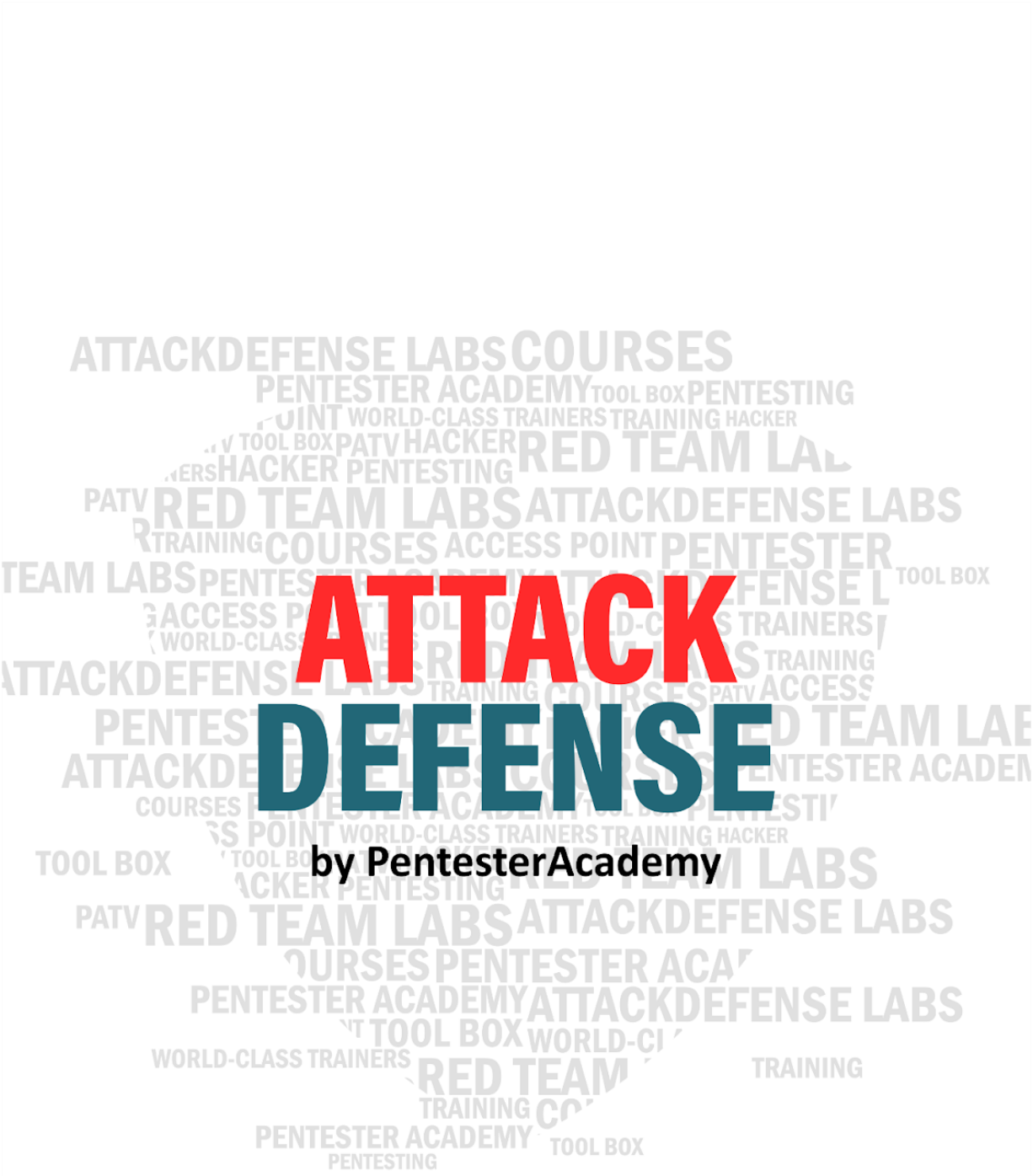
ATTACK
DEFENSE
by PentesterAcademy

Name	Git Hound: Sniffing Sensitive Information
URL	https://www.attackdefense.com/challengedetails?cid=2153
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 Git-Hound tool is used to find sensitive information in the application source code.

