ATTACK DEFENSE

by PentesterAcademy

Name	Pre-commit: Scanning source code for Sensitive Information
URL	https://www.attackdefense.com/challengedetails?cid=2266
Type	DevSecOps 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

The Pre-commit tool is used to find sensitive data in the source code of the application using the defined plugins in the config.

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

Objective: Use the pre-commit utility to find sensitive information in the applications!

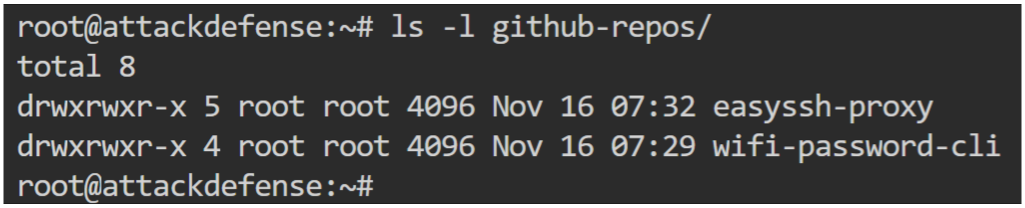
Instructions:

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

Solution

Step 1: Check the provided applications.

Command: ls -l github-repos



```
root@attackdefense:~# ls -l github-repos/
total 8
drwxrwxr-x 5 root root 4096 Nov 16 07:32 easyssh-proxy
drwxrwxr-x 4 root root 4096 Nov 16 07:29 wifi-password-cli
root@attackdefense:~#
```

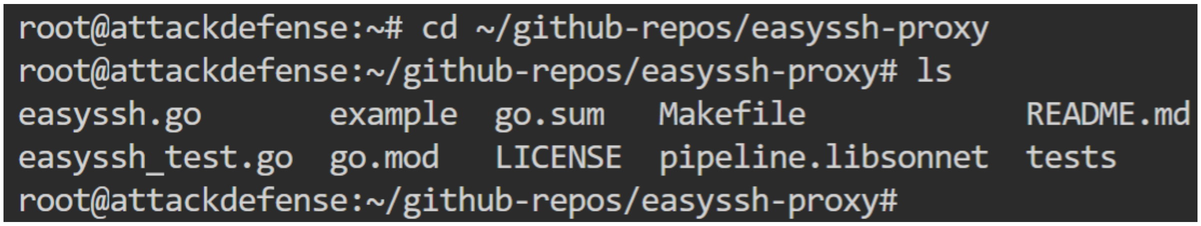
We will take one example at a time and run the tool on that.

Example 1: easyssh-proxy

Step 1: Navigate to the easyssh-proxy project directory

Commands:

```
cd ~/github-repos/easyssh-proxy
ls
```



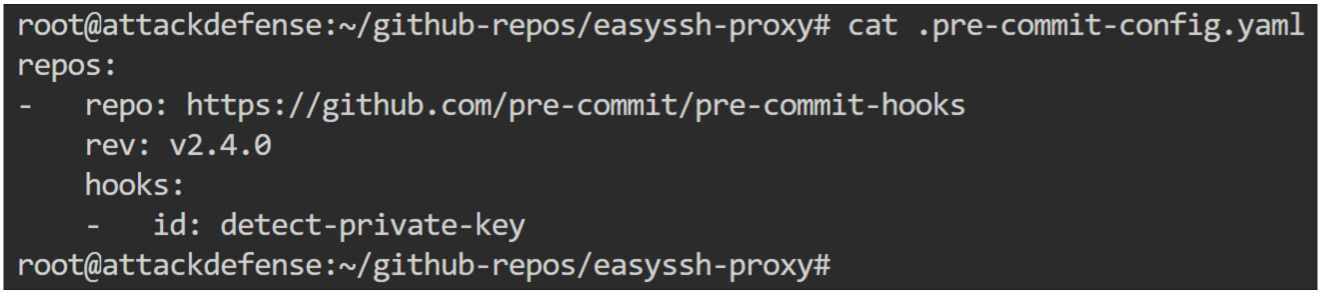
```
root@attackdefense:~# cd ~/github-repos/easyssh-proxy
root@attackdefense:~/github-repos/easyssh-proxy# ls
easyssh.go       example  go.sum   Makefile            README.md
easyssh_test.go  go.mod   LICENSE  pipeline.libsonnet  tests
root@attackdefense:~/github-repos/easyssh-proxy#
```

Step 2: Create the config file for pre-commit tool to detect the private keys.

