ATTACK DEFENSE

by PentesterAcademy

Name	PyPi Server: Reversing Packages
URL	https://www.attackdefense.com/challengedetails?cid=1066
Type	Code Repository : Python PyPi

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.

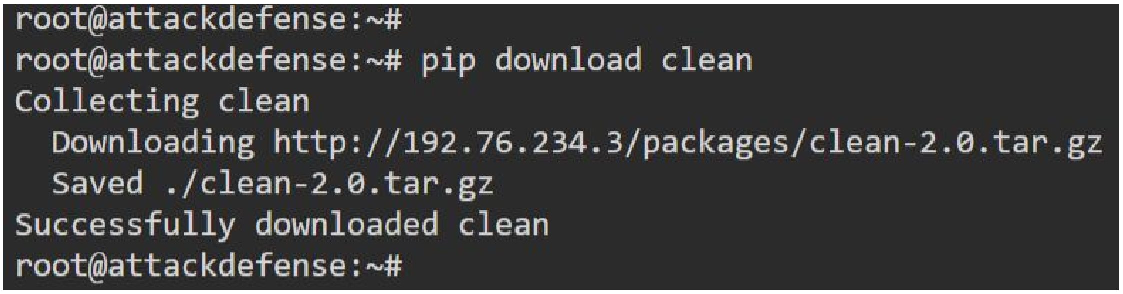
A flag file is hidden in a python package named "clean" which is hosted on a local PyPi server. Your machine is already configured to use this PyPi server.

Objective: Retrieve the flag!

Solution:

Step 1: Download “clean” package from the PyPi server.

Commands: pip download clean

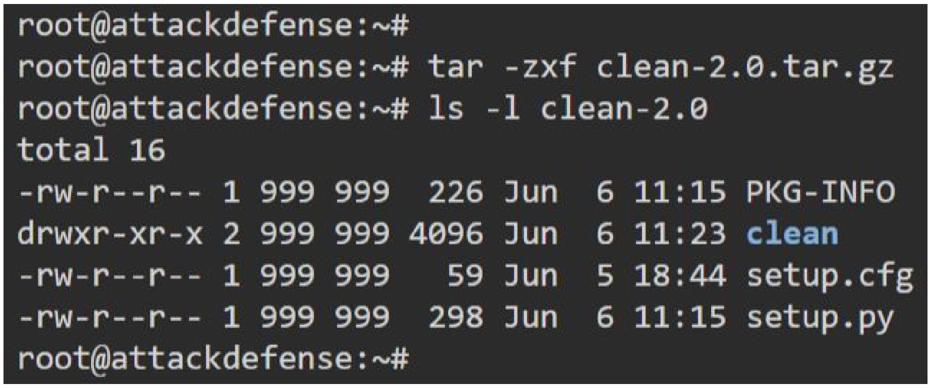


```
root@attackdefense:~#
root@attackdefense:~# pip download clean
Collecting clean
  Downloading http://192.76.234.3/packages/clean-2.0.tar.gz
  Saved ./clean-2.0.tar.gz
Successfully downloaded clean
root@attackdefense:~#
```

Step 2: Extract the package and check its contents.

Commands:
tar -zxf clean-2.0.tar.gz

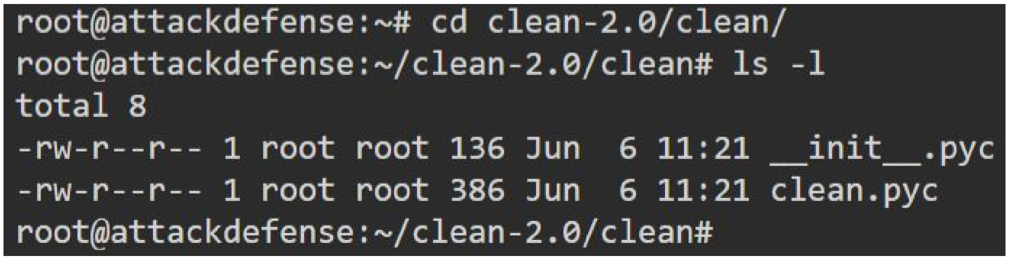
ls -l clean-2.0



```
root@attackdefense:~#
root@attackdefense:~# tar -zxf clean-2.0.tar.gz
root@attackdefense:~# ls -l clean-2.0
total 16
-rw-r--r-- 1 999 999  226 Jun  6 11:15 PKG-INFO
drwxr-xr-x 2 999 999 4096 Jun  6 11:23 clean
-rw-r--r-- 1 999 999   59 Jun  5 18:44 setup.cfg
-rw-r--r-- 1 999 999  298 Jun  6 11:15 setup.py
root@attackdefense:~#
```

Step 3: Change to code directory. Only .pyc files are present in it.