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

Objective: Use the git-hound utility to find vulnerabilities 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 8 root root 4096 Nov 18 07:09 django-rosetta
drwxrwxr-x 7 root root 4096 Nov 18 07:08 django-todolist
root@attackdefense:~#
```

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

Example 1: django-todolist

Step 1: Navigate to the django-todolist project directory.

Commands:
cd ~/github-repos/django-todolist
ls

```
root@attackdefense:~# cd ~/github-repos/django-todolist
root@attackdefense:~/github-repos/django-todolist#
root@attackdefense:~/github-repos/django-todolist# ls
accounts  api  LICENSE  lists  manage.py  README.md  requirements.txt  todolist
root@attackdefense:~/github-repos/django-todolist#
```

Step 2: Create a configuration file as ".githound.yml" to get warnings wherever "username" has appeared in the source code.

Command: vim .githound.yml

warn:
  - '(?i)user(name)?\W*[:=,]\W*.+$'

```
root@attackdefense:~/github-repos/django-todolist# cat .githound.yml
warn:
  - '(?i)user(name)?\W*[:=,]\W*.+$'

root@attackdefense:~/github-repos/django-todolist#
```

Step 3: Run the git hound tool inside the project directory.

Command: git-hound sniff

```
root@attackdefense:~/github-repos/django-todolist# git-hound  sniff
warning: pattern `(?i)user(name)?\W*[:=,]\W*.+$` match found for `self.user = User.objects.create_user("test"
, "test@example.com", "test")` starting at line 1 in lists/tests.py
warning: pattern `(?i)user(name)?\W*[:=,]\W*.+$` match found for `+    username = forms.CharField(` starting
at line 1 in accounts/forms.py
warning: pattern `(?i)user(name)?\W*[:=,]\W*.+$` match found for `self.client.login(username="test", password
="test")` starting at line 1 in lists/tests.py
warning: pattern `(?i)user(name)?\W*[:=,]\W*.+$` match found for `+        username = self.cleaned_data.get("
username")` starting at line 1 in accounts/forms.py
warning: pattern `(?i)user(name)?\W*[:=,]\W*.+$` match found for `user = User.objects.filter(username=usernam
e).first()` starting at line 1 in accounts/forms.py
warning: pattern `(?i)user(name)?\W*[:=,]\W*.+$` match found for `+    username = forms.CharField(` starting
at line 1 in accounts/forms.py
warning: pattern `(?i)user(name)?\W*[:=,]\W*.+$` match found for `self.user = User.objects.create_user("test"
, "test@example.com", "test")` starting at line 1 in lists/tests.py
warning: pattern `(?i)user(name)?\W*[:=,]\W*.+$` match found for `fields = ("id", "username", "last_login", "
date_joined", "todolists")` starting at line 1 in api/serializers.py
warning: pattern `(?i)user(name)?\W*[:=,]\W*.+$` match found for `user = authenticate(` starting at line 1 in
 accounts/views.py
warning: pattern `(?i)user(name)?\W*[:=,]\W*.+$` match found for `form = LoginForm({"username": "test", "pass
word": ""})` starting at line 1 in accounts/tests.py
warning: pattern `(?i)user(name)?\W*[:=,]\W*.+$` match found for `"username": "test",` starting at line 1 in
accounts/tests.py
warning: pattern `(?i)user(name)?\W*[:=,]\W*.+$` match found for `"username": "test",` starting at line 1 in
accounts/tests.py
warning: pattern `(?i)user(name)?\W*[:=,]\W*.+$` match found for `"username": "test",` starting at line 1 in
accounts/tests.py
root@attackdefense:~/github-repos/django-todolist#
```

The output displayed multiple warnings which contain part of the source code where “username” was written.

Example 2: django-todolist (Multiple errors)

Step 1: Modify the “.githound.yml” file to detect “password” in the source code and display them as errors

Command: vim .githound.yml

```
fail:
  - '["'"](?!.*[\s])(?=.*[A-Za-z])(?=.*[0-9])(?=.*[!@#$&*])?.{16,}["'"]'
  - '(?i)pass(word)?\W*[:=,]\W*.+$'
```

```
root@attackdefense:~/github-repos/django-todolist# cat .githound.yml
fail:
  - '['"](?!.*[\s])(?=.*[A-Za-z])(?=.*[0-9])(?=.*[!@#$&*])?.{16,}['"]'
  - '(?i)pass(word)?\W*[:=,]\W*.+$'

root@attackdefense:~/github-repos/django-todolist#
```

Step 2: Run the git hound tool inside the project directory.

Command: git-hound sniff