Command: vim .pre-commit-config.yaml

```
repos:
-   repo: https://github.com/pre-commit/pre-commit-hooks
    rev: v2.4.0
    hooks:
    -   id: detect-private-key
```

Save the file

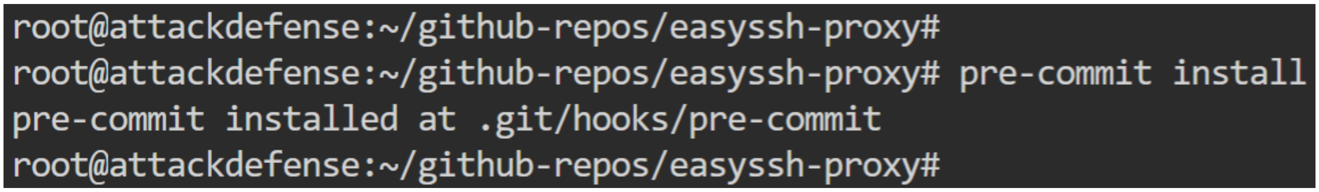


```
root@attackdefense:~/github-repos/easyssh-proxy# cat .pre-commit-config.yaml
repos:
-   repo: https://github.com/pre-commit/pre-commit-hooks
    rev: v2.4.0
    hooks:
    -   id: detect-private-key
root@attackdefense:~/github-repos/easyssh-proxy#
```

The configuration will check for the SSH private keys in the source code of the application

Step 3: Initialise the pre-commit in the repository

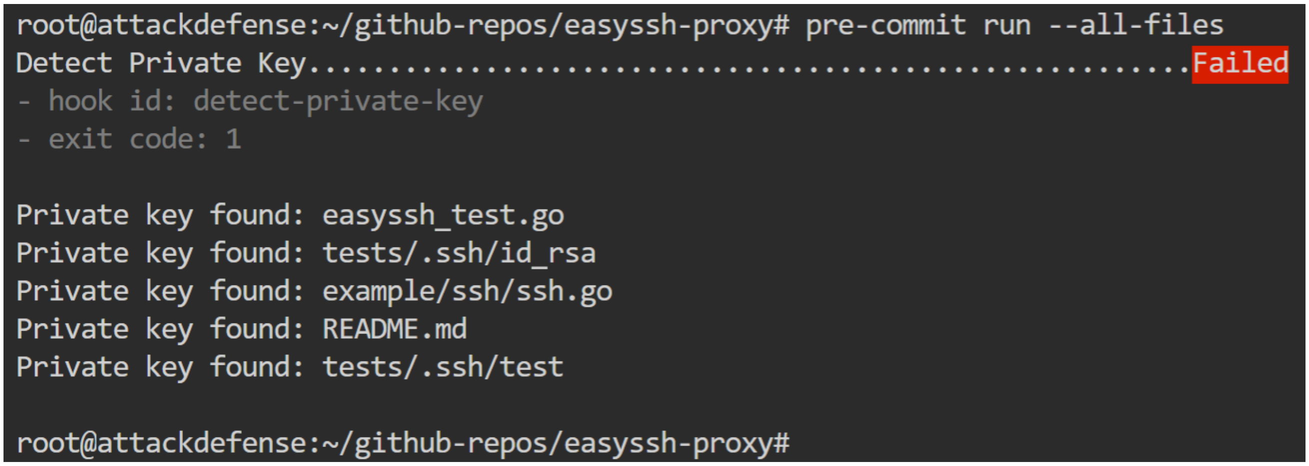
Command: pre-commit install



```
root@attackdefense:~/github-repos/easyssh-proxy#
root@attackdefense:~/github-repos/easyssh-proxy# pre-commit install
pre-commit installed at .git/hooks/pre-commit
root@attackdefense:~/github-repos/easyssh-proxy#
```

Step 4: Run the pre-commit tool on the repository to find the private keys.

