Python for Pentesters

Start AttackBox | Show Split View | Cloud Details | Awards | Help

Python is probably the most widely used and most convenient scripting language in cybersecurity. This room covers real examples of Python scripts including hash cracking, key logging, enumeration and scanning.

✕

Chart | Scoreboard | Discuss | Writeups | More

Difficulty: Easy

Active Machine Information

Title	IP Address	Expires	
Py4PT2	10.10.96.99	1h 40m 28s	? Add 1 hour Terminate

41%

Task 1 ✓ Introduction

Task 2 ✓ Subdomain Enumeration

Task 3 ✓ Directory Enumeration

Task 4 ✓ Network Scanner

Task 5 ○ Port Scanner

In this task, we will be looking at a script to build a simple port scanner.

The code:

```
import sys
import socket
import pyfiglet


ascii_banner = pyfiglet.figlet_format("TryHackMe \n Python 4 Pentesters \nPort Scanner")
print(ascii_banner)


ip = '192.168.1.6'
open_ports =[]

ports = range(1, 65535)


def probe_port(ip, port, result = 1):
  try:
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    sock.settimeout(0.5)
    r = sock.connect_ex((ip, port))
    if r == 0:
      result = r
    sock.close()
  except Exception as e:
    pass
  return result


for port in ports:
    sys.stdout.flush()
    response = probe_port(ip, port)
    if response == 0:
        open_ports.append(port)


if open_ports:
  print ("Open Ports are: ")
  print (sorted(open_ports))
else:
  print ("Looks like no ports are open :(")
```

To better understand the port scanning process, we can break down the code into several sections:

Importing modules that will help the code run:

```
import sys
```

```
import socket
```

Modules could also be imported with a single line using

```
import socket,sys
```

Specifying the target:

```
ip = '192.168.1.6'
```

An empty "open_ports" array that will be populated later with the detected open ports:

```
open_ports =[]
```

Ports that will be probed:

```
ports = range(1, 65535)
```

For this example, we have chosen to scan all TCP ports using the range() function. However, if you are looking for a specific service or want to save time by scanning a few common ports, the code could be changed as follows;

```
ports = { 21, 22, 23, 53, 80, 135, 443, 445}
```

The list above is relatively small. As we are trying to keep a rather low profile, we have limited the list to ports that will likely be used by systems connected to a corporate network.

Getting the IP address of the domain name given as target. The code also works if the user directly provides the IP address.

```
ip = socket.gethostbyname(host)
```

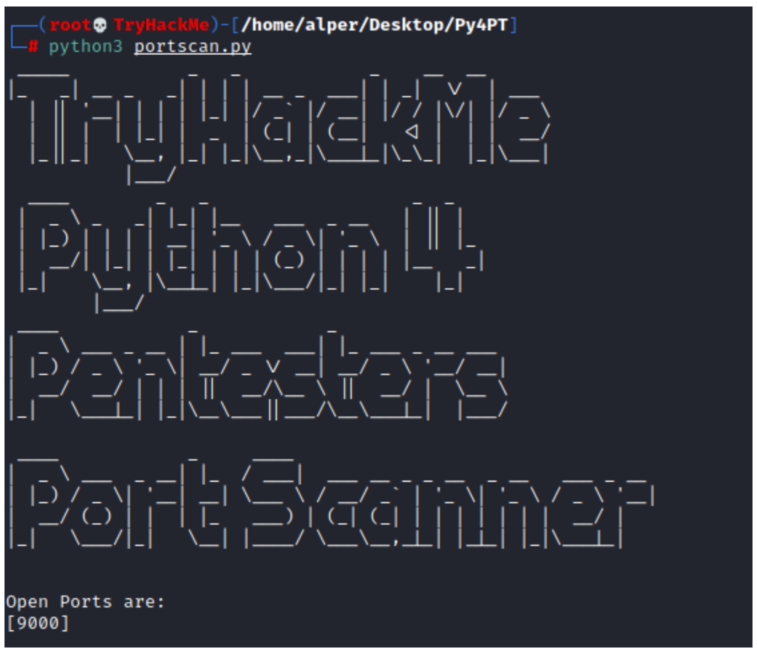
Tries to connect to the port:

```
def probe_port(ip, port, result = 1):
  try:
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    sock.settimeout(0.5)
    r = sock.connect_ex((ip, port))
    if r == 0:
      result = r
    sock.close()
  except Exception as e:
    pass
  return result
```

This code is followed by a for loop that iterates through the specified port list:

```
for port in ports:
    sys.stdout.flush()
    response = probe_port(ip, port)
    if response == 0:
        open_ports.append(port)
```

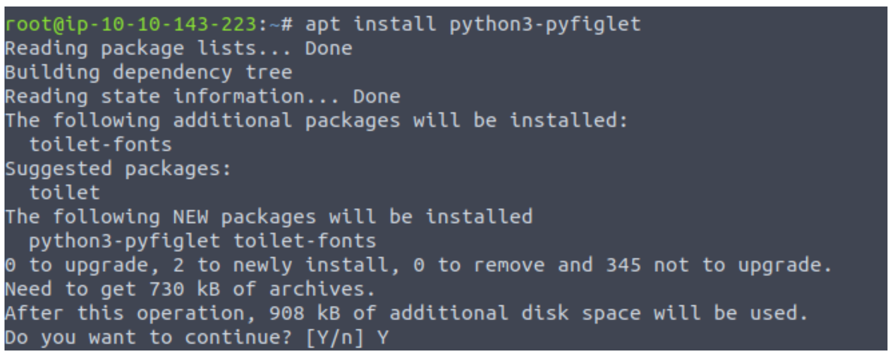
Below are the results of the port scanning script run against a random target.



```
┌──(root💀 TryHackMe)-[/home/alper/Desktop/Py4PT]
└─# python3 portscan.py
```

```
Open Ports are:
[9000]
```

Of course, I will be the first one to admit the ASCII art banner was a bit much. The banner will require Pyfiglet to be imported. If you are using the AttackBox, you can easily install pyfiglet using the "apt install python3-pyfiglet" command.



```
root@ip-10-10-143-223:~# apt install python3-pyfiglet
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  toilet-fonts
Suggested packages:
  toilet
The following NEW packages will be installed
  python3-pyfiglet toilet-fonts
0 to upgrade, 2 to newly install, 0 to remove and 345 not to upgrade.
Need to get 730 kB of archives.
After this operation, 908 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

If you wish to remove the banner you can simply delete the following lines:

```
ascii_banner = pyfiglet.figlet_format("TryHackMe \n Python 4 Pentesters \nPort Scanner")
```

```
print(ascii_banner)
```

Answer the questions below

What protocol will most likely be using TCP port 22?

Answer format: *** Submit

What module did we import to be able to use sockets?

Answer format: ****** Submit

What function is likely to fail if we didn't import sys?

Answer format: ***.******.******* Submit

How many ports are open on the target machine?

Answer format: * Submit

What is the highest port number open on the target system?

Answer format: **** Submit

Task 6 ○ File Downloader

Task 7 ○ Hash Cracker

Task 8 ○ Keyloggers

Task 9 ○ SSH Brute Forcing

Task 10 ○ Extra challenges

Created by

tryhackme

Only subscribers can deploy virtual machines in this room! Go to your profile page to subscribe (if you have not already). 20121 users are in here and this room is 594 days old.