

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Writing a simple Port Scanner in Python3](#)

guardian - December 29, 2020, 7:20 am

Python, a simple, yet so powerful, language

It was what got me into coding, made my first steps with it

I know how frustrating it can be to know and understand all the basic stuff, but still not be able to build useful tools

In this tutorial I will teach you how to write a simple port scanner in python, which can be really useful in some situations, i.e. pentesting (you have a system and python3 installed and want to scan ports quickly)

We are going to use the Python3 socket library for this

The first thing we have to is to import the socket library inside our python file

Code import socket

Now that we have it imported, let's set a default timeout for connections so that ports will not load forever, without returning any valuable data

This sets the default timeout for connections to 5 seconds

Code socket.setdefaulttimeout(5)

We also need a socket to send and receive data, so let's create one

Code s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

AF_INET indicates that we will connect using IP protocol version 4

SOCK_STREAM indicates that we will use TCP as our transfer protocol

The variable named s can now be used to utilize the socket

Of course we will want to connect to a host and know, whether it is reachable through the specified port or not

Connections using the socket can be established as follows:

Code s.connect((host, port))

Note that the host needs to be a string and it needs to be reachable using IPV4 (works in most cases)

The port needs to be an integer, so you have to cast it to one, should you receive it as a string at first

Here is the code for a basic port scanner that scans one specified port of one host

Code import socket

def scan(sck, host, port):

try:

sck.connect((host,port))

sck.close()

```
    return True
```

```
except:
```

```
    return False
```

```
def main():
```

```
    port = input("Port to scan: ")
```

```
    host = input("Host to scan: ")
```

```
    socket.setdefaulttimeout(5)
```

```
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
```

```
    if (scan(s, host, int(port))):
```

```
        print("[+] Open port: "+host+"."+port)
```

```
    else:
```

```
        print("[-] "+host+"."+port+" -> Port is closed or protected by a firewall")
```

```
main()
```

It can be modified easily, by simply adding some loop (to check multiple ports) or changing the socket itself to scan via UDP or scan an IPv6 address

If you understand this code and have been struggling to code useful stuff before, congrats! You are now one step further :)

As always, feedback and criticism is welcome