Command: pre-commit run --all-files



```
root@attackdefense:~/github-repos/easyssh-proxy# pre-commit run --all-files
Detect Private Key.................................................Failed
- hook id: detect-private-key
- exit code: 1

Private key found: easyssh_test.go
Private key found: tests/.ssh/id_rsa
Private key found: example/ssh/ssh.go
Private key found: README.md
Private key found: tests/.ssh/test

root@attackdefense:~/github-repos/easyssh-proxy#
```

The pre-commit tool identified multiple keys being exposed in the source code of the application

Issues Detected:

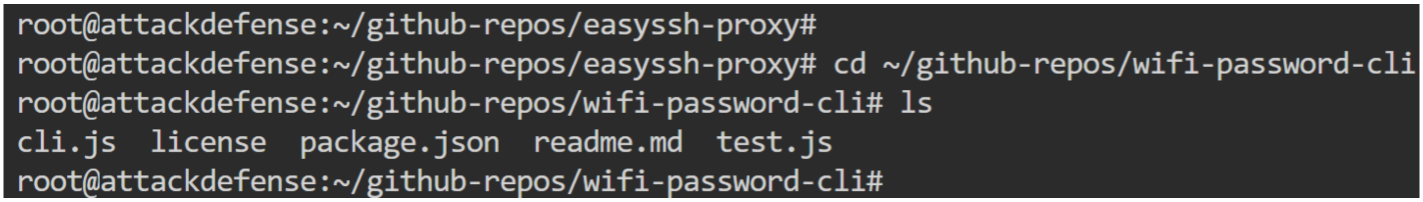
- Private key exposed in multiple files

Example 2: wifi-password-cli

Step 1: Navigate to the wifi-password-cli directory.

Commands:

```
cd ~/github-repos/wifi-password-cli
ls
```



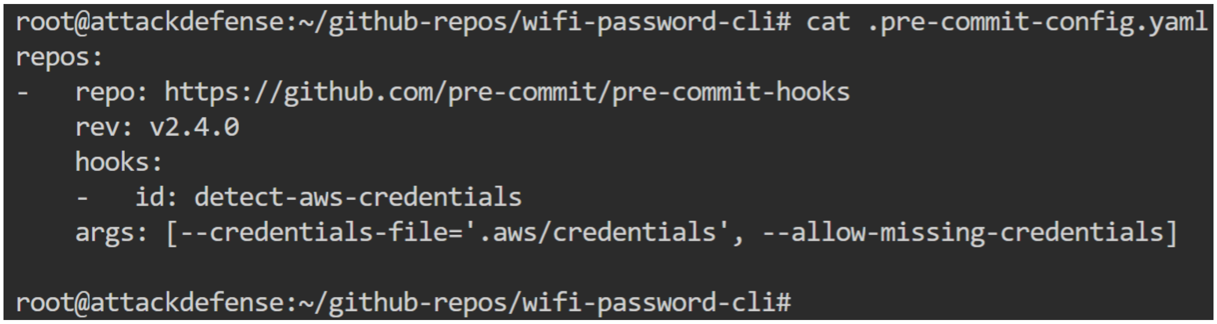
```
root@attackdefense:~/github-repos/easyssh-proxy#
root@attackdefense:~/github-repos/easyssh-proxy# cd ~/github-repos/wifi-password-cli
root@attackdefense:~/github-repos/wifi-password-cli# ls
cli.js  license  package.json  readme.md  test.js
root@attackdefense:~/github-repos/wifi-password-cli#
```

Step 2: Create the config file for pre-commit tool to detect the aws credentials files and insecure configuration.

