triggered by pre-commit hooks..

A Kali CLI machine (kali-cli) is provided to the user with Talisman installed on it. The source code for three sample web applications is provided in the home directory of the root user.

Objective: Commit the Source code in the local repository and analyse the talisman report.

Instructions:

- The source code of web applications is provided at /root/github-repos

Solution

Step 1: Check the provided web applications.

Command: ls -l github-repos

```
root@attackdefense:~# ls -l github-repos/
total 8
drwxr-xr-x 4 root root 4096 Sep 17 15:48 flask-recipes
drwxr-xr-x 8 root root 4096 Sep 17 16:14 sqlitedborm
root@attackdefense:~#
```

Step 2: Add the git configuration in order to add and commit repositories locally.

Commands:
git config --global user.name "root"
git config --global user.email root@server.xyz

```
root@attackdefense:~#
root@attackdefense:~# git config --global user.name "root"
root@attackdefense:~# git config --global user.email root@server.xyz
root@attackdefense:~#
```

We will take one example at a time and run the tool on that.

Example 1: flask-recipes

Step A: Change to the flask-recipes directory.

Commands:
cd ~/github-repos/flask-recipes
ls -lah

```
root@attackdefense:~/github-repos/flask-recipes# ls -lah
total 48K
drwxr-xr-x 4 root root 4.0K Sep 17 15:48 .
drwxr-xr-x 4 root root 4.0K Sep 17 16:28 ..
drwxr-xr-x 5 root root 4.0K Sep 17 16:24 app
-rw-r--r-- 1 root root 1.7K Sep 17 15:48 db_manage.py
-rw-r--r-- 1 root root  214 Sep 17 15:48 download-recipes.sh
drwxrwxr-x 8 root root 4.0K Sep 17 16:25 .git
-rw-r--r-- 1 root root  534 Sep 17 15:48 import_recipes.py
-rw-r--r-- 1 root root 1.1K Sep 17 15:48 LICENSE
-rw-r--r-- 1 root root   26 Sep 17 15:48 Procfile
-rw-r--r-- 1 root root  594 Sep 17 15:48 README.md
-rw-r--r-- 1 root root  303 Sep 17 15:48 requirements.txt
-rw-r--r-- 1 root root  111 Sep 17 15:48 run.py
root@attackdefense:~/github-repos/flask-recipes#
```

Step B: Create a local git commit into the repository to trigger the talisman pre-commit hook. Pre-commit hook gets triggered whenever the developer makes a commit into the repository.

Command: git add . && git commit -m "ADD files"

```
root@attackdefense:~/github-repos/flask-recipes# git add . && git commit -m "ADD files"
Failed to retrieve latest version, skipping update.

Talisman Report:
+-----------------+-----------------------------------------------------+----------+
|      FILE       |                       ERRORS                        | SEVERITY |
+-----------------+-----------------------------------------------------+----------+
| app/database.db | Expected file to not to contain                     | medium   |
|                 | hex encoded texts such as:                          |          |
|                 | ('openbmp','*DEA173C85CAA046B885A36D702D38A6459... |          |
+-----------------+-----------------------------------------------------+----------+
| app/database.db | Potential secret pattern : /*!40014 SET             | medium   |
|                 | @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS        |          |
+-----------------+-----------------------------------------------------+----------+
| app/database.db | Potential secret pattern : /*!40014 SET             | medium   |
|                 | FOREIGN_KEY_CHECKS=@OLD_FOREIGN_KEY_CHECKS          |          |
|                 | */                                                  |          |
+-----------------+-----------------------------------------------------+----------+


If you are absolutely sure that you want to ignore the above files from talisman detectors, consider pasting the following f
ormat in .talismanrc file in the project root

fileignoreconfig:
- filename: app/database.db
  checksum: 7c22ac5f66f01c3ff2026ce79e8228137cfe15e88f4f3d8399f2ceccce31360d
```

Issues Detected

- Database.db contains encoded texts which could be password hashes
- Database.db contains a secret pattern which is detected by talisman.

Example 2: sqlitedborm

Step A: Change to the sqlitedborm directory.

