

[illegible]

Name	PyPi Server: Recon Basics
URL	https://www.attackdefense.com/challengedetails?cid=1053
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.

Q1. Which service is running on the target machine? State the complete name.

Answer: WSGIServer 0.2

Command: nmap -p80 -sV 192.4.247.3

```
root@attackdefense:~# nmap -p80 -sV 192.4.247.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-04 18:18 UTC
Nmap scan report for e8a4tp2udvej68ig43gj1kher.temp-network_a-4-247 (192.4.247.3)
Host is up (0.000077s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      WSGIServer 0.2 (Python 3.6.7)
MAC Address: 02:42:C0:04:F7:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 7.01 seconds
root@attackdefense:~#
```

Q2. What is hosted on the HTTP server of the target machine?

Answer: pypiserver

Command: curl http://192.4.247.3

```

root@attackdefense:~# curl http://192.4.247.3
<html><head><title>Welcome to pypiserver!</title></head><body>
<h1>Welcome to pypiserver!</h1>
<p>This is a PyPI compatible package index serving 11 packages.</p>

<p> To use this server with pip, run the the following command:
<blockquote><pre>
pip install --extra-index-url http://192.4.247.3/ PACKAGE [PACKAGE2...]
</pre></blockquote></p>

<p> To use this server with easy_install, run the the following command:
<blockquote><pre>
easy_install -i http://192.4.247.3/simple/ PACKAGE
</pre></blockquote></p>

<p>The complete list of all packages can be found <a href="/packages/">here</a>
or via the <a href="/simple/">simple</a> index.</p>

```

Q3. Install pywinwifi from local repository, to attacker machine?

Command: `pip install --trusted-host 192.4.247.3 --index-url http://192.4.247.3 pywinwifi`

```

root@attackdefense:~# pip install --trusted-host 192.4.247.3 --index-url http://192.4.247.3 pywinwifi
Looking in indexes: http://192.4.247.3
Collecting pywinwifi
  Downloading http://192.4.247.3/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/ee/52/d3/db7a28dbb1e98965694238552d84a90cf07064453bba75bb91
Successfully built pywinwifi
Installing collected packages: pywinwifi
Successfully installed pywinwifi-1.0.0
root@attackdefense:~#

```

Q4. Which version of awscli is available on the remote server?

Answer: 1.16.170

Solution:

Step 1: Configure local repo as default and trusted.

```
root@attackdefense:~#  
root@attackdefense:~# cat /etc/pip.conf  
[global]  
index = http://192.4.247.3  
index-url = http://192.4.247.3  
trusted-host = 192.4.247.3  
root@attackdefense:~#
```

Step 2: Search for package using pip

Commands: pip search awscli

```
root@attackdefense:~#  
root@attackdefense:~# pip search awscli  
awscli (1.16.170) - 1.16.170  
root@attackdefense:~#
```

Q5. How many packages are present on the PyPi server?

Answer: 6

Solution:

Curl command to PyPi repository URL returns list of packages

Command: curl http://192.4.247.3/simple/


```
root@attackdefense:~# curl http://192.4.247.3/simple/
<html>
  <head>
    <title>Simple Index</title>
  </head>
  <body>
    <h1>Simple Index</h1>
    <a href="awscli/">awscli</a><br>
    <a href="docutils/">docutils</a><br>
    <a href="pywinwifi/">pywinwifi</a><br>
    <a href="requests/">requests</a><br>
    <a href="s3transfer/">s3transfer</a><br>
    <a href="urllib3/">urllib3</a><br>
  </body>
</html>
root@attackdefense:~#
```

Alternatively, one can also use browsh to access the same page.

Command: browsh --startup-url 192.4.247.3/simple/

```
Simple Index |
http://192.4.247.3/simple/

Simple Index
awscli
docutils
pywinwifi
requests
s3transfer
urllib3
```

Q6. There is a flag hidden in pywinwifi package. Retrieve and submit that flag.

Answer: ab437d40430985a1abd69b1747f37a12

Solution:

Download the pywinwifi package from the server

Command: pip download --trusted-host 192.4.247.3 --index-url http://192.4.247.3 pywinwifi

```
root@attackdefense:~# pip download --trusted-host 192.4.247.3 --index-url http://192.4.247.3 pywinwifi
Looking in indexes: http://192.4.247.3
Collecting pywinwifi
  Downloading http://192.4.247.3/packages/pywinwifi-1.0.0.zip
  Saved ./pywinwifi-1.0.0.zip
Successfully downloaded pywinwifi
root@attackdefense:~#
```

Extract the zip archive.


Command: unzip pywinwifi-1.0.0.zip

```
root@attackdefense:~# unzip pywinwifi-1.0.0.zip
Archive:  pywinwifi-1.0.0.zip
  creating: pywinwifi-1.0.0/
  inflating: pywinwifi-1.0.0/setup.py
  inflating: pywinwifi-1.0.0/PKG-INFO
  creating: pywinwifi-1.0.0/pywinwifi/
  inflating: pywinwifi-1.0.0/pywinwifi/WindowsWifi.py
  extracting: pywinwifi-1.0.0/pywinwifi/__init__.py
  inflating: pywinwifi-1.0.0/pywinwifi/pywinwifi.py
  extracting: pywinwifi-1.0.0/pywinwifi/flag
  inflating: pywinwifi-1.0.0/pywinwifi/WindowsNativeWifiApi.py
root@attackdefense:~#
```

Print the flag file.

Command: cat pywinwifi-1.0.0/pywinwifi/flag

```
root@attackdefense:~#
root@attackdefense:~# cat pywinwifi-1.0.0/pywinwifi/flag
ab437d40430985a1abd69b1747f37a12
root@attackdefense:~#
```



Flag: ab437d40430985a1abd69b1747f37a12

References:

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