Command: vim .pre-commit-config.yaml

```
repos:
-   repo: https://github.com/pre-commit/pre-commit-hooks
    rev: v2.4.0
    hooks:
    -   id: detect-aws-credentials
    args: [--credentials-file='.aws/credentials', --allow-missing-credentials]
```

Save the file



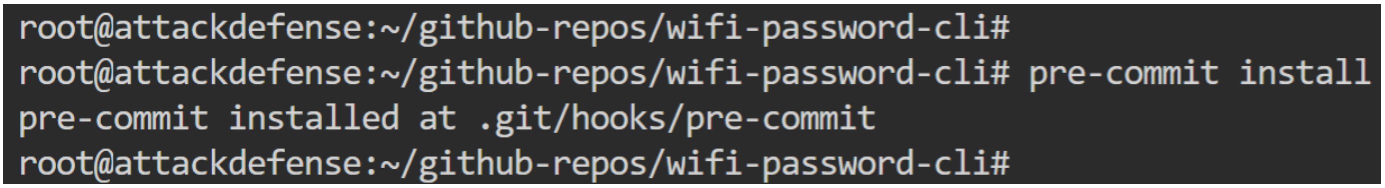
```
root@attackdefense:~/github-repos/wifi-password-cli# cat .pre-commit-config.yaml
repos:
-   repo: https://github.com/pre-commit/pre-commit-hooks
    rev: v2.4.0
    hooks:
    -   id: detect-aws-credentials
    args: [--credentials-file='.aws/credentials', --allow-missing-credentials]

root@attackdefense:~/github-repos/wifi-password-cli#
```

The configuration will check for the AWS credentials in the source code of the application

Step 3: Initialise the pre-commit in the repository

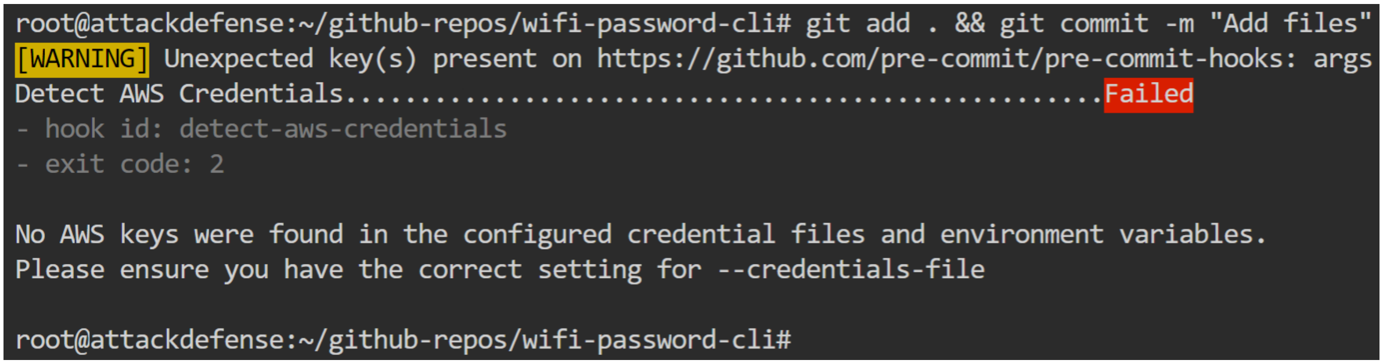
Command: pre-commit install



```
root@attackdefense:~/github-repos/wifi-password-cli#
root@attackdefense:~/github-repos/wifi-password-cli# pre-commit install
pre-commit installed at .git/hooks/pre-commit
root@attackdefense:~/github-repos/wifi-password-cli#
```

Step 4: Add the changes to the local git repository.

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



```
root@attackdefense:~/github-repos/wifi-password-cli# git add . && git commit -m "Add files"
[WARNING] Unexpected key(s) present on https://github.com/pre-commit/pre-commit-hooks: args
Detect AWS Credentials...................................................Failed
- hook id: detect-aws-credentials
- exit code: 2

No AWS keys were found in the configured credential files and environment variables.
Please ensure you have the correct setting for --credentials-file

root@attackdefense:~/github-repos/wifi-password-cli#
```

While trying to commit the files, the pre-commit identified AWS credentials stored inside the source code which could be leaked publicly.

Issues Detected:

- AWS Credentials exposed

Learnings

Perform Sensitive Information Scan using the Pre-commit tool.