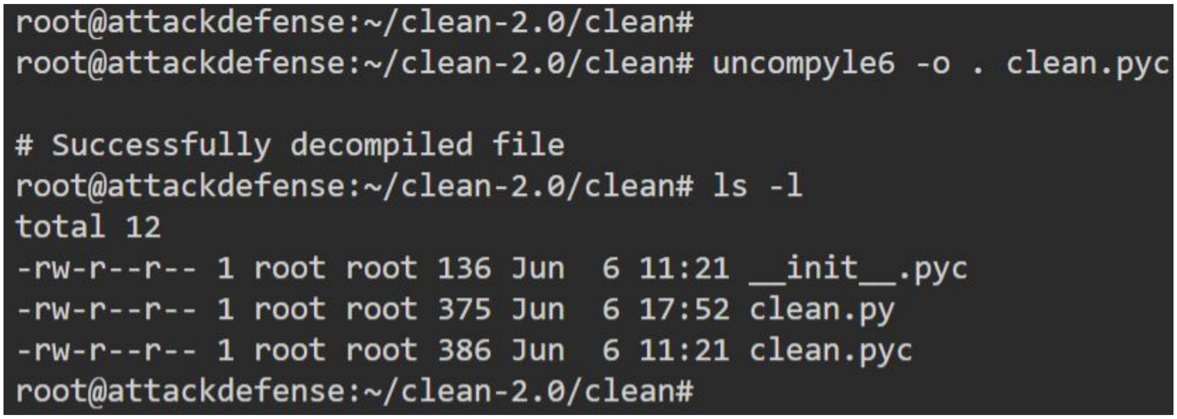
Commands:
cd clean-2.0/clean/
ls -l



```
root@attackdefense:~# cd clean-2.0/clean/
root@attackdefense:~/clean-2.0/clean# ls -l
total 8
-rw-r--r-- 1 root root 136 Jun  6 11:21 __init__.pyc
-rw-r--r-- 1 root root 386 Jun  6 11:21 clean.pyc
root@attackdefense:~/clean-2.0/clean#
```

Step 4: Use uncompyle6 to convert .pyc content to .py code. It successfully recovered the python code.

Command: uncompyle6 -o . clean.pyc

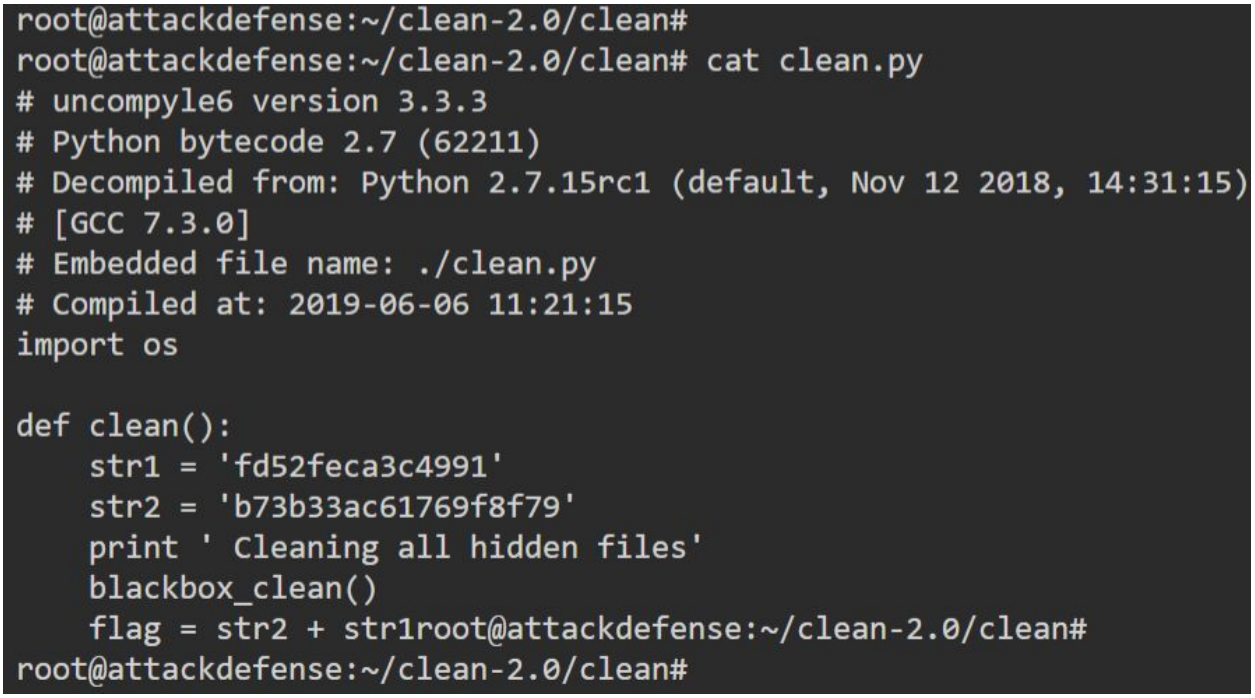


```
root@attackdefense:~/clean-2.0/clean#
root@attackdefense:~/clean-2.0/clean# uncompyle6 -o . clean.pyc

# Successfully decompiled file
root@attackdefense:~/clean-2.0/clean# ls -l
total 12
-rw-r--r-- 1 root root 136 Jun  6 11:21 __init__.pyc
-rw-r--r-- 1 root root 375 Jun  6 17:52 clean.py
-rw-r--r-- 1 root root 386 Jun  6 11:21 clean.pyc
root@attackdefense:~/clean-2.0/clean#
```

Step 5: Check the code for flag value.

Commands: cat clean.py



```
root@attackdefense:~/clean-2.0/clean#
root@attackdefense:~/clean-2.0/clean# cat clean.py
# uncompyle6 version 3.3.3
# Python bytecode 2.7 (62211)
# Decompiled from: Python 2.7.15rc1 (default, Nov 12 2018, 14:31:15)
# [GCC 7.3.0]
# Embedded file name: ./clean.py
# Compiled at: 2019-06-06 11:21:15
import os

def clean():
    str1 = 'fd52feca3c4991'
    str2 = 'b73b33ac61769f8f79'
    print ' Cleaning all hidden files'
    blackbox_clean()
    flag = str2 + str1root@attackdefense:~/clean-2.0/clean#
root@attackdefense:~/clean-2.0/clean#
```

Step 6: Figure out the flag from code.

Flag: b73b33ac61769f8f79fd52feca3c4991

References:

1. pypi (https://pypi.org)
2. pip (https://pypi.org/project/pip/)
3. Python Uncompyle6 (https://github.com/rocky/python-uncompyle6/)