```
root@attackdefense:~/github-repos/django-todolist# git-hound sniff
failure: pattern `(?i)pass(word)?\W*[:=,]\W*.+$` match found for `username=request.POST["username"], passwor
d=request.POST["password"]` starting at line 1 in accounts/views.py
failure: pattern `(?i)pass(word)?\W*[:=,]\W*.+$` match found for `password=request.POST["password"],` starti
ng at line 1 in accounts/views.py
failure: pattern `(?i)pass(word)?\W*[:=,]\W*.+$` match found for `self.client.login(username="test", passwor
d="test")` starting at line 1 in api/tests.py
failure: pattern `['"](?!.*[\s])(?=.*[A-Za-z])(?=.*[0-9])(?=.*[!@#$&*])?.{16,}['"]` match found for `SECRET_
KEY = "@e2(yx)v&tgh3_s=0yja-i!dpebxsz^dg47x)-k&kq_3zf*9e*"` starting at line 1 in todolist/settings.py
failure: pattern `(?i)pass(word)?\W*[:=,]\W*.+$` match found for `self.client.login(username="admin", passwo
rd="admin")` starting at line 1 in api/tests.py
failure: pattern `(?i)pass(word)?\W*[:=,]\W*.+$` match found for `self.client.login(username="test", passwor
d="test")` starting at line 1 in api/tests.py
failure: pattern `['"](?!.*[\s])(?=.*[A-Za-z])(?=.*[0-9])(?=.*[!@#$&*])?.{16,}['"]` match found for `"ENGINE
": "django.db.backends.sqlite3",` starting at line 1 in todolist/settings.py
failure: pattern `['"](?!.*[\s])(?=.*[A-Za-z])(?=.*[0-9])(?=.*[!@#$&*])?.{16,}['"]` match found for `respons
e = self.client.get("/api/todolists/1/")` starting at line 1 in api/tests.py
failure: pattern `['"](?!.*[\s])(?=.*[A-Za-z])(?=.*[0-9])(?=.*[!@#$&*])?.{16,}['"]` match found for `respons
e = self.client.get("/api/todolists/0/")` starting at line 1 in api/tests.py
failure: pattern `(?i)pass(word)?\W*[:=,]\W*.+$` match found for `self.assertEqual(form.errors, {"password":
 ["This field is required."]})` starting at line 1 in accounts/tests.py
failure: pattern `(?i)pass(word)?\W*[:=,]\W*.+$` match found for `"password": "test",` starting at line 1 in
 accounts/tests.py
failure: pattern `(?i)pass(word)?\W*[:=,]\W*.+$` match found for `"password": "test",` starting at line 1 in
 accounts/tests.py
failure: pattern `(?i)pass(word)?\W*[:=,]\W*.+$` match found for `"password": "test1",` starting at line 1 i
n accounts/tests.py
36 severe smell(s) detected - please fix them before you can commit
root@attackdefense:~/github-repos/django-todolist#
```

The output displayed multiple warnings including “test” as hardcoded credentials as username and password.

Issues Detected:

- Hardcoded credentials found in the application

Example 2: Django-rosetta

Step 1: Navigate to the django-rosetta project directory.

Commands:
cd ~/github-repos/django-rosetta
ls

```
root@attackdefense:~/github-repos/django-todolist#
root@attackdefense:~/github-repos/django-todolist# cd ~/github-repos/django-rosetta
root@attackdefense:~/github-repos/django-rosetta# ls
CHANGES  docs  LICENSE  MANIFEST.in  README.rst  rosetta  setup.py  testproject  tox.ini
root@attackdefense:~/github-repos/django-rosetta#
```

Step 2: Create a configuration file as ".githound.yml" to detect AWS Client ID from the source code.

Command: vim .githound.yml

```
fail:
  - '(A3T[A-Z0-9]|AKIA|AGPA|AIDA|AROA|AIPA|ANPA|ANVA|ASIA)[A-Z0-9]{16}'
```

```
root@attackdefense:~/github-repos/django-rosetta#
root@attackdefense:~/github-repos/django-rosetta# cat .githound.yml
fail:
  - '(A3T[A-Z0-9]|AKIA|AGPA|AIDA|AROA|AIPA|ANPA|ANVA|ASIA)[A-Z0-9]{16}'
root@attackdefense:~/github-repos/django-rosetta#
```

Step 3: Run the git hound tool inside the project directory.

Command: git-hound sniff

```
root@attackdefense:~/github-repos/django-rosetta# cat .githound.yml
fail:
  - '(A3T[A-Z0-9]|AKIA|AGPA|AIDA|AROA|AIPA|ANPA|ANVA|ASIA)[A-Z0-9]{16}'
root@attackdefense:~/github-repos/django-rosetta#
root@attackdefense:~/github-repos/django-rosetta#
root@attackdefense:~/github-repos/django-rosetta# git-hound sniff
failure: pattern `(A3T[A-Z0-9]|AKIA|AGPA|AIDA|AROA|AIPA|ANPA|ANVA|ASIA)[A-Z0-9]{16}` match found for `aws_cl
ient_id = AKIAUAWOPGE5KXVUKUPE` starting at line 1 in .aws/credentials
1 severe smell(s) detected - please fix them before you can commit
root@attackdefense:~/github-repos/django-rosetta#
```

The output displayed the hardcoded AWS client id found in the source code.

Issues Detected:

- Exposed AWS client ID

Learnings

Perform Sensitive Information Scan using the Git Hound tool.

References:

- Django-todolist (https://github.com/rtzll/django-todolist)
- Django-rosetta (https://github.com/mbi/django-rosetta.git)