Command:
cd ~/github-repos/sqlitedborm
ls -lah

```
root@attackdefense:~/github-repos/sqlitedborm# ls -lah
total 76K
drwxr-xr-x 8 root root 4.0K Sep 17 16:14 .
drwxr-xr-x 1 root root 4.0K Sep 17 16:28 ..
drwxr-xr-x 3 root root 4.0K Sep 17 15:48 build
-rw-r--r-- 1 root root  103 Sep 17 15:48 build.ps1
drwxr-xr-x 2 root root 4.0K Sep 17 16:14 dist
drwxrwxr-x 8 root root 4.0K Sep 17 16:25 .git
-rw-r--r-- 1 root root   65 Sep 17 15:48 install.ps1
-rw-r--r-- 1 root root 1.1K Sep 17 15:48 LICENSE
-rw-r--r-- 1 root root 5.1K Sep 17 15:48 main.py
-rw-r--r-- 1 root root 1.6K Sep 17 15:48 README.md
-rw-r--r-- 1 root root  809 Sep 17 15:48 setup.py
drwxr-xr-x 3 root root 4.0K Sep 17 16:14 sqlitedborm
drwxr-xr-x 2 root root 4.0K Sep 17 15:48 sqlitedborm.egg-info
drwxr-xr-x 2 root root 4.0K Sep 17 15:48 sqliteormsch.egg-info
-rw-r--r-- 1 root root  12K Sep 17 15:48 testdata.sqlite3
root@attackdefense:~/github-repos/sqlitedborm#
```

Step B: Create a local git commit into the repository to trigger the talisman pre-commit hook.

Command: git add . && git commit -m "ADD files"

```
root@attackdefense:~/github-repos/sqlitedborm# git add . && git commit -m "ADD files"
Failed to retrieve latest version, skipping update.

Talisman Report:
+------------------------+-----------------------------------------------------+----------+
|          FILE          |                       ERRORS                        | SEVERITY |
+------------------------+-----------------------------------------------------+----------+
| dist/id_rsa            | The file name "dist/id_rsa"                         | low      |
|                        | failed checks against the                           |          |
|                        | pattern ^.+_rsa$                                    |          |
+------------------------+-----------------------------------------------------+----------+
| dist/id_rsa            | Expected file to not to contain                     | medium   |
|                        | base64 encoded texts such as:                       |          |
|                        | NhAAAAAwEAAQAAAYEApvr8Xq14mIsegb0IyRWXKlR9tS5aG...  |          |
+------------------------+-----------------------------------------------------+----------+
| dist/id_rsa            | Expected file to not to contain                     | medium   |
|                        | base64 encoded texts such as:                       |          |
|                        | hvroGenpK/IXcW4WSZYo9mIlCBfBg811z0pvSe/Z78L1g8t...  |          |
+------------------------+-----------------------------------------------------+----------+
| dist/id_rsa            | Expected file to not to contain                     | medium   |
|                        | base64 encoded texts such as:                       |          |
|                        | M2C/UMDCAWH2zHWwAAABFyb290QDJlOGJlZWEwZjQyNg==      |          |
+------------------------+-----------------------------------------------------+----------+
| sqlitedborm/id_rsa.pub | Expected file to not to contain                     | medium   |
|                        | base64 encoded texts such as:                       |          |
|                        | AAAAB3NzaC1yc2EAAAADAQABAAABgQCm+vxerXiYix6BvQj...  |          |
```

```
If you are absolutely sure that you want to ignore the above files from talisman detectors, consider pasting the following f
ormat in .talismanrc file in the project root

fileignoreconfig:
- filename: dist/id_rsa
  checksum: 3d7877ad9147d39ab600628dc684a785e28402e8c966d3c70cef3a8ea538f375
- filename: sqlitedborm/id_rsa.pub
  checksum: 3e5299e779af3cb809d5723b1e6a87e5fd92c97d8b0a67be010e820284b71082

root@attackdefense:~/github-repos/sqlitedborm#
```

Issues Detected

- SSH keys are detected by the talisman.

Learnings

Perform sensitive information scanning with talisman utility.